Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22412B

Configuration des services avancés de Windows Server® 2012

Les informations contenues dans ce document, notamment les URL et les autres références aux sites Web, pourront faire l'objet de modifications sans préavis. Sauf mention contraire, les sociétés, produits, noms de domaines, adresses de messagerie, logos, personnes, lieux et événements utilisés dans les exemples sont fictifs et toute ressemblance avec des sociétés, produits, noms de domaines, adresses de messagerie, logos, personnes, lieux et événements réels est purement fortuite et involontaire. L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicable dans son pays. Aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans la permission expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets ou être titulaire de marques, droits d'auteur ou autres droits de propriété intellectuelle portant sur tout ou partie des éléments qui font l'objet du présent document. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

Les noms de fabricants, de produits ou les URL sont fournis uniquement à titre indicatif et Microsoft ne fait aucune déclaration et exclut toute garantie légale, expresse ou implicite, concernant ces fabricants ou l'utilisation des produits avec toutes les technologies Microsoft. L'inclusion d'un fabricant ou produit n'implique pas l'approbation par Microsoft du fabricant ou du produit. Des liens vers des sites Web tiers peuvent être fournis. Ces sites ne sont pas sous le contrôle de Microsoft et Microsoft n'est pas responsable de leur contenu ni des liens qu'ils sont susceptibles de contenir, ni des modifications ou mises à jour de ces sites. Microsoft n'est pas responsable de la diffusion Web ou de toute autre forme de transmission reçue d'un site connexe. Microsoft fournit ces liens pour votre commodité, et l'insertion de n'importe quel lien n'implique pas l'approbation du site en question ou des produits qu'il contient par Microsoft.

© 2013 Microsoft Corporation. Tous droits réservés.

Microsoft et les marques répertoriées à l'adresse http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx sont des marques du groupe de sociétés Microsoft. Toutes les autres marques sont la propriété de leurs propriétaires respectifs.

Numéro de produit : 22412B

Numéro de référence : X18-86876

Date de publication : 3/2013

TERMES DU CONTRAT DE LICENCE MICROSOFT
COURS MICROSOFT AVEC FORMATEUR

Les présents termes du contrat de licence constituent un contrat entre Microsoft Corporation (ou en fonction du lieu où vous vivez, l'un de ses affiliés) et vous. Lisez-les attentivement. Ils portent sur votre utilisation du contenu qui accompagne le présent contrat, y compris le support sur lequel vous l'avez reçu, le cas échéant. Les présents termes de licence s'appliquent également au Contenu du Formateur et aux mises à jour et suppléments pour le Contenu Concédé sous Licence, à moins que d'autres termes n'accompagnent ces produits. ces derniers prévalent.

EN ACCÉDANT AU CONTENU CONCÉDÉ SOUS LICENCE, EN LE TÉLÉCHARGEANT OU EN L'UTILISANT, VOUS ACCEPTEZ CES TERMES. SI VOUS NE LES ACCEPTEZ PAS, N'ACCÉDEZ PAS AU CONTENU CONCÉDÉ SOUS LICENCE, NE LE TÉLÉCHARGEZ PAS ET NE L'UTILISEZ PAS.

Si vous vous conformez aux présents termes du contrat de licence, vous disposez des droits stipulés ci-dessous pour chaque licence acquise.

1. DÉFINITIONS.

a. « Centre de Formation Agréé » désigne un Membre du Programme Microsoft IT Academy ou un Membre Microsoft Learning Competency, ou toute autre entité que Microsoft peut occasionnellement désigner.

b. « Session de Formation Agréée » désigne le cours avec formateur utilisant le Cours Microsoft avec Formateur et mené par un Formateur ou un Centre de Formation Agréé.

c. « Dispositif de la Classe » désigne un (1) ordinateur dédié et sécurisé qu'un Centre de Formation Agréé possède ou contrôle, qui se trouve dans les installations de formation d'un Centre de Formation Agréé et qui répond ou est supérieur au niveau matériel spécifié pour le Cours Microsoft avec Formateur concerné.

d. « Utilisateur Final » désigne une personne qui est (i) dûment inscrite et participe à une Session de Formation Agréée ou à une Session de Formation Privée, (ii) un employé d'un membre MPN, ou (iii) un employé à temps plein de Microsoft.

e. « Contenu Concédé sous Licence » désigne le contenu qui accompagne le présent contrat et qui peut inclure le Cours Microsoft avec Formateur ou le Contenu du Formateur.

f. « Formateur Agréé Microsoft » ou « MCT » désigne une personne qui est (i) engagée pour donner une session de formation à des Utilisateurs Finaux au nom d'un Centre de Formation Agréé ou d'un Membre MPN, et (ii) actuellement Formateur Agréé Microsoft dans le cadre du Programme de Certification Microsoft.

g. « Cours Microsoft avec Formateur » désigne le cours avec formateur Microsoft qui forme des professionnels de l'informatique et des développeurs aux technologies Microsoft. Un Cours Microsoft avec Formateur peut être labellisé cours MOC, Microsoft Dynamics ou Microsoft Business Group.

h. « Membre du Programme Microsoft IT Academy » désigne un membre actif du Programme Microsoft IT Academy.

i. « Membre Microsoft Learning Competency » désigne un membre actif du programme Microsoft Partner Network qui a actuellement le statut Learning Competency.

j. « MOC » désigne le cours avec formateur « Produit de Formation Officiel Microsoft » appelé Cours Officiel Microsoft qui forme des professionnels de l'informatique et des développeurs aux technologies Microsoft.

k. « Membre MPN » désigne un membre actif Silver ou Gold du programme Microsoft Partner Network.

l. « Dispositif Personnel » désigne un (1) ordinateur, un dispositif, une station de travail ou un autre dispositif électronique numérique qui vous appartient ou que vous contrôlez et qui répond ou est supérieur au niveau matériel spécifié pour le Cours Microsoft avec Formateur concerné.

m. « Session de Formation Privée » désigne les cours avec formateur fournis par des Membres MPN pour des clients d'entreprise en vue d'enseigner un objectif de formation prédéfini à l'aide d'un Cours Microsoft avec Formateur. Ces cours ne font l'objet d'aucune publicité ni promotion auprès du grand public et la participation aux cours est limitée aux employés ou sous-traitants du client d'entreprise.

n. « Formateur » désigne (i) un formateur accrédité sur le plan académique et engagé par un Membre du Programme Microsoft IT Academy pour donner une Session de Formation Agréée et/ou (ii) un MCT.

o. « Contenu du Formateur » désigne la version du formateur du Cours Microsoft avec Formateur et tout contenu supplémentaire uniquement conçu à l'usage du Formateur pour donner une session de formation en utilisant le Cours Microsoft avec Formateur. Le Contenu du Formateur peut inclure des présentations Microsoft PowerPoint, un guide de préparation du formateur, des documents de formation du formateur, des packs Microsoft One Note, un guide de préparation de la classe et un formulaire préliminaire de commentaires sur le cours. À des fins de clarification, le Contenu du Formateur ne contient aucun logiciel, disque dur virtuel ni machine virtuelle.

2. DROITS D'UTILISATION. Le Contenu Concédé sous Licence n'est pas vendu. Le Contenu Concédé sous Licence est concédé sous licence sur la ***base d'une copie par utilisateur***, de sorte que vous devez acheter une licence pour chaque personne qui accède au Contenu Concédé sous Licence ou l'utilise.

2.1 Vous trouverez ci-dessous cinq sections de droits d'utilisation. Une seule vous est applicable.

a. **Si vous êtes un Membre du Programme Microsoft IT Academy :**

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :

1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final qui est inscrit à la Session de Formation Agréée et uniquement immédiatement avant le début de la Session de Formation Agréée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
2. fournir à un (1) Utilisateur Final le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
3. fournir à un (1) Formateur le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

pour autant que vous vous conformiez à ce qui suit :

iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,

iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

v. vous veillerez à ce que chaque Utilisateur Final ayant reçu la version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumises aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,

vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

vii. vous n'utiliserez que des Formateurs qualifiés qui ont une connaissance et une expérience approfondies de la technologie Microsoft qui est l'objet du Cours Microsoft avec Formateur donné pour toutes vos Sessions de Formation Agréées.

viii. vous ne donnerez qu'un maximum de 15 heures de formation par semaine pour chaque Session de Formation Agréée qui utilise un cours MOC, et

ix. vous reconnaissez que les Formateurs qui ne sont pas MCT n'auront pas accès à l'ensemble des ressources destinées au formateur du Cours Microsoft avec Formateur.

b. **Si vous êtes un Membre du Microsoft Learning Competency :**

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :

1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final participant à la Session de Formation Agréée et uniquement immédiatement avant le début de la Session de Formation Agréée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
2. fournir à un (1) Utilisateur Final participant à la Session de Formation Agréée le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
3. fournir à un (1) Formateur le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

pour autant que vous vous conformiez à ce qui suit :

iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,

iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

v. vous veillerez à ce que chaque Utilisateur Final ayant reçu une version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumise aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,
vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,
vii. vous n'utiliserez que des Formateurs qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du Cours Microsoft avec Formateur donné pour vos Sessions de Formation Agréées,
viii. vous n'utiliserez que des MCT qualifiés qui possèdent également la Certification Microsoft applicable qui est l'objet du cours MOC donné pour toutes vos Sessions de Formation Agréées utilisant MOC,
ix. vous ne donnerez accès au Cours Microsoft avec Formateur qu'aux Utilisateurs Finaux, et
x. vous ne donnerez accès au Contenu du Formateur qu'aux Formateurs.

c. **Si vous êtes un Membre MPN :**

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.
ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :
    1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final participant à la Session de Formation Privée et uniquement immédiatement avant le début de la Session de Formation Privée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
    2. fournir à un (1) Utilisateur Final qui participe à la Session de Formation Privée le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
    3. fournir à un (1) Formateur qui donne la Session de Formation Privée le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

    pour autant que vous vous conformiez à ce qui suit :
iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,
iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Privée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Privée,
v. vous veillerez à ce que chaque Utilisateur Final ayant reçu une version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumise aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,

vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Privée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Privée,
vii. vous n'utiliserez que des Formateurs qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du Cours Microsoft avec Formateur donné pour toutes vos Sessions de Formation Privées,
viii. vous n'utiliserez que des MCT qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du cours MOC donné pour toutes vos Sessions de Formation Privées utilisant MOC,
ix. vous ne donnerez accès au Cours Microsoft avec Formateur qu'aux Utilisateurs Finaux, et
x. vous ne donnerez accès au Contenu du Formateur qu'aux Formateurs.

d. **Si vous êtes un Utilisateur Final :**
Pour chaque licence que vous achetez, vous êtes autorisé à utiliser le Cours Microsoft avec Formateur exclusivement pour votre formation personnelle. Si le Cours Microsoft avec Formateur est en format numérique, vous pouvez y accéder en ligne à l'aide du code d'accès unique que vous a fourni le prestataire de formation et installer et utiliser une (1) copie du Cours Microsoft avec Formateur sur un maximum de trois (3) Dispositifs Personnels. Vous êtes également autorisé à imprimer une (1) copie du Cours Microsoft avec Formateur. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

e. **Si vous êtes un Formateur :**
i. Pour chaque licence que vous achetez, vous êtes autorisé à installer et utiliser une (1) copie du Contenu du Formateur sous la forme dans laquelle il vous a été fourni sur un (1) Dispositif Personnel exclusivement pour préparer et donner une Session de Formation Agréée ou une Session de Formation Privée, et à installer une (1) copie supplémentaire sur un autre Dispositif Personnel comme copie de sauvegarde, utilisable uniquement pour réinstaller le Contenu du Formateur. Vous n'êtes pas autorisé à installer ou utiliser une copie du Contenu du Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas. Vous êtes également autorisé à imprimer une (1) copie du Contenu du Formateur uniquement pour préparer et assurer une Session de Formation Agréée ou une Session de Formation Privée.
ii. Vous pouvez personnaliser les parties écrites du Contenu du Formateur qui sont logiquement associées à la présentation d'une session de formation conformément à la version la plus récente du contrat MCT. Si vous choisissez d'exercer les droits qui précèdent, vous acceptez de vous conformer à ce qui suit : (i) les personnalisations ne peuvent être utilisées que pour donner des Sessions de Formation Agréées et des Sessions de Formation Privées, et (ii) toutes les personnalisations seront conformes au présent contrat. À des fins de clarté, toute utilisation de « *personnaliser* » ne fait référence qu'à la modification de l'ordre des diapositives et du contenu, et/ou à la non-utilisation de l'ensemble du contenu ou des diapositives, et ne signifie pas le changement ou la modification d'aucune diapositive ni d'aucun contenu.

2.2 **Dissociation de composants.** Le Contenu Concédé sous Licence est concédé sous licence en tant qu'unité unique et vous n'êtes pas autorisé à dissocier les composants ni à les installer sur différents dispositifs.

2.3 **Redistribution du Contenu Concédé sous Licence.** Sauf stipulation contraire expresse dans les droits d'utilisation ci-dessus, vous n'êtes pas autorisé à distribuer le Contenu Concédé sous Licence ni aucune partie de celui-ci (y compris les éventuelles modifications autorisées) à des tiers sans l'autorisation expresse et écrite de Microsoft.

2.4 **Programmes et Services Tiers.** Le Contenu Concédé sous Licence peut contenir des programmes ou services tiers. Les présents termes du contrat de licence s'appliqueront à votre utilisation de ces programmes ou services tiers, excepté si d'autres termes accompagnent ces programmes et services.

2.5 **Conditions supplémentaires.** Le Contenu Concédé sous Licence est susceptible de contenir des composants auxquels s'appliquent des termes, conditions et licences supplémentaires en termes d'utilisation. Les termes non contradictoires desdites conditions et licences s'appliquent également à votre utilisation du composant correspondant et complètent les termes décrits dans le présent contrat.

3. CONTENU CONCÉDÉ SOUS LICENCE BASÉ SUR UNE TECHNOLOGIE PRÉCOMMERCIALE. Si l'objet du Contenu Concédé sous Licence est basé sur une version précommerciale d'une technologie Microsoft (« **version précommerciale** »), les présents termes s'appliquent en plus des termes de ce contrat :

a. **Contenu sous licence en version précommerciale**. L'objet du présent Contenu Concédé sous Licence est basé sur la version précommerciale de la technologie Microsoft. La technologie peut ne pas fonctionner comme une version finale de la technologie et nous sommes susceptibles de modifier cette technologie pour la version finale. Nous sommes également autorisés à ne pas éditer de version finale. Le Contenu Concédé sous Licence basé sur la version finale de la technologie est susceptible de ne pas contenir les mêmes informations que le Contenu Concédé sous Licence basé sur la version précommerciale. Microsoft n'a aucune obligation de vous fournir quelque autre contenu, y compris du Contenu Concédé sous Licence basé sur la version finale de la technologie.

b. **Commentaires**. Si vous acceptez de faire part à Microsoft de vos commentaires concernant le Contenu Concédé sous Licence, directement ou par l'intermédiaire de son représentant tiers, vous concédez à Microsoft, gratuitement, le droit d'utiliser, de partager et de commercialiser vos commentaires de quelque manière et à quelque fin que ce soit. Vous concédez également à des tiers, à titre gratuit, tout droit de propriété sur leurs produits, technologies et services, nécessaires pour utiliser ou interfacer des parties spécifiques d'un logiciel, produit ou service Microsoft qui inclut les commentaires. Vous ne donnerez pas d'informations faisant l'objet d'une licence qui impose à Microsoft de concéder sous licence son logiciel, ses technologies ou produits à des tiers parce que nous y incluons vos commentaires. Ces droits survivent au présent contrat.

c. **Durée de la Version Précommerciale**. Si vous êtes un Membre du Programme Microsoft IT Academy, un Membre Microsoft Learning Competency, un Membre MPN ou un Formateur, vous cesserez d'utiliser toutes les copies du Contenu Concédé sous Licence basé sur la technologie précommerciale (i) à la date que Microsoft vous indique comme date de fin d'utilisation du Contenu Concédé sous Licence basé sur la technologie précommerciale, ou (ii) soixante (60) jours après la mise sur le marché de la technologie qui fait l'objet du Contenu Concédé sous Licence, selon la date la plus proche (« **Durée de la Version Précommerciale** »). Dès l'expiration ou la résiliation de la durée de la version précommerciale, vous supprimerez définitivement et détruirez toutes les copies du Contenu Concédé sous Licence en votre possession ou sous votre contrôle.

4. **CHAMP D'APPLICATION DE LA LICENCE.** Le Contenu Concédé sous Licence n'est pas vendu. Le présent contrat ne fait que vous conférer certains droits d'utilisation du Contenu Concédé sous Licence. Microsoft se réserve tous les autres droits. Sauf si la réglementation applicable vous confère d'autres droits, nonobstant la présente limitation, vous n'êtes autorisé à utiliser le Contenu Concédé sous Licence qu'en conformité avec les termes du présent contrat. Ce faisant, vous devez vous conformer aux restrictions techniques contenues dans le Contenu Concédé sous Licence qui ne vous permettent de l'utiliser que d'une certaine façon. Sauf stipulation expresse dans le présent contrat, vous n'êtes pas autorisé à :
   - accéder au Contenu Concédé sous Licence ou à y autoriser l'accès à quiconque qui n'a pas acheté une licence valide du Contenu Concédé sous Licence,
   - modifier, supprimer ou masquer les mentions de droits d'auteur ou autres notifications de protection (y compris les filigranes), marques ou identifications contenue dans le Contenu Concédé sous Licence,
   - modifier ou créer une œuvre dérivée d'un Contenu Concédé sous Licence,
   - présenter en public ou mettre à disposition de tiers le Contenu Concédé sous Licence à des fins d'accès ou d'utilisation,
   - copier, imprimer, installer, vendre, publier, transmettre, prêter, adapter, réutiliser, lier ou publier, mettre à disposition ou distribuer le Contenu Concédé sous Licence à un tiers,
   - contourner les restrictions techniques contenues dans Contenu Concédé sous Licence, ou
   - reconstituer la logique, décompiler, supprimer ou contrecarrer des protections, ou désassembler le Contenu Concédé sous Licence, sauf dans la mesure où ces opérations seraient expressément permises par les termes du contrat de licence ou la réglementation applicable nonobstant la présente limitation.

5. **DROITS RÉSERVÉS ET PROPRIÉTÉ.** Microsoft se réserve tous les droits qui ne vous sont pas expressément concédés dans le présent contrat. Le Contenu Concédé sous Licence est protégé par les lois et les traités internationaux en matière de droits d'auteur et de propriété intellectuelle. Les droits de propriété, droits d'auteur et autres droits de propriété intellectuelle sur le Contenu Concédé sous Licence appartiennent à Microsoft ou à ses fournisseurs.

6. **RESTRICTIONS À L'EXPORTATION.** Le Contenu Concédé sous Licence est soumis aux lois et réglementations américaines en matière d'exportation. Vous devez vous conformer à toutes les lois et réglementations nationales et internationales en matière d'exportation applicables au Contenu Concédé sous Licence. Ces lois comportent des restrictions sur les utilisateurs finals et les utilisations finales. Des informations supplémentaires sont disponibles sur le site www.microsoft.com/exporting.

7. **SERVICES D'ASSISTANCE TECHNIQUE.** Dans la mesure où le Contenu Concédé sous Licence est fourni « en l'état », nous ne fournissons pas de services d'assistance technique.

8. **RÉSILIATION.** Sans préjudice de tous autres droits, Microsoft pourra résilier le présent contrat si vous n'en respectez pas les conditions générales. Dès la résiliation du présent contrat pour quelque raison que ce soit, vous arrêterez immédiatement toute utilisation et détruirez toutes les copies du Contenu Concédé sous Licence en votre possession ou sous votre contrôle.

9. **LIENS VERS DES SITES TIERS.** Vous êtes autorisé à utiliser le Contenu Concédé sous Licence pour accéder à des sites tiers. Les sites tiers ne sont pas sous le contrôle de Microsoft et Microsoft n'est pas responsable du contenu de ces sites, des liens qu'ils contiennent ni des modifications ou mises à jour qui leur sont apportées. Microsoft n'est pas responsable du Webcasting ou de toute autre forme de transmission reçue d'un site tiers. Microsoft fournit ces liens vers des sites tiers pour votre commodité uniquement et l'insertion de tout lien n'implique pas l'approbation du site en question par Microsoft.

10. **INTÉGRALITÉ DES ACCORDS.** Le présent contrat et les éventuelles conditions supplémentaires pour le Contenu du Formateur, les mises à jour et les suppléments constituent l'intégralité des accords en ce qui concerne le Contenu Concédé sous Licence, les mises à jour et les suppléments.

11. **RÉGLEMENTATION APPLICABLE.**

    a. États-Unis. Si vous avez acquis le Contenu Concédé sous Licence aux États-Unis, les lois de l'État de Washington, États-Unis d'Amérique, régissent l'interprétation de ce contrat et s'appliquent en cas de réclamation ou d'actions en justice pour rupture dudit contrat, sans donner d'effet aux dispositions régissant les conflits de lois. Les lois du pays dans lequel vous vivez régissent toutes les autres réclamations, notamment les réclamations fondées sur les lois fédérales en matière de protection des consommateurs, de concurrence déloyale et de délits.

    b. En dehors des États-Unis. Si vous avez acquis le Contenu Concédé sous Licence dans un autre pays, les lois de ce pays s'appliquent.

12. **EFFET JURIDIQUE.** Le présent contrat décrit certains droits légaux. Vous pouvez bénéficier d'autres droits prévus par les lois de votre État ou pays. Vous pouvez également bénéficier de certains droits à l'égard de la partie auprès de laquelle vous avez acquis le Contenu Concédé sous Licence. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre État ou pays si celles-ci ne le permettent pas.

13. **EXCLUSIONS DE GARANTIE. LE CONTENU CONCÉDÉ SOUS LICENCE EST FOURNI « EN L'ÉTAT » ET « TEL QUE DISPONIBLE ». VOUS ASSUMEZ TOUS LES RISQUES LIÉS À SON UTILISATION. MICROSOFT ET SES AFFILIÉS RESPECTIFS N'ACCORDENT AUCUNE GARANTIE OU CONDITION EXPRESSE. VOUS POUVEZ BÉNÉFICIER DE DROITS SUPPLÉMENTAIRES RELATIFS AUX CONSOMMATEURS EN VERTU DU DROIT DE VOTRE PAYS, QUE CE CONTRAT NE PEUT MODIFIER. LORSQUE CELA EST AUTORISÉ PAR LE DROIT LOCAL, MICROSOFT ET SES AFFILIÉS RESPECTIFS EXCLUENT TOUTES GARANTIES IMPLICITES DE QUALITÉ, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE VIOLATION.**

14. **LIMITATION ET EXCLUSION DE RECOURS ET DE DOMMAGES. VOUS POUVEZ OBTENIR DE MICROSOFT, DE SES AFFILIÉS RESPECTIFS ET DE SES FOURNISSEURS UNE INDEMNISATION EN CAS DE DOMMAGES DIRECTS LIMITÉE À U.S. $5.00. VOUS NE POUVEZ PRÉTENDRE À AUCUNE INDEMNISATION POUR LES AUTRES DOMMAGES, Y COMPRIS LES DOMMAGES SPÉCIAUX, INDIRECTS, INCIDENTS OU ACCESSOIRES ET LES PERTES DE BÉNÉFICES.**

    Cette limitation concerne :
    - toute affaire liée au Contenu Concédé sous Licence, au logiciel, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
    - les réclamations pour rupture de contrat ou violation de garantie, les réclamations en cas de responsabilité sans faute, de négligence ou autre délit dans la limite autorisée par la loi en vigueur.

    Elle s'applique également même si Microsoft connaissait l'éventualité d'un tel dommage. La limitation ou l'exclusion ci-dessus peut également ne pas vous être applicable si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages incidents, indirects ou de quelque nature que ce soit.

Dernière mise à jour : septembre 2012.

Bienvenue !

Merci de suivre notre formation. En collaboration avec nos sites Microsoft Certified Partners for Learning Solutions et nos centres Microsoft IT Academy, nous avons élaboré des formations de premier plan aussi bien destinées aux informaticiens souhaitant approfondir leurs connaissances qu'aux étudiants se destinant à une carrière informatique.

- **Formateurs et instructeurs Microsoft Certified**—Votre instructeur possède des compétences techniques et pédagogiques. Il répond aux exigences actuelles en matière de certification. En outre, si les instructeurs dispensent des formations sur l'un de nos sites Certified Partners for Learning Solutions, ils sont également évalués tout au long de l'année par les stagiaires et par Microsoft.
- **Avantages des examens de certification**—À l'issue d'une formation, pensez aux examens de certification Microsoft. Les certifications Microsoft valident vos compétences en matière de technologies Microsoft et peuvent faire la différence lors d'une recherche d'emploi ou pour faire progresser votre carrière. Une étude IDC indépendante a conclu que pour 75 % des responsables, les certifications sont importantes pour les performances des équipes1. Renseignez-vous auprès de votre instructeur pour connaître les promotions et remises auxquels vous pourriez avoir droit sur les examens de certification Microsoft.
- **Garantie de satisfaction du client**—Nos Certified Partners for Learning Solutions offrent une garantie de satisfaction et engagent leur responsabilité à ce sujet. À la fin du cours, nous vous demandons de bien vouloir remplir un formulaire d'évaluation sur votre expérience du jour. Vos commentaires sont les bienvenus !

Nous vous souhaitons une agréable formation et une carrière couronnée de succès.

Cordialement,

Microsoft Learning
www.microsoft.com/france/formation

Microsoft | Learning

[1] *IDC*, Value of Certification: Team Certification and Organizational Performance, *novembre 2006*

Remerciements

Formation Microsoft souhaite reconnaître la contribution apportée par les personnes citées ci-dessous à l'élaboration de ce titre et les en remercier. Elles ont en effet déployé des efforts aux différents stades de ce processus pour vous proposer une expérience de qualité en classe.

Stan Reimer – Développeur de contenu

Stan Reimer est président de S. R. Technical Services Inc. et travaille comme consultant, instructeur et auteur. Stan possède une solide expérience de consultant sur les déploiements des services de domaine Active Directory® et Microsoft® Exchange Server car il a travaillé en ce sens avec certaines des plus grandes entreprises du Canada. Stan est le principal auteur de deux ouvrages Active Directory pour Microsoft Press®. Au cours des neuf dernières années, Stan a écrit des cours pour la Formation Microsoft, en se spécialisant dans les cours Active Directory et Exchange Server. Stan est instructeur certifié par Microsoft (MCT) depuis plus de 12 ans.

Damir Dizdarevic – Expert technique/Développeur de contenu

Damir Dizdarevic est MCT (Microsoft Certified Trainer), MCSE (Microsoft Certified Solutions Expert), MCTS (Microsoft Certified Technology Specialist) et MCITP (Microsoft Certified IT Professional). Il est l'un des responsables et instructeurs du centre de formation de Logosoft d.o.o. (Sarajevo, Bosnie-Herzégovine). Damir a plus de 17 années d'expérience en matière de plateformes Microsoft et il est spécialiste de Windows Server®, Exchange Server, de la sécurité et de la virtualisation. Il a travaillé en tant qu'expert technique et réviseur technique sur de nombreux cours MOC (Microsoft Official Courses) et a publié plus de 400 articles dans différents magazines informatiques tels que *Windows ITPro* et *INFO Magazine*. Il intervient aussi fréquemment et avec brio dans la plupart des conférences Microsoft en Europe de l'Est. En outre, Damir est membre du programme Microsoft MVP (Most Valuable Professional) pour la gestion de l'infrastructure Windows Server.

Orin Thomas – Développeur de contenu

Orin Thomas possède les certifications MVP, MCT, ainsi qu'un grand nombre de certifications MCSE et MCITP. Il a écrit plus de 20 manuels pour Microsoft Press et il est conseiller de rédaction pour le magazine *Windows IT Pro*. Orin travaille dans l'informatique depuis le début des années 1990. Il intervient régulièrement lors d'événements tels que TechED en Australie, et dans le monde entier, sur Windows Server, sur les systèmes d'exploitation clients Windows®, sur Microsoft System Center, et sur des sujets relatifs à la sécurité. Orin a fondé et dirige le Melbourne System Center Users Group.

Vladimir Meloski – Développeur de contenu

Vladimir Meloski est MCT, MVP sur Exchange Server, et un consultant qui fournit des solutions de communications et d'infrastructure unifiées basées sur Exchange Server, Microsoft Lync® Server et System Center. Vladimir a 16 ans d'expérience professionnelle en informatique et a participé à des conférences Microsoft en Europe et aux États-Unis en tant que présentateur, modérateur, surveillant d'ateliers pratiques et expert technique. Il a également travaillé en tant qu'expert technique et réviseur technique pour plusieurs cours MOC.

Nick Portlock – Auteur

Nick Portlock est MCT depuis 15 ans. Il est instructeur informatique indépendant, consultant et auteur. L'année dernière, Nick a enseigné dans plus de 20 pays. Il est spécialiste des services de domaine Active Directory, des stratégies de groupe, de DNS (Domain Name System), et il est intervenu en tant que consultant dans de nombreuses entreprises au cours des dix dernières années. Nick a révisé plus de 100 cours Microsoft et est membre du programme Series Technical Expert Panel (STEP) de Windows® 7.

Gary Dunlop – Expert technique

Gary Dunlop est basé à Winnipeg, au Canada, et est consultant technique et instructeur pour Broadview Networks. Gary a écrit plusieurs titres de la Formation Microsoft et il est MCT depuis 1997.

Ulf B. Simon-Weidner – Réviseur technique

Ulf B. Simon-Weidner est un consultant expérimenté qui travaille avec un fournisseur européen de solutions d'infrastructure en Allemagne. Il est également auteur, consultant, présentateur et instructeur indépendant. Au cours des dix dernières années, Ulf a été désigné MVP (Most Valuable Professional) à plusieurs reprises pour les services d'annuaire de Windows Server. Il est également MCT depuis plus de 10 ans. Durant sa carrière professionnelle, Ulf a été engagé plusieurs fois comme consultant par de grandes entreprises européennes ou internationales. Il a également publié plusieurs livres et articles de magazine portant sur les services de domaine Active Directory, Windows Server, les systèmes d'exploitation clients Windows et la sécurité. Ulf intervient fréquemment dans des conférences telles que Microsoft TechEd en Amérique du Nord et en Europe ou encore la conférence The Experts. Ulf transmet son expérience technique et du terrain dans plusieurs supports pédagogiques Windows Server en tant que réviseur technique.

Sommaire

Module 1 : Implémentation des services réseau avancés

Leçon 1 : Configuration des fonctionnalités DHCP avancées 1-2
Leçon 2 : Configuration des paramètres DNS avancés 1-11
Leçon 3 : Implémentation de la réplication IPAM 1-21
Atelier pratique : Implémentation des services réseau avancés 1-31

Module 2 : Implémentation des services de fichiers avancés

Leçon 1 : Configuration du stockage iSCSI 2-2
Leçon 2 : Configuration de la fonctionnalité BranchCache 2-10
Leçon 3 : Optimisation de l'utilisation du stockage 2-19
Atelier pratique A : Implémentation des services de fichiers avancés 2-26
Atelier pratique B : Implémentation de la fonctionnalité BranchCache 2-33

Module 3 : Implémentation du contrôle d'accès dynamique

Leçon 1 : Vue d'ensemble du contrôle d'accès dynamique 3-2
Leçon 2 : Planification du contrôle d'accès dynamique 3-9
Leçon 3 : Déploiement du contrôle d'accès dynamique 3-15
Atelier pratique : Implémentation du contrôle d'accès dynamique 3-27

Module 4 : Implémentation des déploiements de services de domaine Active Directory distribués

Leçon 1 : Vue d'ensemble des déploiements AD DS distribués 4-2
Leçon 2 :Déploiement d'un environnement AD DS distribué 4-8
Leçon 3 : Configuration d'approbations AD DS 4-18
Atelier pratique : Implémentation des déploiements AD DS distribués. 4-25

Module 5 : Implémentation des sites et de la réplication Active Directory Domain Services (AD DS)

Leçon 1 : Vue d'ensemble de la réplication AD DS 5-2
Leçon 2 : Configuration des sites AD DS 5-12
Leçon 3 : Configuration et contrôle de la réplication AD DS 5-21
Atelier pratique : Implémentation des sites et de la réplication AD DS 5-29

Module 6 : Implémentation des services de certificats Active Directory

Leçon 1 : Présentation de l'infrastructure à clé publique (PKI) **6-2**
Leçon 2 : Déploiement d'autorités de certification **6-13**
Atelier pratique A : Déploiement et configuration de la hiérarchie d'autorités de certification **6-21**
Leçon 3 : Déploiement et gestion des modèles de certificats **6-25**
Leçon 4 : Implémentation de la distribution et de la révocation de certificats **6-31**
Leçon 5 : Gestion de la récupération de certificats **6-42**
Atelier pratique B : Déploiement et gestion de certificats **6-47**

Module 7 : Implémentation des services AD RMS (Active Directory Rights Management Services)

Leçon 1 : Vue d'ensemble d'AD RMS **7-2**
Leçon 2 : Déploiement et gestion d'une infrastructure d'AD RMS **7-8**
Leçon 3 : Configuration de la protection du contenu AD RMS **7-15**
Leçon 4: Configuration d'un accès externe à AD RMS **7-22**
Atelier pratique : Implémentation AD RMS **7-27**

Module 8 : Implémentation des services AD FS (Active Directory Federation Services)

Leçon 1 : Vue d'ensemble d'AD FS **8-2**
Leçon 2 : Déploiement d'AD FS **8-14**
Leçon 3 : Implémentation d'AD FS pour une seule organisation **8-22**
Leçon 4 : Déploiement d'AD FS dans un scénario de fédération B2B **8-29**
Atelier pratique : Implémentation des services AD FS (Active Directory Federation Services) **8-36**

Module 9 : Implémentation de l'équilibrage de la charge réseau

Leçon 1 : Vue d'ensemble de NLB **9-2**
Leçon 2 : Configuration d'un cluster NLB **9-6**
Leçon 3 : Planification d'une implémentation NLB **9-13**
Atelier pratique : Implémentation de l'équilibrage de la charge réseau **9-19**

Module 10 : Implémentation du clustering avec basculement

Leçon 1 : Vue d'ensemble du clustering avec basculement **10-2**
Leçon 2 : Implémentation d'un cluster de basculement **10-16**
Leçon 3 : Configuration d'applications et de services hautement disponibles sur un cluster de basculement **10-23**
Leçon 4 : Maintenance d'un cluster de basculement **10-29**
Leçon 5 : Implémentation d'un cluster de basculement multisite **10-36**
Atelier pratique : Implémentation du clustering avec basculement **10-42**

Module 11 : Implémentation du clustering avec basculement à l'aide d'Hyper-V

Leçon 1 : Vue d'ensemble de l'intégration d'Hyper-V au clustering avec basculement **11-2**
Leçon 2 : Implémentation des ordinateurs virtuels d'Hyper-V sur des clusters de basculement **11-9**
Leçon 3 : Implémentation des déplacements d'ordinateurs virtuels Hyper-V **11-19**
Leçon 4 : Gestion des environnements virtuels Hyper-V à l'aide de VMM **11-27**
Atelier pratique : Implémentation du clustering avec basculement à l'aide d'Hyper-V **11-39**

Module 12 : Implémentation de la récupération d'urgence

Leçon 1 : Vue d'ensemble de la récupération d'urgence **12-2**
Leçon 1 : Implémentation de la Sauvegarde Windows Server **12-8**
Leçon 1 : Implémentation de la récupération de données et de serveurs **12-19**
Atelier pratique : Implémentation des fonctionnalités de sauvegarde et de restauration de Windows Server **12-25**

Corrigés des ateliers pratiques

Atelier pratique du module 1 : Implémentation des services réseau avancés **L1-1**
Atelier pratique A du module 2 : Implémentation des services de fichiers avancés **L2-13**
Atelier pratique B du module 2 : Implémentation de la fonctionnalité BranchCache **L2-21**
Atelier pratique du module 3 : Implémentation du contrôle d'accès dynamique **L3-29**
Atelier pratique du module 4 : Implémentation des déploiements AD DS distribués **L4-41**
Atelier pratique du module 5 : Implémentation des sites et de la réplication AD DS **L5-47**
Atelier pratique A du module 6 : Déploiement et configuration de la hiérarchie d'autorités de certification **L6-53**
Atelier pratique B du module 6 : Déploiement et gestion de certificats **L6-60**
Atelier pratique du module 7 : Implémentation AD RMS **L7-71**
Atelier pratique du module 8 : Implémentation des services AD FS (Active Directory Federation Services) **L8-83**
Atelier pratique du module 9 : Implémentation de l'équilibrage de la charge réseau **L9-97**

Atelier pratique du module 10 : Implémentation du clustering avec basculement **L10-103**
Atelier pratique du module 11 : Implémentation du clustering avec basculement à l'aide d'Hyper-V **L11-113**
Atelier pratique du module 12 : Implémentation des fonctionnalités de sauvegarde et de restauration de Windows Server **L12-97**

À propos de ce cours

Cette section décrit brièvement le cours et ses objectifs, le public visé, ainsi que les connaissances préalables requises.

Description du cours

Ce cours vous fournira les connaissances et les compétences nécessaires pour mettre en service des services avancés dans un environnement d'entreprise Windows Server® 2012. Ce cours vous expliquera comment configurer et gérer les fonctionnalités de haute disponibilité, les solutions de fichiers et de stockage, ainsi que les services réseau dans Windows Server 2012. Vous apprendrez également comment configurer l'infrastructure AD DS (Active Directory® Domain Services) et implémenter les sauvegardes et la récupération d'urgence.

Audience

Ce cours s'adresse aux professionnels de l'informatique possédant une expérience pratique et concrète de l'implémentation, de la gestion et de la maintenance d'une infrastructure Windows Server 2012 dans un environnement d'entreprise existant, et souhaitant acquérir les qualifications et les connaissances nécessaires pour effectuer la gestion et l'approvisionnement de services avancés dans cet environnement Windows Server 2012.

Ce cours peut s'adresser en second lieu à des candidats qui souhaitent obtenir la certification MCSA (Microsoft Certified Systems Administrator) en tant que telle, ou poursuivre leur formation afin d'acquérir la certification MCSE (Microsoft Certified System Engineer), pour laquelle ce cours est une condition préalable. Les professionnels de l'informatique souhaitant acquérir la certification relative à l'examen 70-412 : Configuration des services avancés de Windows Server® 2012, peuvent également suivre ce cours.

Connaissances préalables des stagiaires

Pour suivre ce cours, vous devez disposer de connaissances pratiques dans les domaines suivants :

- Au moins deux ans d'expérience professionnelle pratique dans un environnement Windows Server 2008 ou Windows Server 2012.
- Des connaissances équivalentes au cours *22410 : Installation et configuration de Windows Server® 2012* :
    - installation et configuration de Windows Server 2012 dans les environnements d'entreprise existants ou en tant qu'installations autonomes ;
    - configuration du stockage local ;
    - configuration des rôles et fonctionnalités ;
    - configuration des services de fichiers et d'impression ;
    - configuration des serveurs Windows Server 2012 pour l'administration locale et distante ;
    - configuration des adresses IPv4 et IPv6 ;
    - configuration des services DNS (Domain Name System) et DHCP (Dynamic Host Configuration Protocol) ;
    - installation de contrôleurs de domaine ;
    - création et configuration d'utilisateurs, groupes, ordinateurs et unités d'organisation ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- création et gestion de stratégies de groupes ;
- configuration de stratégies de sécurité locales ;
- configuration du Pare-feu Windows
- configuration de Windows Server 2012 Hyper-V®.

- Des connaissances équivalentes au cours *22411 : Administration de Windows Server® 2012* :
  - déploiement et gestion d'images Windows Server ;
  - installation et configuration des services WSUS ;
  - analyse de l'environnement Windows Server 2012 ;
  - installation et configuration du système de fichiers DFS ;
  - installation et configuration du Gestionnaire de ressources du serveur de fichiers (FSRM) ;
  - configuration de l'accès aux disques et aux fichiers, et des stratégies d'audit ;
  - configuration de la sécurité et de l'intégration de DNS à AD DS ;
  - maintenance de l'intégrité réseau par la configuration de l'accès réseau à l'aide du serveur de stratégie réseau (NPS) et de la protection d'accès réseau (NAP) ;
  - configuration de l'accès à distance à l'aide des réseaux privés virtuels (VPN) et de DirectAccess ;
  - configuration des contrôleurs de domaine ;
  - gestion et maintenance de l'environnement AD DS ;
  - gestion et maintenance de l'environnement de domaine Windows Server 2012 à l'aide de la stratégie de groupe.

Objectifs du cours

À la fin de ce cours, les stagiaires seront à même d'effectuer les tâches suivantes :

- configurer les fonctionnalités avancées pour les services DHCP et DNS, et configurer la gestion des adresses IP (IPAM) ;
- configurer les services de fichiers pour répondre à des exigences professionnelles avancées ;
- configurer le contrôle d'accès dynamique pour gérer et auditer l'accès aux fichiers partagés ;
- fournir la haute disponibilité et l'équilibrage de charge aux applications Web en implémentant l'équilibrage de la charge réseau (NLB) ;
- fournir la haute disponibilité aux applications et services réseau en implémentant le clustering avec basculement ;
- déployer et gérer des ordinateurs virtuels Hyper-V dans un cluster de basculement ;
- implémenter une solution de sauvegarde et de récupération d'urgence en fonction des exigences professionnelles et techniques de l'entreprise ;
- planifier et implémenter un déploiement AD DS incluant plusieurs domaines et forêts ;
- planifier et implémenter un déploiement AD DS incluant plusieurs emplacements ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- implémenter un déploiement AD CS (Active Directory Certificate Services) ;
- implémenter un déploiement AD RMS (Active Directory Rights Management Services) ;
- implémenter un déploiement AD FS (Active Directory Federation Services).

Plan du cours

Le plan du cours est le suivant :

Le **module 1**, « Implémentation des services réseau avancés », décrit comment configurer les fonctionnalités DHCP et paramètres DNS avancés, et comment implémenter IPAM, qui est une nouvelle fonctionnalité de Windows Server 2012.

Le **module 2**, « Implémentation des services de fichiers avancés », décrit comment configurer le stockage iSCSI (Internet Small Computer System Interface) et la fonctionnalité Windows BranchCache®. Le module décrit également comment implémenter les fonctionnalités de Windows Server 2012 qui optimisent l'utilisation du stockage.

Le **module 3**, « Implémentation du contrôle d'accès dynamique », décrit le contrôle d'accès dynamique, qui est une nouvelle fonctionnalité de Windows Server 2012. Il explique également comment planifier et configurer une implémentation du contrôle d'accès dynamique.

Le **module 4**, « Implémentation de déploiements AD DS distribués », fournit une vue d'ensemble des déploiements AD DS distribués et du processus permettant de les implémenter. Il décrit également comment configurer des approbations AD DS et comment implémenter des déploiements AD DS complexes.

Le **module 5**, « Mise en œuvre des sites Active Directory Domain Services (AD DS) et de la réplication » décrit le fonctionnement de la réplication dans AD DS dans un environnement Windows Server 2012 et comment configurer des sites AD DS pour optimiser le trafic réseau AD DS. Il explique également comment configurer et analyser la réplication AD DS.

Le **module 6**, « Implémentation des services de certificats Active Directory », fournit une vue d'ensemble de l'infrastructure à clé publique (PKI) et décrit comment déployer des autorités de certification (CA) et des modèles de certificats. Ce module couvre également la distribution et la révocation de certificats, ainsi que la gestion de la récupération de certificats.

Le **module 7**, « Implémentation des services AD RMS (Active Directory Rights Management Services) » décrit les services AD RMS et la façon dont vous pouvez les utiliser pour protéger du contenu. Il explique également comment déployer et gérer une infrastructure AD RMS et comment configurer la protection du contenu AD RMS, ainsi que l'accès externe à AD RMS.

Le **module 8**, « Implémentation des services AD FS (Active Directory Federation Services) » décrit les scénarios d'entreprise de fédération d'identités et la façon dont vous pouvez utiliser AD FS pour y faire face. Il décrit également comment déployer AD FS et comment implémenter ces services pour une organisation unique ou encore dans un scénario interentreprise (B2B).

Le **module 9**, « Implémentation de l'équilibrage de la charge réseau » décrit les fonctionnalités et le fonctionnement de NLB. Il explique également comment configurer un cluster NLB et planifier une implémentation NLB.

Le **module 10**, « Implémentation du clustering avec basculement » décrit les fonctionnalités de clustering avec basculement dans Windows Server 2012. Il explique également comment implémenter et assurer la maintenance de clusters de basculement et comment configurer des applications et services hautement disponibles sur un cluster de basculement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le **module 11**, « Implémentation du clustering avec basculement avec Hyper-V » décrit des options permettant de rendre des ordinateurs virtuels hautement disponibles. Le module décrit également l'implémentation d'ordinateurs virtuels Hyper-V sur des clusters de basculement, ainsi que le déplacement d'ordinateurs virtuels Hyper-V.

Le **module 12**, « Implémentation de la récupération d'urgence » décrit la récupération d'urgence, la récupération de données et la récupération de serveurs, ainsi que la planification et l'implémentation d'une solution de sauvegarde pour Windows Server 2012.

Mappage d'examen/de cours

Ce cours, *22412B : Configuration des services avancés de Windows Server® 2012*, mappe directement son contenu aux objectifs de l'examen Microsoft *70-412 : Configuration des services avancés de Windows Server® 2012*.

Le tableau ci-dessous est fourni sous la forme d'une aide d'étude pour vous aider à préparer cet examen et vous montrer la manière dont s'imbriquent les objectifs de l'examen et le contenu du cours. Le cours n'est pas conçu exclusivement en vue de l'examen, mais fournit plutôt des connaissances et compétences plus larges pour permettre une implémentation réelle de cette technologie particulière. Le cours contient également du contenu qui n'est pas directement lié à l'examen et qui utilisera l'expérience et les compétences uniques de votre instructeur certifié Microsoft.

Remarque Les objectifs de l'examen sont disponibles en ligne à l'adresse suivante : http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-412&locale=en-us#tab2 (*Certains de ces sites adressées dans ce cours sont en anglais.*)

Examen 70-412 : Configuration des services avancés de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer et gérer la haute disponibilité (16 %)		**Module**	**Leçon**	**Atelier pratique**
Configurer l'équilibrage de la charge réseau (NLB)	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer des nœuds NLB, procéder à la configuration requise pour NLB, configurer l'affinité, configurer les règles de port, configurer le mode d'opération du cluster, mettre à niveau un cluster NLB	Mod 9	Leçons 1/2/3	Mod 9 Ex 1/2/3
Configurer le clustering avec basculement	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer le quorum, configurer la mise en réseau de cluster, restaurer la configuration du cluster ou nœud unique, configurer le stockage en cluster, implémenter la mise à jour adaptée aux clusters, mettre à niveau un cluster	Mod 10	Leçons 1/2/3/4/5	Mod 10 Ex 1/2/3/4

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Examen 70-412 : Configuration des services avancés de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer et gérer la haute disponibilité (16 %)				
Gérer les rôles de clustering avec basculement	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les paramètres spécifiques aux rôles, notamment les partages disponibles en continu, configurer l'analyse des ordinateurs virtuels, configurer les paramètres de basculement et de préférence	Mod 10	Leçons 1/2/3/4/5	Mod 10 Ex 1/2/3/4
Gérer le déplacement d'ordinateurs virtuels	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : procéder à la migration dynamique, effectuer la migration rapide, procéder à la migration du stockage, importer, exporter et copier des ordinateurs virtuels, effectuer une migration à partir d'autres plateformes (P2V et V2V)	Mod 11	Leçons 1/2/3/4	Mod 11 Ex 1/2/3
Configurer des solutions de stockage et de fichiers (15 %)				
Configurer les services de fichiers avancés	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer le magasin de données NFS, configurer BranchCache, configurer l'infrastructure de classification des fichiers (FCI) à l'aide du Gestionnaire de ressources du serveur de fichiers (FSRM), configurer l'audit d'accès aux fichiers	Mod 2	Leçons 2/3	Mod 2 Atelier A Ex 2 et Atelier B Ex 1/2/3/4
Implémenter le contrôle d'accès dynamique	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les types de revendication d'utilisateur et de périphérique, implémenter la mise en attente et les changements de stratégie, procéder aux actions correctives en cas d'accès refusé, configurer la classification des fichiers	Mod 3	Leçons 1/2/3	Mod 3 Ex 1/2/3/4/ 5/6
Configurer et optimiser le stockage	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer l'initiateur et la cible iSCSI, configurer le serveur iSNS (Internet Storage Name Server), implémenter l'allocation dynamique et le stockage optimisé, gérer l'espace libre sur le serveur à l'aide des fonctionnalités à la demande	Mod 2	Leçons 1/3	Mod 2 Atelier A Ex 1

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Examen 70-412 : Configuration des services avancés de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Implémenter la continuité des activités et la récupération d'urgence (18 %)				
Configurer et gérer les sauvegardes	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les sauvegardes de Windows Server, configurer les sauvegardes en ligne de Windows, configurer les sauvegardes spécifiques aux rôles, gérer les paramètres VSS à l'aide de VSSAdmin, créer les instantanés de restauration de système	Mod 12	Leçons 1/2/3	Mod 12 Ex 1/2/3
Récupérer les serveurs	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : procéder à la restauration à partir de sauvegardes, procéder à une récupération complète, procéder à une récupération de serveurs à l'aide de l'environnement de récupération Windows et du mode sans échec, appliquer les instantanés de restauration du système, configurer le magasin de données de configuration du démarrage	Mod 12	Leçons 1/2/3	Mod 12 Ex 2/3
Configurer la tolérance de pannes de niveau site	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer le réplica Hyper-V incluant le service Broker de réplication Hyper-V et les ordinateurs virtuels, configurer le clustering multisite incluant les paramètres réseau, le quorum et les paramètres de basculement	Mod 10	Leçons 1/5	
		Mod 11	Leçons 1/3	Mod 11 Ex 1
Configurer les services réseau (17 %)				
Implémenter une solution DHCP (Dynamic Host Configuration Protocol) avancée	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : créer et configurer des étendues globales et des étendues de multidiffusion, implémenter DHCPv6, configurer la haute disponibilité pour DHCP, y compris le basculement DHCP et les étendues fractionnées, configurer la protection des noms DHCP	Mod 1	Leçon 1	Mod 1 Ex 1

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Examen 70-412 : Configuration des services avancés de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer les services réseau (17 %)				
Implémenter une solution DNS avancée	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer la sécurité pour DNS, y compris DNSSEC, le pool de sockets DNS et le verrouillage de cache, configurer la journalisation DNS, configurer l'administration déléguée, configurer la récursivité, configurer le tri de masques réseau, configurer une zone GlobalNames	Mod 1	Leçon 2	Mod 1 Ex 2
Déployer et gérer la fonctionnalité IPAM	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer la fonctionnalité IPAM manuellement ou à l'aide de la stratégie de groupe, configurer la découverte de serveurs, créer et gérer des blocs et des plages IP, analyser l'utilisation de l'espace des adresses IP, migrer vers IPAM, déléguer l'administration d'IPAM, gérer les collections IPAM	Mod 1	Leçon 3	Mod 1 Ex 3
Configurer l'infrastructure Active Directory (18 %)				
Configurer une forêt ou un domaine	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : implémenter des environnements Active Directory multidomaines et à forêts multiples, y compris l'interopérabilité avec des versions précédentes d'Active Directory, mettre à niveau les forêts et domaines existants, y compris la préparation de l'environnement et les niveaux fonctionnels, configurer plusieurs suffixes UPN (User Principal Name)	Mod 4	Leçons 1/2	Mod 4 Ex 1
Configurer des approbations	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer des approbations externes, de forêt, de raccourci et de domaine, configurer l'authentification d'approbations, configurer le filtrage SID, configurer le routage des suffixes de noms	Mod 4	Leçon 3	Mod 4 Ex 1/2

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Examen 70-412 : Configuration des services avancés de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer l'infrastructure Active Directory (18 %)				
Configurer des sites	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer des sites et des sous-réseaux, créer et configurer des liens de sites, gérer la couverture de site, gérer l'inscription des enregistrements SRV, déplacer des contrôleurs de domaine entre des sites	Mod 5	Leçons 2/3	Mod 5 Ex 1/2/3
Gérer Active Directory et la réplication SYSVOL	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer la réplication vers des contrôleurs de domaine en lecture seule, configurer la stratégie de réplication de mots de passe pour des contrôleurs de domaine en lecture seule, analyser et gérer la réplication, mettre à niveau la réplication SYSVOL vers la réplication du système de fichiers DFS	Mod 5	Leçons 1/3	Mod 5 Ex 3
Configurer les solutions d'identités et d'accès (15 %)				
Implémenter les services AD FS (Active Directory Federation Services) 2.1	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : implémenter l'authentification basée sur les revendications, y compris les approbations de partie de confiance, configurer les règles d'approbation de fournisseur de revendications, configurer les magasins d'attributs, y compris AD LDS (Active Directory Lightweight Directory Services), gérer les certificats AD FS, configurer le proxy AD FS, intégrer les services AD FS aux services de cloud computing	Mod 8	Leçons 1/2/3/4	Mod 8 Ex 1/2/3/4
Installer et configurer les services AD CS (Active Directory Certificate Services)	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer une autorité de certification (CA) d'entreprise, configurer des points de distribution de liste de révocation de certificats, installer et configurer le répondeur en ligne, implémenter la séparation des rôles administratifs, configurer la sauvegarde et la récupération d'autorités de certification	Mod 6	Leçons 1/2/4	Mod 6 Atelier A Ex 1/2

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Examen 70-412 : Configuration des services avancés de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer les solutions d'identités et d'accès (15 %)				
Gérer les certificats	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : gérer les modèles de certificats, implémenter et gérer le déploiement de certificats, leur validation et leur révocation, gérer le renouvellement de certificats, gérer l'inscription et le renouvellement de certificats pour des ordinateurs et utilisateurs à l'aide des stratégies de groupe, configurer et gérer l'archivage et la récupération de clés	Mod 6	Leçons 3/4 /5	Mod 6 Atelier B Ex 1/2/3/4
Installer et configurer les services AD RMS (Active Directory Rights Management Services)	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer un serveur AD RMS d'octroi de licences ou de certificats, gérer le point de connexion de service AD RMS, gérer le déploiement du client AD RMS, gérer les domaines d'utilisateurs approuvés, gérer les domaines de publication approuvés, gérer la prise en charge des identités fédérées, gérer les modèles RMS, configurer les stratégies d'exclusion	Mod 7	Leçons 1/2 /3/4	Mod 7 Ex 1/2/3/4

Important : suivre ce cours ne vous préparera pas à passer les examens de certification associés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Suivre ce cours ne garantit pas que vous réussirez automatiquement n'importe quel examen de certification. En plus de suivre ce cours, vous devez également :

- disposer d'une expérience pratique et concrète approfondie en matière d'implémentation, de gestion et de configuration d'une infrastructure Active Directory et de mise en réseau Windows Server 2012 ;
- disposer d'une expérience dans la mise en service d'une infrastructure et de services avancés dans un environnement Windows Server 2012 ;
- suivre des études supplémentaires extérieures au contenu du présent manuel.

Il se peut que des ressources d'étude et de préparation supplémentaires soient également disponibles pour vous permettre de préparer cet examen. Vous trouverez plus de détails à ce sujet à l'aide de l'URL suivante : http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-412&locale=en-us#tab3

Vous devez vous familiariser avec le profil des stagiaires et les connaissances requises pour l'examen afin d'être suffisamment préparé pour cet examen de certification. Le profil complet des stagiaires pour cet examen est disponible à l'adresse URL suivante : http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-412&locale=en-us#tab1

Le tableau de mappage examen/cours présenté ci-dessus est exact au moment de l'impression, toutefois il pourra faire l'objet de modifications à tout moment et la société Microsoft ne pourra pas être tenue pour responsable d'éventuelles incohérences entre la version publiée ici et la version accessible en ligne, et ne donnera aucune notification quant à de telles modifications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Documents de cours

Votre kit de cours contient les documents suivants :

- *Manuel du cours :* guide de formation succinct qui fournit toutes les informations techniques importantes dans un format concis et très ciblé, parfaitement adapté à l'apprentissage en classe.
    - Leçons : vous guident dans les objectifs de formation et fournissent les points clés essentiels pour un apprentissage en classe réussi.
    - Ateliers pratiques : fournissent une plateforme qui vous permettra de mettre en application les connaissances et compétences acquises dans le module.
    - Contrôles des acquis et éléments à retenir : fournissent une documentation de référence pratique qui favorise la mémorisation des connaissances et compétences.
    - Corrigés des ateliers pratiques : fournissent des instructions pas à pas.



Contenu d'accompagnement du cours sur le site *http://www.microsoft.com/learning/companionmoc :* contenu numérique, facile à parcourir, dans lequel il est possible d'effectuer des recherches et qui comprend de précieuses ressources en ligne intégrées, proposées en complément du manuel du cours.

- Modules : incluent l'accompagnement du cours, tel que les questions et les réponses, les étapes détaillées de la démonstration et les liens de la rubrique Documentation supplémentaire, pour chaque leçon. De plus, les modules incluent les questions et réponses de contrôle des acquis de l'atelier pratique, ainsi que des sections sur les contrôles des acquis et éléments à retenir, qui contiennent les questions et réponses de contrôle des acquis, les méthodes conseillées, des astuces et réponses sur les problèmes courants et la résolution des problèmes, des scénarios et problèmes concrets avec les réponses.
- Ressources : incluent des ressources supplémentaires présentées par catégories qui vous donnent un accès immédiat à du contenu utile et à jour disponible sur TechNet, MSDN®, ou Microsoft®, Press®,



Fichiers de cours destinés aux stagiaires à l'adresse *http://www.microsoft.com/learning/companionmoc* : incluent le fichier exécutable à extraction automatique Allfiles.exe, qui contient les fichiers requis pour les ateliers pratiques et les démonstrations.

- Évaluation du cours : À la fin du cours, vous aurez l'occasion de remplir une fiche d'évaluation en ligne pour faire part de vos commentaires sur le cours, le centre de formation et l'instructeur.
    - Pour adresser d'autres commentaires ou remarques sur le cours, envoyez un message électronique à l'adresse support@mscourseware.com. Pour obtenir des informations sur le programme MCP (Microsoft Certification Program), envoyez un message électronique à l'adresse mcphelp@microsoft.com.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Environnement des ordinateurs virtuels

Cette section fournit les informations nécessaires pour configurer l'environnement de la classe afin de prendre en charge le scénario d'entreprise du cours.

Configuration des ordinateurs virtuels

Dans ce cours, vous allez utiliser Microsoft Hyper-V pour effectuer les ateliers pratiques.

Important : à la fin de chaque atelier pratique, vous devez fermer l'ordinateur virtuel sans enregistrer les modifications. Pour fermer un ordinateur virtuel sans enregistrer les modifications, procédez comme suit :

1. Sur l'ordinateur virtuel, dans le menu **Action**, cliquez sur **Fermer**.
2. Dans la boîte de dialogue **Fermer**, dans la liste **Que doit faire l'ordinateur virtuel ?**, cliquez sur **Éteindre** et supprimer les modifications, puis cliquez sur **OK**.

Le tableau suivant montre le rôle de chaque ordinateur virtuel utilisé dans ce cours :

Ordinateur virtuel	Rôle
22412B-LON-DC1/-B	Windows Server 2012 Contrôleur de domaine dans le domaine Adatum.com
22412B-LON-CA1	Windows Server 2012 Serveur autonome
22412B-LON-CL1	Ordinateur client Windows 8 Membre du domaine Adatum.com
22412B-LON-CL2	Ordinateur client Windows 8 Membre du domaine Adatum.com
22412B-LON-CORE	Windows Server 2012 Serveur membre dans le domaine Adatum.com
22412B-LON-SVR1/-B	Windows Server 2012 Serveur membre dans le domaine Adatum.com
22412B-LON-SVR2	Windows Server 2012 Serveur membre dans le domaine Adatum.com
22412B-LON-SVR3	Windows Server 2012 Serveur membre dans le domaine Adatum.com
22412B-LON-SVR4	Windows Server 2012 Serveur membre dans le domaine Adatum.com
22412B-MUN-CL1	Ordinateur client Windows 8 Membre du domaine Treyresearch.net
22412B-MUN-DC1	Windows Server 2012 Contrôleur du domaine TreyResearch.net

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Ordinateur virtuel	Rôle
22412B-LON-HOST1	Windows Server 2012 Serveur membre dans le domaine Adatum.com
22412B-LON-HOST2	Windows Server 2012 Serveur membre dans le domaine Adatum.com
22412B-TOR-DC1	Windows Server 2012 Serveur membre dans le domaine Adatum.com
MSL-TMG1	Ordinateur virtuel Microsoft Forefront® Threat Management Gateway (TMG)

Configuration logicielle

Les logiciels suivants sont installés sur chaque ordinateur virtuel :

- Windows Server 2012 Datacenter Edition
- Windows 8
- Office 2010, Service Pack 1 (SP1)

Configuration de la classe

L'ordinateur virtuel sera configuré de la même façon sur tous les ordinateurs de la classe.

Niveau des éléments matériels du cours

Pour garantir une utilisation satisfaisante, les formations Microsoft requièrent une configuration matérielle minimale pour les ordinateurs de l'instructeur et des stagiaires dans toutes les classes Microsoft CPLS (Certified Partner for Learning Solutions) dans lesquelles les produits officiels de formation Microsoft sont utilisés.

- Processeur Intel VT (Intel Virtualization Technology) ou AMD-V (AMD Virtualization)
- Deux disques durs SATA (Serial ATA) de 120 Go à 7 200 tr/mn ou supérieurs*
- 8 Go de mémoire vive (RAM)
- Lecteur de DVD
- Carte réseau
- Moniteur Super VGA (SVGA) de 17 pouces
- Souris Microsoft ou dispositif de pointage compatible
- Carte son avec haut-parleurs

*Agrégés par bandes

En outre, l'ordinateur de l'instructeur doit être connecté à un projecteur vidéo prenant en charge la carte SVGA 1024 x 768 pixels, couleurs 16 bits.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Navigation dans Windows Server 2012

Si vous n'êtes pas familiarisé avec l'interface utilisateur de Windows Server 2012 ou Windows 8, les informations suivantes vous aideront à vous orienter dans la nouvelle interface.

- Se connecter et Se déconnecter remplacent Connexion et Déconnexion.
- Les outils d'administration sont accessibles à partir du menu Outils du Gestionnaire de serveur.
- Déplacez la souris dans l'angle inférieur droit du bureau pour ouvrir un menu comportant :
  - Paramètres : comprend le Panneau de configuration et Alimentation
  - Menu Démarrer : permet d'accéder à des applications
  - Rechercher : permet de rechercher des applications, des paramètres et des fichiers

Les touches de raccourci suivantes vous seront peut-être également utiles :

- Windows : ouvre le menu Démarrer
- Windows+C : ouvre le même menu que le déplacement de la souris dans l'angle inférieur droit
- Windows+I : ouvre Paramètres
- Windows+R : ouvre la fenêtre Exécuter

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1

Implémentation des services réseau avancés

Table des matières :

Vue d'ensemble du module **1-1**

Leçon 1 : Configuration des fonctionnalités DHCP avancées **1-2**

Leçon 2 : Configuration des paramètres DNS avancés **1-12**

Leçon 3 : Implémentation de la réplication IPAM **1-24**

Atelier pratique : Implémentation des services réseau avancés **1-35**

Contrôle des acquis et éléments à retenir **1-43**

Vue d'ensemble du module

Dans Windows Server® 2012, les services réseau tels que Domain Name System (DNS) assurent la prise en charge cruciale de la résolution de noms des ressources réseau et Internet. Dans DNS, Extensions de sécurité DNS (DNSSEC) est une fonctionnalité avancée qui fournit des moyens de sécuriser les réponses de DNS aux requêtes clientes de sorte que les utilisateurs malveillants ne puissent pas les falsifier. Avec le protocole DHCP, vous pouvez gérer et distribuer des adresses IP aux ordinateurs clients. DHCP est essentiel pour gérer des réseaux IP. Le basculement DHCP est une fonctionnalité avancée qui peut empêcher les clients de perdre l'accès au réseau en cas de défaillance du serveur DHCP. La gestion des adresses IP (IPAM) fournit un moyen unifié de contrôler l'adressage IP.

Ce module présente les améliorations de DNS et DHCP, la gestion des adresses IP, et explique comment implémenter ces fonctionnalités.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- configurer les fonctionnalités DHCP avancées ;
- configurer les paramètres DNS avancés ;
- Implémentez la protection IPAM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Configuration des fonctionnalités DHCP avancées

Le protocole DHCP joue un rôle important dans l'infrastructure du système d'exploitation Windows Server® 2012. Il s'agit non seulement du principal moyen employé pour distribuer les informations de configuration réseau importantes aux clients réseau, mais il fournit également certaines informations de configuration à d'autres services réseau, notamment les services de déploiement Windows et la protection d'accès réseau (NAP). Pour prendre en charge une infrastructure de réseau basé sur un serveur Windows, il est important que vous compreniez le rôle de serveur DHCP. Windows Server 2012 améliore les fonctionnalités de DHCP en fournissant des fonctions de basculement.

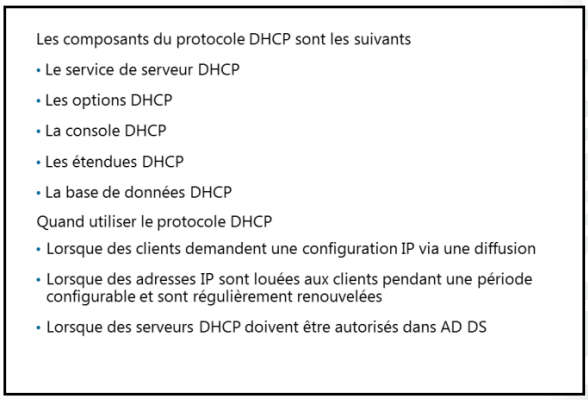
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les composants de DHCP ;
- expliquer comment configurer l'interaction de DHCP avec DNS ;
- expliquer comment configurer des créations avancées d'étendue de DHCP ;
- expliquer le fonctionnement de DHCP avec IPv6 ;
- décrire la protection de nom de DHCP ;
- décrire le basculement DHCP ;
- expliquer comment configurer le basculement DHCP.

Vue d'ensemble des composants DHCP

Le DHCP est un rôle de serveur que vous pouvez installer sur Windows Server 2012. Avec le rôle de serveur DHCP, vous pouvez vérifier que tous les clients ont des adresses IP appropriées et des informations de configuration réseau, qui peuvent aider à éliminer l'erreur humaine pendant la configuration. Un *client DHCP* désigne tout périphérique exécutant le logiciel client DHCP, et qui peut demander et récupérer des paramètres réseau d'un service de serveur DHCP. Les clients DHCP peuvent être des ordinateurs, des appareils mobiles, des imprimantes ou des commutateurs. Le DHCP peut également fournir des informations d'adresse IP aux clients de démarrage réseau.



Lorsque des modifications sont apportées à des informations de configuration réseau clés (telles que l'adresse de la passerelle par défaut), vous pouvez mettre la configuration à jour à l'aide du rôle de serveur DHCP sans avoir à intervenir directement sur chaque ordinateur. De même, DHCP est un service clé pour les utilisateurs itinérants qui changent souvent de réseau. Vous pouvez installer le rôle de serveur DHCP sur un serveur autonome, un serveur de membre du domaine ou un contrôleur de domaine.

Le DHCP comprend les composants qui sont énumérés dans le tableau suivant.

Composant	Description
Service Serveur DHCP	Après l'installation du rôle de DHCP, le serveur DHCP est implémenté en tant que service. Ce service peut distribuer des adresses IP et d'autres informations de configuration réseau aux clients qui les demandent.
Étendues DHCP	L'administrateur DHCP configure la plage des adresses IP et les informations relatives allouées au serveur pour la distribution aux clients en faisant la demande. Chaque étendue peut être associée à un seul sous-réseau IP unique. Une étendue doit se composer des éléments suivants : • un nom et une description ; • une plage d'adresses pouvant être distribuées ; • un masque de sous-réseau. Une étendue peut également définir : • les adresses IP qui devraient être exclues de la distribution ; • la durée du bail d'adresse IP ; • les options DHCP. Vous pouvez configurer un serveur DHCP unique avec plusieurs étendues, mais le serveur doit être connecté directement à chaque sous-réseau qu'il sert, ou avoir un agent relais DHCP en place. Les étendues représentent également pour le serveur le principal moyen de gérer et de distribuer tous les paramètres de configuration relatifs (options DHCP) aux clients sur le réseau.
Options DHCP	Quand vous attribuez l'adresse IP au client, vous pouvez également simultanément attribuer beaucoup d'autres paramètres de configuration réseau. Les options DHCP les plus courantes sont notamment les suivantes : • Adresse IP de passerelle par défaut • Adresse IP du serveur DNS • Suffixe du domaine DNS • Adresse IP du serveur Windows Internet Name Service (WINS) Vous pouvez appliquer les options à différents niveaux. Elles peuvent être appliquées comme suit : • globalement à toutes les étendues ; • spécifiquement à des étendues particulières ; • aux clients spécifiques selon une valeur d'ID de classe ; • aux clients avec des réservations d'adresses IP spécifiques configurées.  **Remarque :** Les étendues d'IPv6 sont légèrement différentes, et seront présentées plus tard dans cette leçon.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Composant	Description
Base de données DHCP	La base de données DHCP contient des données de configuration au sujet du serveur DHCP, et stocke des informations sur les adresses IP qui ont été distribuées. Par défaut, les bases de données DHCP sont enregistrées dans le dossier %systemroot%\System32\Dhcp.
Console DHCP	La console DHCP est l'outil d'administration principal pour gérer tous les aspects du serveur DHCP. Cette console de gestion est installée automatiquement sur tous les serveurs sur lesquels le rôle DHCP est installé. Cependant, vous pouvez également l'installer sur un serveur distant ou un client Windows® 8 à l'aide des outils d'administration de serveur distant (RSAT) et en vous connectant au serveur DHCP pour la gestion à distance.

Comment les clients acquièrent des adresses IP

Lorsque vous configurez un système d'exploitation client Windows pour utiliser le service DHCP, le client utilisera au démarrage un message IP dans son sous-réseau pour demander la configuration IP de n'importe quel serveur DHCP pouvant recevoir la demande. Puisque DHCP utilise des messages IP pour établir des communications, la communication des serveurs DHCP est limitée à leurs sous-réseaux IP. Ceci signifie qu'un serveur DHCP doit être présent sur chaque sous-réseau IP, ou qu'un agent relais DHCP doit être configuré sur le sous-réseau distant. Le service de relais DHCP peut transmettre les paquets de diffusion DHCP en tant que messages dirigés dans d'autres sous-réseaux IP à travers un routeur. L'agent de relais acquiert une configuration d'adresse IP au nom du client qui a effectué la demande sur le sous-réseau distant, puis fait suivre cette configuration au client.

Baux DHCP

DHCP alloue les adresses IP dynamiquement. selon le principe du *bail*. Vous pouvez configurer la durée du bail. La durée du bail par défaut pour les clients câblés est de huit jours.

Lorsque le bail DHCP a atteint 50 % de sa durée totale, le client essaie de le renouveler. Il s'agit d'un processus automatique qui se produit en arrière-plan. Les ordinateurs peuvent avoir la même adresse IP sur une longue période s'ils fonctionnent de façon continue sur un réseau sans être arrêtés. Les ordinateurs clients tentent également de renouveler le bail pendant le processus de démarrage.

Autorisation du serveur DHCP

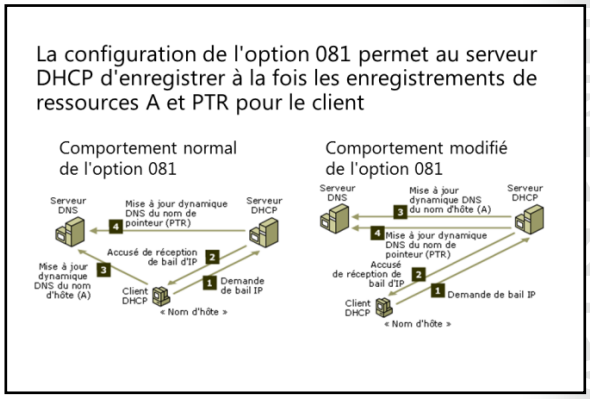
Si le serveur est un membre du domaine, vous devez autoriser le rôle de serveur DHCP de Windows Server 2012 dans Services de domaine Active Directory® (AD DS) avant de pouvoir commencer à louer des adresses IP. Le serveur DHCP doit être autorisé par un compte d'administrateur d'entreprise. Les serveurs autonomes de Microsoft vérifient s'il y a un serveur DHCP sur le réseau, et ne mettent pas sur pied le service DHCP si c'est le cas.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de l'interaction de DHCP avec DNS

Pendant l'allocation d'adresse IP dynamique, le serveur DHCP crée automatiquement des enregistrements de ressources pour des clients DHCP dans la base de données DNS. Cependant, ces enregistrements ne peuvent pas être supprimés automatiquement quand le bail du client DHCP expire. Vous pouvez configurer des options DHCP pour permettre au serveur DHCP de détenir et de contrôler entièrement la création et la suppression de ces enregistrements de ressources DNS.



Configuration de l'option DHCP 081

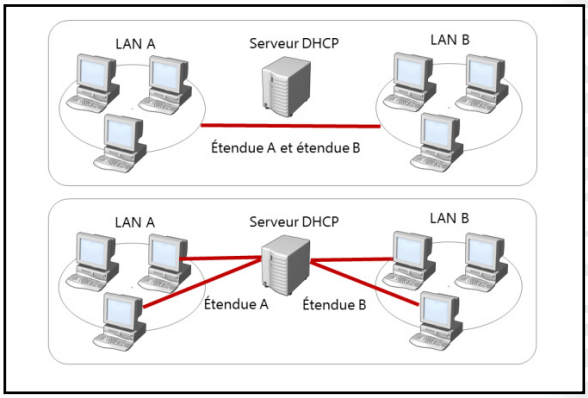
Vous pouvez configurer l'option DHCP 081 pour contrôler la manière dont les enregistrements de ressources sont mis à jour dans la base de données DNS. Cette option permet au client de fournir son nom de domaine complet (FQDN) et ses instructions au serveur DHCP au sujet de la façon dont le serveur doit traiter les mises à jour dynamiques de DNS en son nom. Configurez l'option 081 sur l'onglet **DNS** de la boîte de dialogue **Propriétés** pour le nœud de protocole, ou par étendue dans la console DHCP. Vous pouvez également configurer DHCP pour effectuer des mises à jour au nom de ses clients sur tous les serveurs DNS qui prennent en charge les mises à jour dynamiques.

Par défaut, le serveur DHCP se comporte de la façon suivante :

- Le serveur DHCP met dynamiquement à jour les enregistrements de ressources de type A (hôte) et les enregistrements de ressources du pointeur (PTR) dans DNS uniquement si des clients DHCP le demandent. Par défaut, le client demande que le serveur DHCP inscrive l'enregistrement de ressources du pointeur (PTR) de DNS, alors que le client inscrit son propre enregistrement de ressources de l'hôte (A) de DNS.
- Le serveur DHCP ignore les enregistrements de ressources hôte (A) et de pointeur (PTR) quand le bail du client est supprimé.

Vous pouvez modifier cette option de sorte qu'elle demande au serveur DHCP de toujours mettre dynamiquement à jour les enregistrements de ressources hôte (A) et de pointeur (PTR) de DNS, quelles que soient les demandes du client. De cette façon, le serveur DHCP devient le propriétaire de l'enregistrement de ressources parce que le serveur DHCP a exécuté l'inscription des enregistrements de ressources. Une fois que le serveur DHCP devient le propriétaire des enregistrements de ressources de l'hôte (A) et du pointeur (PTR) de l'ordinateur client, seul ce serveur DHCP peut mettre à jour les enregistrements de ressources DNS pour l'ordinateur client en fonction de la durée et du renouvellement du bail de DHCP.

Configuration des créations avancées d'étendue de DHCP



Vous pouvez configurer des créations avancées d'étendue de DHCP appelées *étendues globales*. Une étendue globale est une collection d'étendues individuelles qui sont regroupées à des fins administratives. Les ordinateurs clients peuvent ainsi recevoir une adresse IP de plusieurs sous-réseaux logiques, même si les clients résident sur le même sous-réseau physique. Vous pouvez créer une étendue globale uniquement si deux étendues IP au moins sont déjà créées dans le DHCP. Vous pouvez utiliser l'Assistant Nouvelle étendue globale pour sélectionner les étendues que vous souhaitez combiner pour créer une étendue globale.

Avantages des étendues globales

Une étendue globale s'avère utile dans plusieurs cas de figure. Par exemple, si une étendue est à court d'adresses et que vous ne pouvez pas ajouter d'autres adresses du sous-réseau, vous pouvez ajouter un nouveau sous-réseau au serveur DHCP. Cette étendue louera des adresses aux clients du même réseau physique, mais les clients résideront logiquement dans un réseau distinct. Ce processus s'appelle le *multinetting*. Une fois que vous ajoutez un nouveau sous-réseau, vous devez configurer des routeurs pour identifier le nouveau sous-réseau de sorte à vérifier les communications locales dans le réseau physique.

Une étendue globale est également utile lorsqu'il est nécessaire d'amener progressivement des clients vers un nouveau plan de numérotation IP. Lorsque deux plans de numérotation coexistent pendant la durée du bail d'origine, vous pouvez déplacer des clients dans le nouveau sous-réseau en toute transparence. Lorsque vous avez renouvelé tous les baux clients dans le nouveau sous-réseau, vous pouvez retirer l'ancien.

Étendues de multidiffusion

Une étendue de multidiffusion est une collection d'adresses de multidiffusion issues de la plage d'adresses IP de classe D allant de 224.0.0.0 à 239.255.255.255 (224.0.0.0/3). Ces adresses sont utilisées lorsque les applications doivent communiquer de manière efficace et simultanée avec de nombreux clients. Pour atteindre cet objectif, plusieurs hôtes sont à l'écoute du trafic pour une même adresse IP.

Une étendue de multidiffusion est généralement désignée sous le nom d'étendue MADCAP (Multicast Address Dynamic Client Allocation Protocol). Les applications qui demandent des adresses de ces étendues doivent prendre en charge l'interface de programmation d'applications (API) MADCAP. Les Services de déploiement Windows sont un exemple d'une application qui prend en charge des transmissions par multidiffusion.

Les étendues de multidiffusion permettent aux applications de réserver une adresse IP de multidiffusion afin de remettre des données ou du contenu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Intégration de DHCP à IPv6

IPv6 peut se configurer sans DHCP.
Les clients IPv6 ont une adresse IPv6 locale de liaison affectée automatiquement. Une adresse de liaison locale sert uniquement aux communications dans le réseau local. Elle est équivalente aux adresses 169.254.0.0 affectées automatiquement utilisées par IPv4. Les interfaces réseau IPv6 peuvent avoir plusieurs adresses IPv6 (ce qui est souvent le cas). Par exemple, les adresses pourraient comprendre une adresse de liaison locale affectée automatiquement et une adresse globale affectée par DHCP. À l'aide de DHCP pour IPv6 (DHCPv6), un hôte IPv6 peut obtenir des préfixes de sous-réseau, des adresses globales, et d'autres paramètres de configuration IPv6.

Le protocole DHCPv6 prend en charge les configurations avec et sans état

Le protocole DHCPv6 prend également en charge les étendues configurées avec les propriétés suivantes

- Nom et description
- Préférence
- Durées de vie valide et préférée
- Préfixe
- Exclusions
- Options DHCP

Remarque : Vous devriez obtenir un bloc d'adresses IPv6 d'un registre Internet régional. Il existe cinq registres Internet régionaux dans le monde. Les voici :

- African Network Information Centre (AfriNIC) pour l'Afrique ;
- Asia-Pacific Network Information Centre (APNIC) pour l'Asie, l'Australie, la Nouvelle-Zélande et les pays voisins ;
- American Registry for Internet Numbers (ARIN) pour le Canada, beaucoup d'îles des Caraïbes et de l'Atlantique Nord, et les États-Unis ;
- Latin America and Caribbean Network Information Centre (LACNIC) pour l'Amérique latine et une partie de la région des Caraïbes ;
- Réseaux IP Européens Network Coordination Centre (RIPE NCC) pour l'Europe, la Russie, le Moyen-Orient et l'Asie centrale.

Configuration sans état et avec état

Chaque fois que vous ajoutez le rôle de serveur DHCP à un ordinateur Windows Server 2012, vous installez également automatiquement un serveur DHCPv6. Windows Server 2012 prend en charge les configurations DHCPv6 avec et sans état :

- Configuration avec état. La configuration avec état intervient lorsque le serveur DHCPv6 attribue l'adresse IPv6 au client, en même temps que d'autres données DHCP.
- Configuration sans état. La configuration sans état intervient quand le routeur de sous-réseau attribue l'adresse IPv6 automatiquement et que le serveur DHCPv6 attribue seulement d'autres paramètres de configuration IPv6.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Étendues DHCPv6 pour IPv6

Les étendues DHCPv6 pour IPv6 doivent être créées séparément des étendues IPv4. Les étendues IPv6 ont un mécanisme de bail amélioré et plusieurs options différentes. Lorsque vous configurez une étendue DHCPv6, vous devez définir les propriétés indiquées dans le tableau suivant.

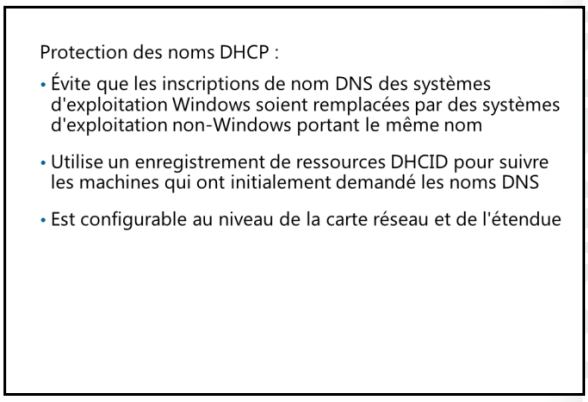
Propriété	Utilisation
Nom et description	Cette propriété identifie l'étendue.
Préfixe	Le préfixe d'adresse IPv6 est analogue à la plage d'adresses IPv4. Il définit la partie réseau de l'adresse IP.
Préférence	Cette propriété indique aux clients DHCPv6 quel serveur utiliser si vous avez plusieurs serveurs DHCPv6.
Exclusions	Cette propriété définit les adresses uniques ou les blocs d'adresses qui font partie du préfixe IPv6, mais qui ne sont pas proposés pour le bail.
Durées de vie valide et préférée	Cette propriété définit la durée de validité des adresses louées.
Options DHCP	Comme avec IPv4, il y a beaucoup d'options disponibles.

Configuration d'une étendue IPv6

Vous pouvez utiliser le nouvel Assistant d'étendue pour créer des étendues IPv6 :

1. Dans la console DHCP, cliquez avec le bouton droit sur le nœud IPv6, puis cliquez sur **Nouvelle étendue**.
2. Configurez un préfixe et une préférence d'étendue.
3. Définissez les adresses IP de début et de fin, et toutes les exclusions.
4. Configurez les propriétés de durée de vie **Préférée** et **Valide**.
5. Activez l'étendue.

Qu'est-ce que la protection des noms DHCP ?



Vous devez empêcher les noms que DHCP inscrit dans DNS au nom d'autres ordinateurs ou systèmes d'être remplacés par des systèmes d'exploitation autres que Windows qui utilisent les mêmes noms. En outre, vous devez également empêcher les noms d'être remplacés par des systèmes utilisant des adresses statiques en conflit avec les adresses affectées par DHCP quand ils utilisent un serveur DNS non sécurisé et que DHCP n'est pas configuré pour détecter les conflits. Par exemple, un système Unix nommé Client1 pourrait éventuellement remplacer l'adresse DNS attribuée et enregistrée par DHCP au nom d'un système Windows également nommé Client1. Une nouvelle fonctionnalité dans Windows Server 2012 - Protection des noms DHCP - se charge de ce problème.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le terme « occupation de nom » est utilisé pour décrire le conflit qui survient quand un client enregistre un nom dans DNS alors que celui-ci est déjà utilisé par un autre client. Ce problème rend la machine d'origine inaccessible et survient en général avec des systèmes portant le même nom que des systèmes d'exploitation Windows. La protection des noms DHCP résout ce problème en utilisant un enregistrement de ressource intitulé Identificateur de configuration d'hôte dynamique (DHCID) pour effectuer le suivi du nom initialement demandé par les machines. Le serveur DHCP fournit l'enregistrement DHCID, qui est enregistré dans DNS. Quand le serveur DHCP reçoit une demande d'une machine avec un nom d'adresse IP existant, le serveur DHCP peut se reporter au DHCID dans DNS pour vérifier que la machine qui demande le nom est la machine d'origine qui utilisait le nom. Si ce n'est pas la même machine, l'enregistrement de ressource DNS n'est pas mis à jour.

Vous pouvez implémenter la protection des noms pour les protocoles IPv4 et IPv6. En outre, vous pouvez configurer la protection des noms DHCP au niveau du serveur et au niveau de l'étendue. L'implémentation au niveau du serveur s'appliquera seulement aux étendues nouvellement créées.

Pour activer la protection des noms DHCP pour un nœud IPv4 ou IPv6 :

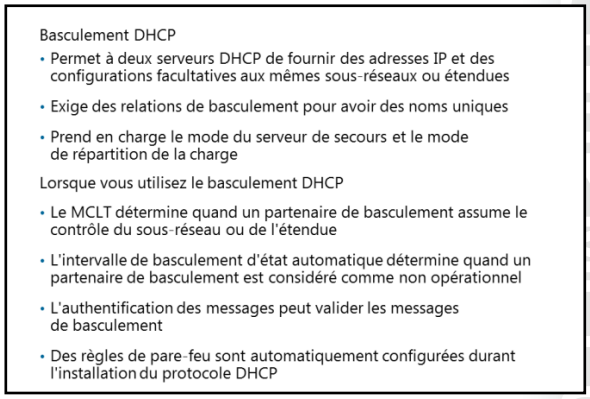
1. ouvrez la console **DHCP** ;
2. cliquez avec le bouton droit sur le nœud IPv4 ou IPv6, puis ouvrez la page **Propriété** ;
3. cliquez sur **DNS**, cliquez sur **Avancé**, puis activez la case à cocher **Activer la protection des noms**.

Pour activer la protection des noms DHCP pour une étendue :

1. Ouvrez la **console MMC (Microsoft Management Console) DHCP**.
2. Développez le nœud IPv4 ou IPv6, puis ouvrez la page **Propriété**.
3. cliquez sur **DNS**, cliquez sur **Avancé**, puis activez la case à cocher **Activer la protection des noms**.

Qu'est-ce que le basculement DHCP ?

Le DHCP gère la distribution des adresses IP dans les réseaux TCP/IP de toutes les tailles. Quand ce service échoue, les clients perdent la connectivité au réseau et à toutes ses ressources. Une nouvelle fonctionnalité dans Windows Server 2012, le basculement DHCP, se charge de ce problème.



Basculement DHCP

Les clients DHCP renouvellent leurs baux d'adresse IP à intervalles réguliers configurables. Quand le service DHCP échoue, les baux expirent et les clients n'ont plus d'adresses IP. Auparavant, le basculement DHCP n'était pas possible car les serveurs DHCP étaient indépendants et ignoraient l'existence les uns des autres. Par conséquent, la configuration de deux serveurs DHCP distincts pour distribuer le même pool d'adresses a pu avoir pour conséquence la présence d'adresses en double. En outre, la mise à disposition de services DHCP redondants vous obligeait à configurer le clustering et à réaliser un grand nombre de tâches de configuration et de surveillance manuelles.

La nouvelle fonctionnalité de basculement DHCP permet à deux serveurs DHCP de fournir des adresses IP et des configurations facultatives aux mêmes sous-réseaux ou étendues. Par conséquent, vous pouvez maintenant configurer deux serveurs DHCP pour répliquer les informations de bail. En cas de défaillance d'un des serveurs DHCP, l'autre serveur sert les clients pour l'ensemble du sous-réseau.

Remarque : Dans Windows Server 2012, vous ne pouvez configurer que deux serveurs DHCP pour le basculement et seulement pour les étendues IPv4 et les sous-réseaux.

Configuration du basculement DHCP

Pour configurer le basculement de DHCP, vous devez établir une relation de basculement entre les deux services des serveurs DHCP. Vous devez également affecter à cette relation un nom unique. Le partenaire de basculement échange ce nom pendant la configuration. Cela permet à un serveur DHCP unique d'avoir plusieurs relations de basculement avec d'autres serveurs DHCP, à condition que tous les serveurs aient des noms uniques. Pour configurer le basculement, utilisez l'Assistant configuration du basculement que vous pouvez lancer en cliquant avec le bouton droit sur le nœud d'IP ou le nœud de l'étendue.

Remarque : Le basculement DHCP est soumis à une contrainte de temps. Vous devez synchroniser le temps entre les partenaires de la relation. Si la différence de temps est supérieure à une minute, le processus de basculement s'interrompt avec une erreur critique.

Vous pouvez configurer le basculement dans un des deux modes suivants.

Mode	Caractéristiques
Serveur de secours	Dans ce mode, un serveur est le serveur principal et l'autre est un serveur secondaire. Le serveur principal affecte activement des configurations IP pour l'étendue ou le sous-réseau. Le serveur DHCP secondaire assurera ce rôle uniquement si le serveur principal devient indisponible. Un serveur DHCP peut agir simultanément en tant que serveur principal pour une étendue ou un sous-réseau, et en tant que serveur secondaire pour un autre. Les administrateurs doivent configurer un pourcentage des adresses d'étendue à attribuer au serveur de secours. Ces adresses sont fournies pendant le délai de transition maximal du client (MCLT) si le serveur principal est en panne. La valeur MCLT par défaut correspond à 5 % de l'étendue. Le serveur secondaire prend le contrôle de la plage d'IP entière après l'expiration du délai MCLT. Le mode du serveur de secours est le mieux adapté aux déploiements où un site de récupération de données est situé à un autre emplacement. De cette façon le serveur DHCP ne dépannera pas les clients à moins d'une panne du serveur principal.
Répartition de la charge	Il s'agit du mode par défaut. Dans ce mode les deux serveurs fournissent la configuration IP aux clients simultanément. Le serveur qui répond aux demandes de configuration IP dépend de la façon dont l'administrateur configure le taux de distribution de la charge. Le taux par défaut est de 50:50.

MCLT

L'administrateur configure le paramètre MCLT pour déterminer la durée pendant laquelle un serveur DHCP doit patienter lorsqu'un partenaire est indisponible avant de prendre le contrôle de la plage d'adresses entière. Cette valeur ne peut pas être égale à zéro, et le délai par défaut est d'une heure.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Intervalle de basculement d'état automatique

Quand un serveur perd le contact avec son partenaire, il passe à l'état Communication interrompue. Étant donné que le serveur ne peut pas déterminer ce qui provoque la perte de communication, il reste dans cet état jusqu'à ce que l'administrateur le remplace manuellement par l'état Partenaire hors service. L'administrateur peut également activer la transition automatique vers l'état Partenaire hors service en configurant l'intervalle de basculement d'état automatique. La valeur par défaut de cet intervalle est de 10 minutes.

Authentification des messages

Windows Server 2012 vous permet d'authentifier le trafic des messages de basculement entre les partenaires de réplication. L'administrateur peut établir un secret partagé, qui agit comme un mot de passe, dans l'Assistant de configuration du basculement pour le basculement DHCP. Cela valide que le message de basculement vient du partenaire de basculement.

Observations relatives au pare-feu

DHCP utilise le port TCP 647 pour écouter le trafic de basculement. L'installation de DHCP crée les règles de pare-feu entrant et sortant suivantes :

- Microsoft-Windows-DHCP-Failover-TCP-In
- Microsoft-Windows-DHCP-Failover-TCP-Out

Démonstration : Configuration du basculement DHCP

Dans cette démonstration, vous allez apprendre à configurer une relation de basculement DHCP.

Procédure de démonstration

Configurer une relation de basculement DHCP

1. Connectez-vous à **LON-SVR1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**. Notez que le serveur est autorisé, mais qu'aucune étendue n'est configurée.
2. Basculez vers **LON-DC1**. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP** dans la liste déroulante.
3. Dans la console DHCP, lancez l'**Assistant de configuration du basculement**.
4. Configurez la réplication du basculement avec les paramètres suivants :
    - Serveur partenaire : **172.16.0.21**
    - Nom de la relation : **Adatum**
    - Délai de transition maximal du client (MCLT) : **15 minutes**
    - Mode : **Équilibrage de charge**
    - Pourcentage d'équilibrage de charge : **50%**
    - Intervalle de basculement d'état : **60 minutes**
    - Secret d'authentification des messages partagé : **Pa$$w0rd**.
5. Exécutez l'Assistant Configuration du basculement.
6. Rebasculez vers **LON-SVR1**, et notez que le nœud IPv4 est **actif** et que l'étendue Adatum est **configurée**.

Leçon 2
Configuration des paramètres DNS avancés

Dans les réseaux TCP/IP de toute taille, certains services sont essentiels. DNS est l'un des services réseau les plus importants pour tout réseau, car beaucoup d'autres applications et services, y compris AD DS, s'appuient sur DNS pour résoudre les noms des ressources vers des adresses IP. Si DNS n'est pas disponible, les authentifications utilisateur peuvent échouer, et les ressources et les applications réseau peuvent devenir inaccessibles. Pour cette raison, vous devez gérer et protéger DNS. Cette leçon présente des techniques et des options de gestion pour optimiser la résolution de DNS. Windows Server 2012 implémente DNSSEC pour protéger les réponses de DNS. Windows Server 2012 prend également en charge les zones de nom globales pour assurer la résolution de noms en une partie.

Objectifs de la leçon

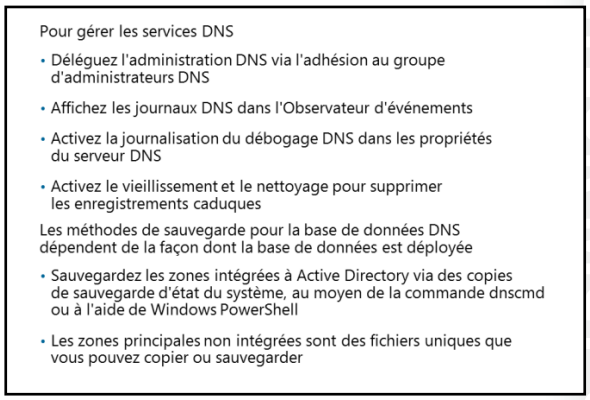
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- gérer les services DNS ;
- optimiser la résolution de nom DNS ;
- décrire les zones de nom globales ;
- décrire les options d'implémentation de la sécurité DNS ;
- expliquer le fonctionnement de DNSSEC ;
- décrire les nouvelles fonctionnalités de DNSSEC pour Windows Server 2012 ;
- expliquer comment configurer DNSSEC.

Gestion des services DNS

Comme d'autres services réseau importants, vous devez gérer DNS. La gestion de DNS comprend les tâches suivantes :

- déléguer l'administration de DNS ;
- configurer la journalisation pour DNS ;
- vieillissement et nettoyage ;
- sauvegarder la base de données DNS.



Déléguer l'administration de DNS

Par défaut, le groupe Administrateurs du domaine dispose de toutes les autorisations pour gérer tous les aspects du serveur DNS dans son domaine natif, et le groupe Administrateurs de l'entreprise dispose de toutes les autorisations pour gérer tous les aspects de tous les serveurs DNS dans n'importe quel domaine de la forêt. Si vous devez déléguer l'administration d'un serveur DNS à un autre utilisateur ou groupe, vous pouvez ajouter cet utilisateur ou groupe global au groupe d'administrateurs DNS pour un domaine donné dans la forêt. Les membres du groupe d'administrateurs DNS peuvent afficher et modifier tous les données, paramètres et configurations DNS des serveurs DNS dans leur domaine natif.

Le groupe d'administrateurs DNS est un groupe de sécurité local du domaine, et ne compte par défaut aucun membre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configurer la journalisation DNS

Par défaut, DNS maintient un journal de serveur DNS, que vous pouvez afficher dans l'Observateur d'événements. Ce journal des événements est situé dans le dossier Journaux des applications et des services dans l'Observateur d'événements. Il enregistre des événements courants tels que :

- démarrage et arrêt du service DNS ;
- chargement d'arrière-plan et événements de signature de zone ;
- Modifications des paramètres de configuration DNS ;
- divers avertissements et événements d'erreur.

Pour une journalisation plus détaillée, vous pouvez activer l'enregistrement de débogage. Les options d'enregistrement de débogage sont désactivées par défaut, mais peuvent être activées de façon sélective. Les options d'enregistrement de débogage comprennent ce qui suit :

- Direction des paquets
- Contenu des paquets
- Protocole de transport
- Type de demande
- Filtrer les paquets par adresse IP
- Spécifier le nom et l'emplacement du fichier journal, situé dans le répertoire %windir%\System32\DNS
- Taille maximale (octets) du fichier journal

L'enregistrement de débogage peut consommer beaucoup de ressources. Il peut affecter les performances générales du serveur et consommer de l'espace disque. Par conséquent, son utilisation ne doit constituer qu'une mesure provisoire, lorsque des informations plus détaillées au sujet des performances du serveur sont requises. Pour activer l'enregistrement du débogage sur le serveur DNS, faites ce qui suit :

1. Ouvrez la console DNS.
2. Cliquez avec le bouton droit sur le serveur DNS applicable, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Enregistrement de débogage**.
4. Sélectionnez **Enregistrer les paquets pour le débogage**, puis sélectionnez les événements que vous souhaitez que le serveur DNS enregistre pour le débogage.

Vieillissement et nettoyage

Les mises à jour dynamiques de DNS ajoutent automatiquement des enregistrements de ressources à la zone, mais dans certains cas ces enregistrements ne sont pas supprimés automatiquement quand ils ne sont plus requis. Ainsi, si un ordinateur inscrit son propre enregistrement de ressource hôte (A) au démarrage et qu'ensuite sa connexion au réseau est rompue de manière incorrecte, cet enregistrement hôte risque ne pas être supprimé. Ces enregistrements, appelés *enregistrements caduques*, occupent de l'espace dans la base de données DNS et peuvent recevoir une réponse incorrecte à leur requête. Windows Server 2012 peut rechercher ces enregistrements caduques et, selon le vieillissement de l'enregistrement, les effacer de la base de données DNS.

Le vieillissement et le nettoyage sont désactivés par défaut. Vous pouvez activer le vieillissement et le nettoyage dans les propriétés **Avancées** du serveur DNS, ou l'activer pour certaines zones dans la fenêtre **Propriétés** de la zone.

Le vieillissement est déterminé à l'aide des paramètres appelés Intervalle d'actualisation et Intervalle de non-actualisation. L'*intervalle d'actualisation* désigne la date et l'heure auxquelles l'enregistrement peut être actualisé par le client. Par défaut, cet intervalle est de sept jours. L'*intervalle de non-actualisation* désigne la période de temps pendant laquelle l'enregistrement ne peut pas être actualisé par le client. Par défaut, cet intervalle est de sept jours. Dans le cours normal des événements, un enregistrement d'hôte de client ne peut pas être actualisé dans la base de données pendant sept jours après sa première inscription ou actualisation. Cependant, il doit être actualisé dans les sept prochains jours suivant l'intervalle de non-actualisation, sans quoi l'enregistrement peut être nettoyé de la base de données. Un client tentera d'actualiser son enregistrement DNS au démarrage, et toutes les 24 heures pendant l'exécution du système.

 **Remarque :** Les enregistrements qui sont ajoutés dynamiquement à la base de données sont horodatés. Les enregistrements statiques que vous entrez manuellement ont une valeur d'horodatage égale à zéro 0 ; ils ne seront par conséquent pas affectés par le vieillissement, et ne seront pas nettoyés de la base de données.

Sauvegarder la base de données DNS

La façon dont vous sauvegardez la base de données DNS dépend de la façon dont le DNS a été implémenté dans votre organisation. Si votre zone DNS a été implémentée en tant que zone intégrée à Active Directory, alors votre zone DNS est incluse dans le fichier de la base de données Active Directory ntds.dit. Si la zone DNS est une zone principale et n'est pas enregistrée dans AD DS, alors le fichier est enregistré en tant que fichier .dns dans le dossier %SystemRoot%\System32\Dns.

Sauvegarde des zones intégrées à Active Directory

Les zones intégrées à Active Directory sont enregistrées dans AD DS et sont sauvegardées comme partie d'une sauvegarde d'état du système ou comme sauvegarde de serveur entier. En outre, vous pouvez sauvegarder uniquement la zone intégrée à Active Directory à l'aide de l'outil de ligne de commande dnscmd.

Pour sauvegarder une zone intégrée à Active Directory, procédez comme suit :

1. Lancez une invite de commandes avec élévation de privilèges.
2. Exécutez la commande suivante :

   ```
   dnscmd /ExportationZone <nom de zone> <nom de fichier de zone>
   ```

   où le <*nom de zone*> correspond au nom de votre zone DNS, et le <*nom de fichier de zone*> correspond au fichier que vous souhaitez créer pour conserver les informations de sauvegarde.

L'outil dnscmd exporte les données de la zone vers le nom de fichier que vous indiquez dans la commande, dans le répertoire %windir%\System32\DNS.

Vous pouvez également utiliser Windows PowerShell® pour effectuer la même tâche. Dans Windows PowerShell, utilisez l'applet de commande **Export-DnsServerZone**. Par exemple, si vous souhaitez exporter une zone intitulée contoso.com, saisissez la commande suivante :

```
Export-DnsServerZone –Name contoso.com –Filename contoso
```

Sauvegarde des zones principales

Sauvegarder une zone principale qui n'est pas enregistrée dans AD DS consiste simplement à copier ou sauvegarder le fichier de zone individuel, *nomdezone*.dns, situé dans le répertoire %windir%\System32\DNS. Par exemple, si votre zone DNS principale est intitulée Adatum.com, le fichier de zone DNS sera intitulé Adatum.com.dns.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Optimisation de la résolution de nom DNS

Dans un événement de requête DNS standard, un ordinateur client tente de résoudre un nom de domaine complet vers une adresse IP. Par exemple, si un utilisateur essaie d'accéder au nom de domaine complet www.microsoft.com, l'ordinateur client envoie une requête récursive au serveur DNS configuré pour découvrir l'adresse IP associée à ce nom de domaine complet. Le serveur DNS local doit alors répondre avec une réponse faisant autorité. Si le serveur DNS local a une copie de la zone DNS pour laquelle elle a été interrogée, elle enverra une réponse faisant autorité à l'ordinateur client. Si le serveur DNS local ne dispose pas de ces informations, il exécutera la récursivité.

Option	Description
Redirection	Transfère les requêtes DNS qui ne peuvent pas être résolues localement à d'autres serveurs DNS spécifiques
Redirection conditionnelle	Transfère les requêtes pour des suffixes DNS spécifiques à des serveurs DNS spécifiques
Zones de stub	Copie régulièrement répliquée de certains enregistrements de ressources qui identifient les serveurs DNS prévalant pour des domaines DNS spécifiques
Classement de masque réseau	Répond aux requêtes DNS avec les adresses des hôtes à proximité en fonction des informations d'adresse IP du client

La *récursivité* désigne le processus par lequel le serveur DNS local envoie une requête récursive à un autre serveur DNS jusqu'à ce qu'il trouve une réponse faisant autorité, puis renvoie la réponse au client ayant fait la demande initiale. Par défaut, ce serveur sera l'un des serveurs sur Internet répertoriés en tant qu'indication de racine. Quand le serveur DNS local reçoit une réponse, il renvoie les informations à l'ordinateur client ayant fait la demande initiale.

Un certain nombre d'options est disponible pour optimiser la résolution de nom DNS. Elles incluent notamment les fonctionnalités suivantes :

- Redirection
- Redirection conditionnelle
- Zones de stub
- Classement de masque réseau

Redirection

Un *redirecteur* est un serveur DNS de réseau que vous configurez pour transférer des requêtes DNS concernant des noms d'hôte qu'il ne peut pas résoudre à d'autres serveurs DNS. Dans un environnement standard, le serveur DNS interne transfère les requêtes concernant des noms d'hôte externes aux serveurs DNS sur Internet. Par exemple, si le serveur DNS de réseau local ne peut pas résoudre avec autorité une requête pour www.microsoft.com, alors le serveur DNS local peut transférer la requête au serveur DNS du fournisseur de service Internet (ISP).

Redirection conditionnelle

Vous pouvez également utiliser des redirecteurs conditionnels pour transférer des requêtes en fonction de noms de domaine spécifiques. Un redirecteur conditionnel est un paramètre de configuration du serveur DNS qui redirige des requêtes DNS en fonction du nom du domaine DNS contenu dans les requêtes. Par exemple, vous pouvez configurer un serveur DNS afin qu'il transfère toutes les requêtes qu'il reçoit concernant des noms se terminant par corp.adatum.com à l'adresse IP d'un serveur DNS spécifique ou aux adresses IP de plusieurs serveurs DNS. Ce transfert peut s'avérer utile lorsque vous avez plusieurs espaces de noms DNS dans une forêt. Par exemple, supposez que Contoso.com et Adatum.com sont fusionnés. Pour éviter que chaque domaine ne soit contraint d'héberger une réplication de la base de données DNS de l'autre domaine, vous pourriez créer des redirecteurs conditionnels indiquant les serveurs DNS spécifiques de chacun pour la résolution des noms DNS internes.

Zones de stub

Une *zone de stub* est une copie d'une zone qui contient uniquement les enregistrements de ressources nécessaires à l'identification des serveurs DNS faisant autorité pour la zone en question. Une zone de stub résout des noms entre les espaces de noms DNS distincts, qui pourraient être nécessaires lorsque vous voulez qu'un serveur DNS hébergeant une zone parent reste informé de tous les serveurs DNS faisant autorité sur l'une de ses zones enfants. Une zone de stub qui est hébergée sur un serveur DNS de domaine parent recevra une liste de tous les nouveaux serveurs DNS pour la zone d'enfant, quand elle demande une mise à jour du serveur principal de la zone de stub. Avec cette méthode, le serveur DNS hébergeant la zone parent conserve une liste actualisée des serveurs DNS faisant autorité sur la zone enfant, reflétant les ajouts et suppressions.

Une zone de stub comprend ce qui suit :

- l'enregistrement de ressource Source de noms (SOA, Start Of Authority), les enregistrements de ressources Serveur de noms (NS, Name Server) et les enregistrements de ressources de type « A » de la zone déléguée ;
- l'adresse IP d'un ou plusieurs serveurs maîtres que vous pouvez utiliser pour mettre à jour la zone de stub.

Les zones de stub présentent les caractéristiques suivantes :

- Vous pouvez créer des zones de stub à l'aide de l'Assistant Nouvelle zone.
- Vous pouvez enregistrer des zones de stub dans AD DS.
- Vous pouvez répliquer des zones de stub dans le domaine seulement, ou dans l'ensemble de la forêt.
- Les serveurs maîtres d'une zone de stub correspondent à un ou plusieurs serveurs DNS responsables de la copie initiale des informations de la zone, et désignent généralement le serveur DNS hébergeant la zone principale du nom de domaine délégué.

Classement de masque réseau

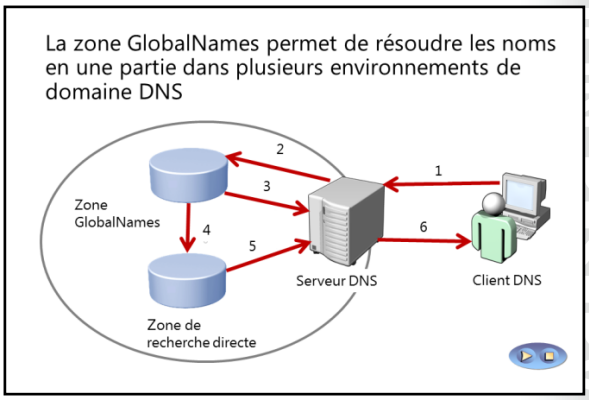
Le classement de masque réseau renvoie des adresses pour des requêtes DNS concernant des enregistrements d'adresse de type A (enregistrement A) qui donnent la priorité aux ressources sur le sous-réseau local de l'ordinateur client au client. En d'autres termes, les adresses des hôtes qui sont sur le même sous-réseau que le client effectuant la demande auront une priorité plus élevée dans la réponse de DNS à l'ordinateur client.

La localisation est basée sur les adresses IP. Par exemple, si plusieurs enregistrements de type A sont associés au même nom DNS, et que tous les enregistrements de type A se trouvent sur un sous-réseau IP différent, le classement de masque réseau renvoie un enregistrement de type A se trouvant sur le même sous-réseau IP que l'ordinateur client ayant effectué la demande.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que la zone GlobalNames ?



Le service de serveur DNS dans Windows Server 2012 offre un nouveau type de zone, la zone GlobalNames, que vous pouvez utiliser pour conserver des noms uniques en une partie dans l'ensemble d'une forêt. Ce type de zone élimine le besoin d'utiliser le service WINS basé sur NetBIOS pour prendre en charge les noms en une partie. Les zones GlobalNames fournissent la résolution de noms en une partie pour les réseaux de grandes entreprises qui ne déploient pas WINS et qui ont plusieurs environnements de domaine DNS. Les zones GlobalNames sont créées manuellement et ne prennent pas en charge l'inscription des enregistrements dynamiques.

Quand les clients tentent de résoudre des noms courts, ils ajoutent leur nom de domaine DNS automatiquement. Selon la configuration, ils essaient également de rechercher le nom dans le nom de domaine de niveau supérieur, ou de parcourir leur liste de suffixes de noms. Par conséquent, les noms courts sont résolus dans le même domaine.

Vous pouvez utiliser une zone GlobalNames pour maintenir une liste de suffixes de recherche DNS pour résoudre des noms parmi plusieurs environnements de domaine DNS. Par exemple, si une organisation prend en charge deux domaines DNS, tels qu'adatum.com et contoso.com, les utilisateurs dans le domaine DNS adatum.com doivent utiliser un nom de domaine complet tel que data.contoso.com pour localiser les serveurs dans contoso.com. Autrement, l'administrateur de domaine doit ajouter un suffixe de recherche DNS pour contoso.com sur tous les systèmes dans le domaine adatum.com. Si les clients cherchent uniquement le nom de serveur « data », la recherche échouera.

Les noms globaux sont basés sur la création d'enregistrements de ressources de noms canoniques (CNAME) dans une zone de recherche directe spéciale qui utilise des noms uniques pour indiquer des noms de domaine complets. Par exemple, les zones GlobalNames permettraient à des clients dans le domaine adatum.com et le domaine contoso.com d'utiliser un nom en une partie, tel que data, pour localiser un serveur dont le nom de domaine complet est data.contoso.com sans devoir utiliser le nom de domaine complet.

Création d'une zone GlobalNames

Pour créer une zone GlobalNames, procédez comme suit :

1. Utilisez l'outil **dnscmd** pour activer la prise en charge des zones GlobalNames.
2. Créez une nouvelle zone de recherche directe nommée **GlobalNames** (ne respectant pas la casse). N'autorisez pas les mises à jour dynamiques pour cette zone.
3. Créez manuellement des enregistrements CNAME qui pointent vers les enregistrements qui existent déjà dans les autres zones hébergées sur vos serveurs DNS.

Par exemple, vous pourriez créer un enregistrement CNAME dans la zone GlobalNames intitulée Data pointant vers Data.contoso.com. Cela permettrait aux clients de n'importe quel domaine DNS de l'organisation de trouver ce serveur à l'aide du nom en une partie Data.

Vous pouvez également utiliser les applets de commande Windows PowerShell cmdlets **Get-DnsServerGlobalNameZone** et **Set-DnsServerGlobalNameZone** pour configurer les zones GlobalNames.

Options d'implémentation de la sécurité DNS

Puisque le DNS est un service réseau critique, vous devez le protéger autant que possible. Un certain nombre d'options sont disponibles pour protéger le serveur DNS, parmi lesquelles :

- Verrouillage de cache DNS
- Pool de sockets DNS
- DNSSEC

Option	Description
Verrouillage de cache DNS	Évite que les entrées du cache ne soient écrasées jusqu'à ce qu'un pourcentage du TTL ait expiré
Pool de sockets DNS	Randomise le port source pour la publication des requêtes DNS Activé par défaut dans Windows Server 2012
DNSSEC	Active la signature cryptographique des enregistrements DNS pour que les ordinateurs client puissent valider les réponses

Verrouillage de cache DNS

Le verrouillage de cache est une fonctionnalité de sécurité de Windows Server 2012 qui vous permet de contrôler le moment auquel les informations dans le cache DNS peuvent être écrasées. Quand un serveur DNS récursif répond à une requête, il met les résultats en cache pour pouvoir répondre rapidement s'il reçoit une autre requête demandant les mêmes informations. La période de temps pendant laquelle le serveur DNS conserve les informations dans son cache est déterminé par la valeur Durée de vie (TTL, Time to Live) pour un enregistrement de ressource. Les informations dans le cache peuvent être écrasées avant l'expiration de la durée de vie si les informations actualisées sur cet enregistrement de ressource sont reçues. Si un utilisateur malveillant écrase avec succès les informations dans le cache, alors l'utilisateur malveillant pourrait être en mesure de rediriger votre trafic réseau vers un site malveillant. Quand vous activez le verrouillage de cache, le serveur DNS interdit l'écrasement des enregistrements mis en cache pendant la durée de vie définie.

Vous allez configurer le verrouillage de cache comme une valeur de pourcentage. Par exemple, si la valeur de verrouillage de cache est définie sur 50, alors le serveur DNS ne remplacera pas une entrée mise en cache pendant la moitié de la durée de vie. Par défaut, la valeur de pourcentage de verrouillage de cache est de 100. Ceci signifie que les entrées mises en cache ne seront pas écrasée pendant toute la durée de vie.

Vous pouvez configurer le verrouillage de cache avec l'outil **dnscmd** comme suit :

1. Lancez une invite de commandes avec élévation de privilèges.
2. Exécutez la commande suivante :

```
dnscmd /Config /CacheLockingPercent <percent>
```

3. Redémarrez le service DNS pour appliquer les modifications.

Vous pouvez également utiliser l'applet de commande Windows PowerShell **Set-DnsServerCache –LockingPercent** cmdlet pour définir cette valeur. Par exemple :

```
Set-DnsServerCache –LockingPercent <value>
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pool de sockets DNS

Le pool de sockets DNS permet à un serveur DNS d'utiliser les ports source de façon aléatoire lors de l'émission de requêtes DNS. Quand le service DNS démarre, le serveur choisit un port source dans un pool de sockets disponibles pour émettre des requêtes. Au lieu d'utiliser un port source prévisible, le serveur DNS utilise un numéro de port aléatoire qu'il choisit parmi le pool de sockets DNS. Le pool de sockets DNS rend les attaques par falsification de cache plus difficiles car un utilisateur malveillant doit deviner à la fois le port source d'une requête DNS et un ID de transaction aléatoire pour exécuter l'attaque avec succès. Dans Windows Server 2012, le pool de sockets DNS est activé par défaut.

La taille par défaut du pool de sockets DNS est de 2 500. Quand vous configurez le pool de sockets DNS, vous pouvez choisir une taille d'une valeur comprise entre 0 et 10 000. Plus la valeur est grande, plus la protection contre les attaques par usurpation d'adresse DNS est élevée. Si le serveur DNS exécute Windows Server 2012, vous pouvez également configurer une liste d'exclusions de pool de sockets DNS.

Vous pouvez configurer la taille du pool de sockets DNS à l'aide de l'outil **dnscmd** comme suit :

1. Lancez une invite de commandes avec élévation de privilèges.
2. Exécutez la commande suivante :

```
dnscmd /Config /SocketPoolSize <value>
```

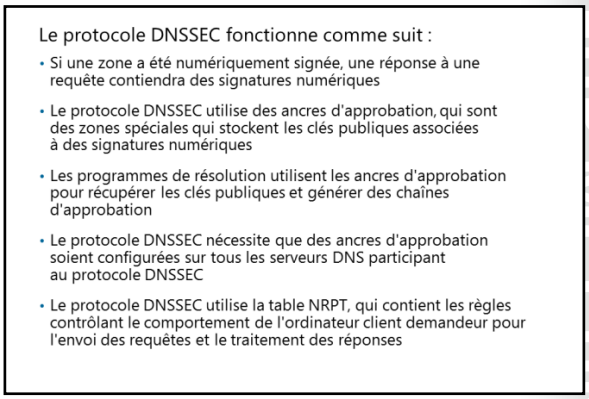
3. Redémarrez le service DNS pour appliquer les modifications.

DNSSEC

DNSSEC active une zone DNS et tous les enregistrements de la zone devant faire l'objet d'une signature cryptographique de telle sorte que les ordinateurs clients peuvent valider la réponse de DNS. Le DNS est souvent sujet à diverses attaques, telles que l'usurpation d'adresse et la falsification de cache. DNSSEC assure la protection contre ces menaces et fournit une infrastructure DNS plus sûre.

Fonctionnement de DNSSEC

Une méthode d'attaque courante consiste à intercepter et falsifier la réponse à une requête DNS d'une organisation. Si une personne malveillante peut modifier la réponse d'un serveur DNS ou envoyer une réponse falsifiée afin de diriger les ordinateurs clients vers ses propres serveurs, elle peut accéder à des informations sensibles. Tous les services qui s'appuient sur DNS pour la connexion initiale, tels que les serveurs Web d'e-commerce et les serveurs de messagerie, sont vulnérables. DNSSEC est conçu pour protéger les clients qui font des requêtes DNS en les empêchant d'accepter de fausses réponses DNS.



Quand un serveur DNS qui héberge une zone numériquement signée reçoit une requête, elle renvoie les signatures numériques avec les enregistrements demandés. Un résolveur ou un serveur différent peut obtenir la clé publique de la paire clé publique/clé privée d'une ancre d'approbation, puis confirmer que les réponses sont authentiques et n'ont pas été falsifiées. Pour ce faire, le résolveur ou le serveur doit être configuré avec une ancre d'approbation pour la zone signée ou pour un parent de la zone signée.

Ancres d'approbation

Une *ancre d'approbation* est une entité faisant autorité représentée par une clé publique. La zone TrustAnchors enregistre les clés publiques préconfigurées qui sont associées à une zone spécifique. Dans DNS, l'ancre d'approbation est l'enregistrement de ressource DNSKEY ou DS. Les ordinateurs clients utilisent ces enregistrements pour générer des chaînes d'approbation. Une ancre d'approbation de la zone doit être configurée sur chaque serveur DNS de domaine pour valider les réponses de cette zone signée. Si le serveur DNS est un contrôleur de domaine, les zones intégrées à Active Directory peuvent distribuer les ancres d'approbation.

Table de stratégie de résolution des noms

La table de stratégie de résolution des noms (NRPT) contient les règles qui contrôlent le comportement des clients DNS en ce qui concerne l'envoi de requêtes DNS et le traitement des réponses à ces requêtes. Par exemple, une règle DNSSEC invite l'ordinateur client à vérifier la validation de la réponse pour un suffixe de domaine DNS particulier. Il est recommandé d'utiliser la stratégie de groupe pour configurer le NRPT. En cas d'absence de NRPT, l'ordinateur client accepte des réponses sans les valider.

Déploiement de DNSSEC

Pour déployer DNSSEC :

1. Installez Windows Server 2012 dans l'environnement et attribuez le rôle DNS au serveur. En général, un contrôleur de domaine agit également en tant que serveur DNS. Cependant, ce n'est pas une obligation.
2. Signez la zone DNS à l'aide de l'Assistant Configuration de DNSSEC situé dans la console DNS.
3. Configurez les points de distribution d'ancres d'approbation.
4. Configurez le NRPT sur les ordinateurs clients.

Attribution du rôle de serveur DNS

Pour attribuer le rôle de serveur DNS, utilisez l'Assistant Ajout de rôles et de fonctionnalités à partir du tableau de bord du Gestionnaire de serveur. Vous pouvez également ajouter ce rôle lorsque vous ajoutez le rôle AD DS. Puis configurez les zones principales sur le serveur DNS. Une fois qu'une zone est signée, tous les nouveaux serveurs DNS ajoutés dans Windows Server 2012 reçoivent automatiquement les paramètres de DNSSEC.

Signature de la zone

Les options de signature suivantes sont disponibles :

- **Configurer les paramètres de signature de zone**. Cette option vous guide tout au long des étapes et vous permet de définir toutes les valeurs de clé de signature de clé (KSK) et de clé de signature de zone (ZSK).
- **Signer la zone avec les paramètres d'une zone existante**. Cette option vous permet de conserver les mêmes valeurs et options qu'une autre zone signée.
- **Utiliser les paramètres recommandés**. Cette l'option signe la zone à l'aide des valeurs par défaut.

 **Remarque :** Les signatures des zones peuvent également être effacées à l'aide de l'interface utilisateur de gestion DNSSEC.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des points de distribution d'ancres d'approbation

Si la zone est intégrée à Active Directory et que tous les contrôleurs de domaine exécutent Windows Server 2012, vous pouvez choisir de distribuer les ancres d'approbation à tous les serveurs de la forêt. Soyez prudent si vous faites ce choix, car l'Assistant active la validation DNSSEC. Si vous activez les ancres d'approbation de DNS sans effectuer un test minutieux, vous pourriez provoquer des pannes de DNS. Si des ancres d'approbation sont requises sur des ordinateurs qui ne sont pas joints au domaine, par exemple, un serveur DNS du réseau de périmètre (également appelé sous-réseau filtré), vous devez activer la substitution de clé automatisée.

Remarque : Une substitution de clé est l'acte de remplacer une paire de clés par une autre à la fin de la période de validité d'une clé.

Configuration de NRPT sur des ordinateurs clients

L'ordinateur client DNS exécute uniquement la validation DNSSEC sur les noms de domaine où l'ordinateur client DNS est configuré pour le faire par la table NRPT. Un ordinateur client exécutant Windows 7 prend en charge DNSSEC, mais n'exécute pas la validation. À la place, il compte sur le serveur DNS orienté sécurité pour exécuter la validation en son nom.

Nouvelles fonctionnalités de DNSSEC pour Windows Server 2012

Windows Server 2012 a simplifié l'implémentation de DNSSEC. Bien que DNSSEC soit pris en charge dans Windows Server 2008 R2, la majeure partie tâches de configuration et d'administration a été effectuée manuellement, et les zones ont été signées alors qu'elles étaient hors connexion.

Les améliorations du protocole DNSSEC pour Windows Server 2012 comprennent

- L'implémentation simplifiée du protocole DNSSEC
- Un Assistant Signature de zone DNSSEC qui vous guide pas à pas dans le processus de signature et de configuration des paramètres de signature pour les zones
- Les nouveaux enregistrements de ressources suivant
  - DNSKEY
  - DS
  - RRSIG
  - NSEC

Assistant Signature de zone DNSSEC

Windows Server 2012 inclut un Assistant Signature de zone DNSSEC pour simplifier les processus de configuration et de signature, et permettre la signature en ligne. L'Assistant vous permet de choisir les paramètres de signature de zone comme indiqué dans la rubrique précédente. Si vous choisissez de configurer les paramètres de signature de zone au lieu d'utiliser les paramètres d'une zone existante ou les valeurs par défaut, vous pouvez utiliser l'Assistant pour configurer des paramètres tels que :

- Options KSK
- Options ZSK
- Options de distribution d'ancres d'approbation
- Paramètres de signature et d'interrogation

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Nouveaux enregistrements de ressources

La validation des réponses DNS est effectuée en associant une paire de clés privée et publique (générée par l'administrateur) à une zone DNS et en définissant des enregistrements de ressources DNS supplémentaires pour signer et publier des clés. Les enregistrements de ressources distribuent la clé publique, tandis que la clé privée reste sur le serveur. Lorsque le client demande une validation, DNSSEC ajoute des données à la réponse qui permettent au client d'authentifier cette réponse.

Le tableau suivant décrit les nouveaux enregistrements de ressources dans Windows Server 2012.

Enregistrement de ressource	Rôle
DNSKEY	Cet enregistrement publie la clé publique de la zone. Il vérifie l'autorité d'une réponse par rapport à la clé privée conservée sur le serveur DNS. Ces clés requièrent le remplacement périodique par substitution de clé. Windows Server 2012 prend en charge les substitutions de clé automatisées. Chaque zone possède plusieurs enregistrements DNSKEY qui sont ensuite divisés en clés ZSK et clés KSK.
Delegation Signer (DS)	Il s'agit d'un enregistrement de délégation qui contient le hachage de la clé publique d'une zone enfant. Cet enregistrement est signé par la clé privée de la zone parente. Si une zone enfant d'une zone parente signée est également signée, les enregistrements DS de la zone enfant doivent être ajoutés manuellement à la zone parente afin de permettre la création d'une chaîne d'approbation.
Resource Record Signature (RRSIG)	Cet enregistrement contient une signature pour un jeu d'enregistrements DNS. Il permet de vérifier l'autorité d'une réponse.
Next Secure (NSEC)	Lorsque la réponse DNS ne contient aucune donnée à fournir au client, cet enregistrement authentifie le fait que l'hôte n'existe pas.
NSEC3	Cette version hachée de l'enregistrement NSEC est conçue pour empêcher les attaques alphabétiques en énumérant la zone.

Autres nouvelles améliorations

Les autres améliorations pour Windows Server 2012 comprennent :

- prise en charge des mises à jour dynamiques de DNS dans les zones signées DNSSEC ;
- distribution automatisée d'ancres d'approbation par AD DS ;
- interface de ligne de commande basée sur Windows PowerShell pour la gestion et les scripts.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration de DNSSEC

Dans cette démonstration, vous allez apprendre à utiliser l'Assistant Signature de zone dans la console DNS pour configurer DNSSEC.

Procédure de démonstration

Configurer DNSSEC

1. Connectez-vous à LON-DC1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Démarrez la console de gestion **DNS**.
3. Utilisez l'Assistant Signature de zone DNSSEC pour signer la zone Adatum.com.
4. Choisissez de personnaliser les paramètres de signature de zone.
5. Assurez-vous que le serveur DNS **LON-DC1 est le maître des clés**.
6. Ajoutez la **clé KSK** en acceptant les valeurs par défaut pour la nouvelle clé.
7. Ajoutez la **clé ZSK** en acceptant les valeurs par défaut pour la nouvelle clé.
8. Choisissez d'utiliser **NSCE3** avec les valeurs par défaut.
9. Ne choisissez pas d'activer la distribution des ancres d'approbation pour cette zone.
10. Acceptez les valeurs par défaut pour **signature** et **interrogation**.
11. Vérifiez que les enregistrements de ressource DNSKEY ont été créés dans la **zone Points d'approbation**.
12. Utilisez la console de gestion des stratégies de groupe (GPMC) pour configurer NRPT. Créez une règle qui active DNSSEC pour le suffixe Adatum.com et qui exige que les ordinateurs clients DNS vérifient que les données de nom et d'adresse sont validées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Implémentation de la réplication IPAM

Avec le développement d'IPv6 et le nombre accru de périphériques nécessitant des adresses IP, les réseaux sont devenus complexes et difficiles à gérer. Le maintien d'une liste actualisée d'adresses IP statiques ayant été émises a souvent été une tâche manuelle, sujette aux erreurs. Pour aider les organisations à gérer les adresses IP, Windows Server 2012 fournit l'outil IPAM.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire IPAM ;
- décrire l'architecture d'IPAM ;
- décrire les conditions requises pour l'implémentation d'IPAM ;
- expliquer comment gérer l'adressage IP à l'aide d'IPAM ;
- expliquer comment installer et configurer IPAM ;
- expliquer comment gérer et surveiller IPAM ;
- décrire les éléments à prendre en compte pour l'implémentation d'IPAM.

Qu'est-ce que IPAM ?

La gestion d'adresse IP est une tâche difficile dans de grands réseaux, parce que le suivi de l'utilisation d'adresse IP est en grande partie une opération manuelle. Windows Server 2012 présente IPAM, une infrastructure pour découvrir, auditer, surveiller l'utilisation et gérer l'espace d'adressage IP dans un réseau. IPAM active l'administration et la surveillance de DHCP et DNS, et fournit une vue complète des endroits où les adresses IP sont utilisées. IPAM collecte des informations auprès des contrôleurs de domaine et des serveurs NPS, puis les enregistre dans la base de données interne Windows.

La fonctionnalité IPAM simplifie la gestion des adresses IP dans les organisations avec des réseaux complexes en activant l'administration et la surveillance du DHCP et du DNS

Zone d'administration d'IP	Description
Planification	Réduit le temps et les dépenses consacrés au processus de planification lorsque le réseau fait l'objet de modifications
Gestion	Fournit un point de gestion unique et aide à optimiser l'utilisation et la planification des capacités pour le DHCP et le DNS
Suivi	Permet de suivre et de prévoir l'utilisation des adresses IP
Audit	Aide à respecter les exigences de conformité et fournit des rapports pour l'analyse des journaux et la gestion des changements

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

IPAM offre son aide dans les domaines de l'administration d'IP, comme illustré dans le tableau suivant.

Zone d'administration d'IP	Fonctions d'IPAM
Planification	Offre un ensemble d'outils permettant de réduire le temps et les dépenses consacrés au processus de planification lorsque le réseau fait l'objet de modifications.
Gestion	Fournit un point de gestion unique et aide à optimiser l'utilisation et la planification des capacités pour le DHCP et le DNS.
Suivi	Permet de suivre et de prévoir l'utilisation des adresses IP.
Audit	Aide à répondre aux exigences de conformité, telles que la Health Insurance Portability and Accountability Act (HIPAA) et la Sarbanes-Oxley Act de 2002, et fournit des rapports pour la gestion des analyses et des changements.

Caractéristiques d'IPAM

Les caractéristiques d'IPAM comprennent :

- Un serveur IPAM unique peut prendre en charge jusqu'à 150 serveurs DHCP et 500 serveurs DNS.
- Un serveur IPAM unique peut prendre en charge jusqu'à 6 000 étendues DHCP et 150 zones DNS.
- IPAM enregistre trois ans de données d'analyse (baux d'adresse IP, adresses hôtes MAC, ouverture de session de l'utilisateur et informations de fermeture de session) pour 100 000 utilisateurs dans une base de données interne Windows. Aucune stratégie de purge de base de données n'est fournie, et l'administrateur doit vider les données manuellement en fonction des besoins.
- IPAM prend en charge uniquement la base de données interne Windows. Aucune base de données externe n'est prise en charge.
- Les tendances d'utilisation des adresses IP sont fournies seulement pour IPv4.
- La prise en charge des réclamations liées aux adresses IP est fournie seulement pour IPv4.
- IPAM ne vérifie pas la compatibilité des adresses IP avec les routeurs et les commutateurs.

Avantages des services IPAM

Les avantages d'IPAM incluent les suivants :

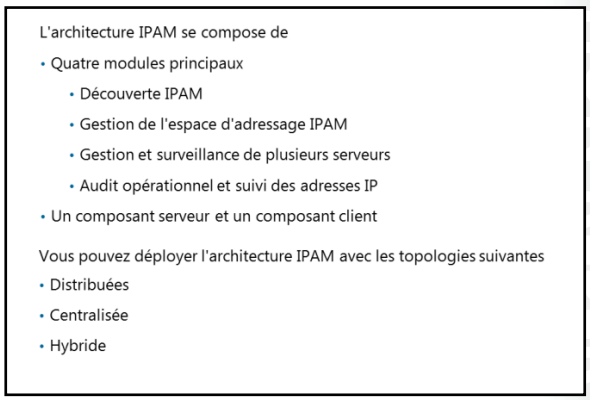
- planification et allocation de l'espace d'adressage IPv4 et IPv6 ;
- contrôle des statistiques et des tendances d'utilisation de l'espace d'adressage IP ;
- gestion de l'inventaire des IP statiques, gestion de la durée de vie, et création et suppression d'enregistrements DHCP et DNS ;
- contrôle du service et des zones des services DNS ;
- suivi des baux d'adresses IP et des événements d'ouverture de session ;
- contrôle d'accès basé sur les rôles (RBAC) ;
- prise en charge de l'administration à distance par RSAT.

Remarque : IPAM ne prend pas en charge la gestion et la configuration des éléments de réseau non-Microsoft.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Architecture du système IPAM

L'architecture d'IPAM se compose de quatre modules principaux, comme indiqué dans le tableau suivant.



Module	Description
Découverte IPAM	Vous pouvez utiliser AD DS pour découvrir les serveurs qui exécutent Windows Server 2008 et les systèmes d'exploitation Windows Server plus récents, et sur lesquels DNS, DHCP ou AD DS sont installés. Vous pouvez définir la portée de la découverte à un sous-ensemble de domaines dans la forêt. Vous pouvez également ajouter des serveurs manuellement.
Gestion de l'espace d'adressage IP	Vous pouvez utiliser ce module pour afficher, surveiller et gérer l'espace d'adressage IP. Vous pouvez émettre dynamiquement ou attribuer statiquement des adresses. Vous pouvez également suivre l'utilisation des adresses et détecter les étendues DHCP qui se chevauchent.
Gestion et surveillance de plusieurs serveurs	Vous pouvez gérer et surveiller plusieurs serveurs DHCP. Ceci permet d'exécuter des tâches sur plusieurs serveurs. Par exemple, vous pouvez configurer et modifier des propriétés et des étendues de DHCP, et suivre le statut de DHCP et l'utilisation des étendues. Vous pouvez également surveiller plusieurs serveurs DNS, et surveiller l'intégrité et le statut des zones DNS dans les serveurs DNS faisant autorité.
Audit opérationnel et suivi des adresses IP	Vous pouvez utiliser les outils d'audit pour suivre les éventuels problèmes de configuration. Vous pouvez également rassembler, gérer, et afficher les détails des modifications de configuration des serveurs DHCP gérés. Vous pouvez également collecter des informations de suivi auprès des journaux de bail DHCP, et collecter des informations sur les événements d'ouverture de session auprès de NPS et des contrôleurs de domaine.

Le serveur IPAM ne peut gérer qu'une seule forêt Active Directory. Par conséquent, vous pouvez déployer IPAM dans l'une de trois topologies suivantes :

- Distribuée. Vous déployez un serveur IPAM sur chaque site dans la forêt.
- Centralisée. Vous déployez un seul serveur IPAM dans la forêt.
- Hybride. Vous déployez un serveur IPAM central ainsi qu'un serveur IPAM dédié dans chaque site.

Remarque : Les serveurs IPAM ne communiquent pas entre eux ou ne partagent pas d'informations sur la base de données. Si vous déployez plusieurs serveurs IPAM, vous devez personnaliser l'étendue de la découverte de chaque serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

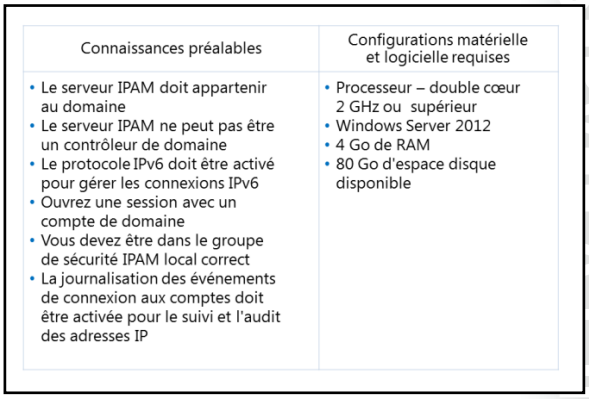
Un IPAM a deux composants principaux :

- Serveur IPAM. Le serveur IPAM exécute la collecte de données auprès des serveurs gérés. Il gère également la base de données interne Windows et fournit RBAC.
- Le client IPAM. Le client IPAM fournit l'interface utilisateur de l'ordinateur client. Il interagit également avec le serveur IPAM, et invoque Windows PowerShell pour exécuter les tâches de configuration de DHCP, la surveillance de DNS et la gestion à distance.

Conditions requises pour l'implémentation d'IPAM

Pour garantir une implémentation d'IPAM réussie, vous devez répondre à plusieurs conditions préalables :

- Le serveur IPAM doit être un membre du domaine, mais ne peut pas être un contrôleur de domaine.
- Le serveur IPAM devrait être un serveur dédié. N'installez pas d'autres rôles de réseau tels que DHCP ou DNS sur le même serveur.
- Pour gérer l'espace d'adressage IPv6, IPv6 doit être activé sur le serveur IPAM.



- Connectez-vous au serveur IPAM avec un compte de domaine, et non un compte local.
- Vous devez être un membre du groupe de sécurité locale IPAM correct sur le serveur IPAM.
- Activez la journalisation des événements d'ouverture de session de compte sur le contrôleur de domaine et les serveurs NPS pour les fonctionnalités de suivi et d'audit des adresses IP d'IPAM.

Configurations matérielles et logicielles d'IPAM requises :

Les configurations matérielles et logicielles requises pour IPAM sont les suivantes :

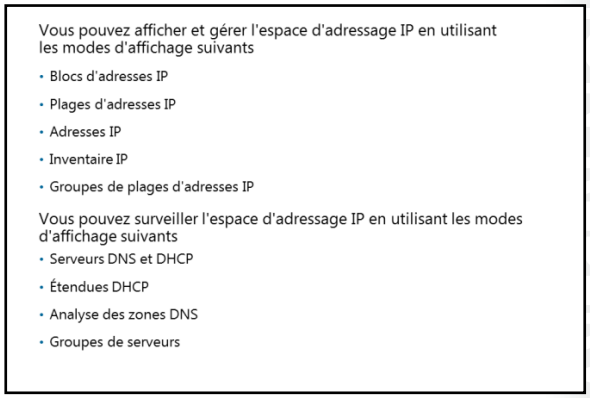
- processeur double cœur de 2,0 gigahertz (GHz) ou plus ;
- Système d'exploitation Windows Server 2012
- 4 gigaoctets (Go) de mémoire vive (RAM) ou plus ;
- 80 Go d'espace disponible sur le disque dur.

En plus des configurations requises précédemment indiquées, Windows Server 2008 et Windows Server 2008 R2 requièrent ce qui suit :

- Service Pack 2 (SP2) doit être installé sur Windows Server 2008.
- Microsoft® .NET Framework 4.0 doit être complètement installé.
- Windows Management Framework 3.0 Beta doit être installé (KB2506146).
- Pour Windows Server 2008 SP2, Windows Management Framework Core (KB968930) est également requis.
- La gestion à distance de Windows doit être activée.
- Vérifiez que des noms de principal du service (SPN) sont écrits.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion de l'adressage IP à l'aide d'IPAM



La gestion de l'espace d'adressage IP permet aux administrateurs de gérer, suivre, auditer et créer des rapports sur les espaces d'adressage IPv4 et IPv6 d'une organisation. La console de l'espace d'adressage IP d'IPAM fournit aux administrateurs des statistiques d'utilisation des adresses IP et des données d'historique des tendances pour leur permettre de prendre des décisions informées sur la planification des espaces d'adressage dynamique, statique et virtuel. Les tâches périodiques d'IPAM découvrent automatiquement les données relatives à l'espace d'adressage et à l'utilisation, comme configuré sur les serveurs DHCP gérés dans IPAM. Vous pouvez également importer des informations d'adresse IP à partir de fichiers .csv.

IPAM permet également aux administrateurs de détecter les plages d'adresses IP se chevauchant définies sur différents serveurs DHCP, de trouver des adresses IP libres dans une plage, de créer des réservations DHCP, et de créer des enregistrements DNS.

IPAM fournit un certain nombre de façons de filtrer l'affichage de l'espace d'adressage IP. Vous pouvez personnaliser la façon dont vous affichez et gérez l'espace d'adressage IP en utilisant l'un des modes d'affichage suivants :

- Blocs d'adresses IP
- Plages d'adresses IP
- Adresses IP
- Inventaire d'adresses IP
- Groupes de plages d'adresses IP

Blocs d'adresses IP

Les blocs d'adresses IP sont les entités au plus haut niveau au sein d'une organisation d'espace d'adressage IP. D'un point de vue conceptuel, un bloc d'IP est un sous-réseau IP marqué par une adresse IP de début et de fin, et est généralement attribué à une organisation par plusieurs registres Internet régionaux (RIR). Les administrateurs réseau utilisent les blocs d'adresses IP pour créer et allouer des plages d'adresses IP au DHCP. Ils peuvent ajouter, importer, modifier et supprimer des blocs d'adresses IP. IPAM mappe automatiquement les plages d'adresses IP au bloc d'adresses IP approprié selon les limites de la plage. Vous pouvez ajouter et importer des blocs d'adresses IP dans la console IPAM.

Plages d'adresses IP

Les plages d'adresses IP sont les entités d'espace d'adressage IP d'un niveau hiérarchique supérieur aux blocs d'adresses IP. Sur un plan conceptuel, une plage d'adresses IP est un sous-réseau IP marqué par une adresse IP de début et de fin, et correspond en général à une étendue DHCP, ou à une plage d'adresses ou pool d'adresses IPv4 ou IPv6 statiques utilisées pour attribuer des adresses aux hôtes. Une plage d'adresses IP est seulement identifiable par la valeur des options obligatoires **Géré par le service** et **Instance du service**, qui aident IPAM à gérer et maintenir les plages d'adresses IP qui se chevauchent ou en double depuis la même console. Vous pouvez ajouter ou importer des plages d'adresses IP depuis la console IPAM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Adresses IP

Les adresses IP sont les adresses qui composent la plage d'adresses IP. IPAM active la gestion de bout en bout du cycle de vie des adresses IPv4 et IPv6, y compris la synchronisation des enregistrements avec les serveurs DHCP et DNS. IPAM mappe automatiquement une adresse à la plage appropriée selon l'adresse de début et de fin de la plage. Une adresse IP est seulement identifiable par la valeur des options obligatoires **Géré par le service** et **Instance du service**, qui aident IPAM à gérer et maintenir les adresses IP qui se chevauchent ou en double depuis la même console. Vous pouvez ajouter ou importer des adresses IP depuis la console IPAM.

Inventaire d'adresses IP

Dans l'affichage de l'inventaire d'adresses IP, vous pouvez afficher une liste de toutes les adresses IP dans l'entreprise avec leurs noms et types de périphérique. L'inventaire d'adresses IP est un groupe logique défini par l'option **Type de périphérique** dans l'affichage des adresses IP. Ces groupes vous permettent de personnaliser la façon dont votre espace d'adressage s'affiche pour gérer et suivre l'utilisation des IP. Vous pouvez ajouter ou importer des adresses IP depuis la console IPAM. Par exemple, vous pourriez ajouter l'adresse IP d'une imprimante ou d'un routeur, associer l'adresse IP au type de périphérique correspondant à l'imprimante ou au routeur, puis afficher votre inventaire d'IP filtré selon le type de périphérique sélectionné.

Groupes de plages d'adresses IP

IPAM vous permet d'organiser des plages d'adresses IP dans des groupes logiques. Par exemple, vous pourriez organiser des plages d'adresses IP géographiquement ou par division d'entreprise. Des groupes logiques sont définis en sélectionnant les critères de regroupement des champs personnalisés intégrés ou définis par l'utilisateur.

Contrôle et gestion

IPAM active la surveillance automatisée et périodique de service des serveurs DHCP et DNS dans une forêt. La surveillance et la gestion est organisée dans modes d'affichage répertoriés dans le tableau suivant.

Vue	Description
Serveurs DNS et DHCP	Par défaut, les serveurs DHCP et DNS gérés sont réorganisés par leur interface réseau dans des sous-réseaux /16 pour IPv4 et des sous-réseaux /48 pour IPv6. Vous pouvez sélectionner la vue pour afficher seulement les propriétés d'étendue de DHCP, seulement les propriétés de serveur DNS, ou les deux.
Étendues DHCP	L'affichage de l'étendue DHCP active la surveillance de l'utilisation de l'étendue. Des statistiques d'utilisation sont collectées périodiquement et automatiquement auprès d'un serveur DHCP géré. Vous pouvez suivre les propriétés d'étendue importantes telles que : **Nom**, **ID**, **Préfixe Longueur** et **État**.
Analyse des zones DNS	La surveillance de zone est activée pour les zones de recherche directe et inversée. L'état de la zone dépend des événements collectés par IPAM. L'état de chaque zone est résumé.
Groupes de serveurs	Vous pouvez organiser vos serveurs DHCP et DNS gérés dans des groupes logiques. Par exemple, vous pourriez organiser les serveurs par unité d'organisation ou zone géographique. Les groupes sont définis en sélectionnant les critères de regroupement des champs personnalisés intégrés ou définis par l'utilisateur.

Démonstration : Installation et configuration du système IPAM

Au cours de cette démonstration, vous allez apprendre à installer et configurer la gestion IPAM.

Procédure de démonstration

Installer les services IPAM

1. Connectez-vous à LON-SVR2 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, ajoutez la fonctionnalité IPAM et toutes les fonctions secondaires requises.

Configurer les services IPAM

1. Dans le volet Vue d'ensemble d'IPAM, configurez le serveur IPAM en utilisant la stratégie de groupe.
2. Entrez **IPAM** comme préfixe de nom d'objet de stratégie de groupe et approvisionnez IPAM. La configuration prendra quelques instants.
3. Dans le volet Vue d'ensemble d'IPAM, configurez la découverte de serveurs pour le domaine Adatum.
4. Dans le volet Vue d'ensemble d'IPAM, démarrez le processus de découverte de serveurs. Le processus de découverte peut durer 5 à 10 minutes. La barre jaune indique quand la découverte est terminée.
5. Dans le volet Vue d'ensemble d'IPAM, ajoutez les serveurs à gérer.
6. Vérifiez que l'accès à IPAM est actuellement bloqué.
7. Utilisez Windows PowerShell pour accorder au serveur IPAM l'autorisation de gérer LON-DC1 à l'aide de la commande suivante :

```
Invoke-IpamGpoProvisioning –Domain Adatum.com –GpoPrefixName IPAM –IpamServerFqdn
LON-SVR2.adatum.com –DelegatedGpoUser Administrateur
```

8. Définissez l'état de la facilité de gestion sur **Géré**.
9. Basculez vers **LON-DC1**.
10. Forcez la mise à jour de la stratégie de groupe.
11. Rebasculez vers **LON-SVR2** et actualisez la vue **IPv4**. Le processus de découverte peut durer 5 à 10 minutes.
12. Dans le volet Présentation d'IPAM, récupérez les données du serveur géré.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion et analyse d'IPAM

La fonctionnalité de gestion de l'espace d'adressage d'IPAM vous permet d'afficher, surveiller et gérer efficacement l'espace d'adressage IP sur le réseau. La gestion de l'espace d'adressage prend en charge les adresses IPv4 publiques et privées, et les adresses IPv6 globales et de monodiffusion. L'affichage des serveurs DNS et DHCP vous permet d'afficher et de surveiller l'intégrité et la configuration de tous les serveurs DNS et DHCP qui sont gérés par IPAM. IPAM utilise des tâches planifiées pour collecter périodiquement des données auprès des serveurs gérés. Vous pouvez également récupérer des données à la demande à l'aide de l'option **Récupérer toutes les données de serveur**.

Avec la fonctionnalité IPAM, vous pouvez
- Surveiller l'utilisation de l'espace d'adressage IP
- Surveiller l'intégrité du DNS et DHCP
- Configurer de nombreuses valeurs et propriétés DHCP à partir de la console IPAM
- Utiliser le catalogue d'événements pour afficher un référentiel centralisé pour toutes les modifications de configuration

Analyse de l'utilisation

Les données d'utilisation sont conservées pour les plages d'adresses IP, les blocs d'adresses IP et les groupes de plages IP dans IPAM. Vous pouvez configurer des seuils pour le pourcentage de l'espace d'adressage IP utilisé, puis utiliser ces seuils pour déterminer la sous-exploitation et la sur-utilisation.

Vous pouvez créer et générer des rapports sur les tendances d'utilisation des plages, des blocs et des groupes de plages d'adresses IPv4. La fenêtre des tendances d'utilisation vous permet d'afficher les tendances sur une période définie (tendances quotidiennes, hebdomadaires, mensuelles ou annuelles), ou d'afficher les tendances correspondant à des plages de dates personnalisées. Les données d'utilisation des étendues DHCP gérées sont découvertes automatiquement et accessibles à la consultation.

Surveillance de DHCP et DNS

Avec IPAM, vous pouvez surveiller les serveurs DHCP et DNS depuis n'importe quel emplacement physique de l'entreprise. L'un des principaux avantages d'IPAM est sa capacité à gérer simultanément plusieurs serveurs DHCP ou étendues DHCP réparties sur un ou plusieurs serveurs DHCP.

L'affichage de surveillance d'IPAM vous permet d'afficher l'état et l'intégrité d'une sélection de serveurs Microsoft DNS et DHCP depuis une console unique. L'affichage de surveillance d'IPAM affiche l'état d'intégrité de base des serveurs et les événements de configuration récents qui se sont produits sur ces serveurs. L'affichage de surveillance vous permet également d'organiser les serveurs gérés dans des groupes de serveurs logiques.

Pour les serveurs DHCP, l'affichage des serveurs vous permet de suivre divers paramètres de serveur, les options de serveur, le nombre d'étendues et le nombre de baux actifs configurés sur le serveur. Pour les serveurs DNS, ce mode d'affichage vous permet de suivre toutes les zones configurées sur le serveur, ainsi que les informations sur le type de zone. Ce mode d'affichage vous permet également d'afficher le nombre total de zones configurées sur le serveur, et l'état de l'intégrité générale de la zone provenant de l'état des zones individuelles sur le serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion du serveur DHCP

À partir de la console IPAM, vous pouvez gérer les serveurs DHCP et exécuter les actions suivantes :

- Modifiez les propriétés de serveur DHCP.
- Modifiez les options de serveur DHCP.
- Créez des étendues DHCP.
- Configurez des options et valeurs prédéfinies.
- Configurez la classe d'utilisateur sur plusieurs serveurs simultanément.
- Créez et modifiez les classes d'utilisateur nouvelles et existantes sur plusieurs serveurs simultanément.
- Configurez la classe de fournisseur sur plusieurs serveurs simultanément.
- Démarrez la console de gestion pour un serveur DHCP sélectionné.
- Récupérez les données de serveur de plusieurs serveurs.

Gestion de serveur DNS

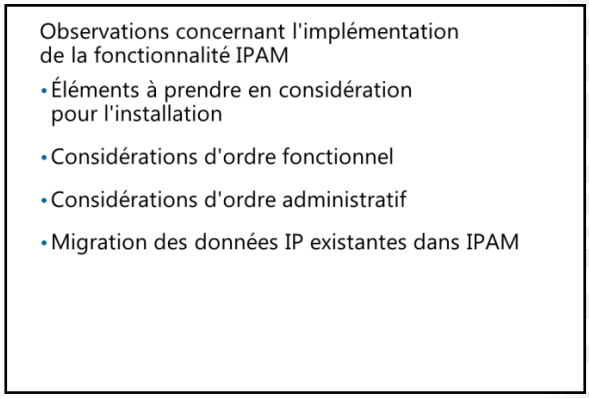
Vous pouvez mettre en marche la console de gestion DNS pour n'importe quel serveur DNS géré, à partir d'une console centrale dans le serveur IPAM. Une fois la console de gestion DNS mise en marche, vous pouvez récupérer des données de serveur de l'ensemble de serveurs sélectionnés. L'affichage Analyse des zones DNS affiche toutes les zones de recherche directe et de recherche inversée sur tous les serveurs DNS qu'IPAM gère actuellement. Pour les zones de recherche directe, IPAM affiche également tous les serveurs qui hébergent la zone et l'intégrité globale de la zone sur tous ces serveurs et les propriétés de zone.

Le catalogue d'événements

Le catalogue d'événements d'IPAM fournit un référentiel centralisé pour auditer toutes les modifications de configuration qui sont exécutées sur les serveurs DHCP gérés depuis une console de gestion IPAM unique. La console d'événements de configuration d'IPAM rassemble tous les événements de configuration. Ces catalogues d'événements de configuration vous permettent d'afficher, d'interroger et de générer des rapports sur les modifications de configuration consolidées, ainsi que des détails spécifiques à chaque enregistrement.

Éléments à prendre en compte pour implémenter IPAM

IPAM est une technologie sans agent qui utilise des protocoles de gestion à distance de Windows pour gérer, surveiller et collecter des données auprès des serveurs distribués dans l'environnement. Vous devriez ainsi prendre conscience de certains éléments à prendre en compte pour l'implémentation.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en considération pour l'installation

Bien qu'IPAM soit relativement simple à installer, vous devez prendre en compte certains éléments :

- IPAM ne doit pas être installé sur un contrôleur de domaine, un serveur DHCP ou un serveur DNS.
- L'assistant d'installation dans le Gestionnaire de serveur installe automatiquement les fonctionnalités requises pour prendre en charge IPAM. Il n'y a aucune étape supplémentaire requise de l'administrateur.
- Le client IPAM est installé automatiquement sur Windows Server 2012 avec le serveur IPAM, mais vous pouvez désinstaller le client séparément.
- Vous pouvez désinstaller IPAM à l'aide du Gestionnaire de serveur. Les dépendances, groupes de sécurité locaux et tâches planifiées seront tous supprimés. La base de données IPAM sera détachée de la base de données interne Windows.

Considérations d'ordre fonctionnel

Tenez compte des caractéristiques fonctionnelles d'IPAM suivantes :

- IPAM ne prend pas en charge plusieurs topologies de forêt.
- IPAM peut seulement utiliser la base de données interne Windows ; il ne peut utiliser aucun autre type de base de données.
- Le serveur IPAM doit collecter des informations de bail DHCP pour activer le suivi d'adresse. Assurez-vous que la taille de fichier du journal d'audit de DHCP est configurée de sorte à être assez grande pour contenir les événements d'audit de la journée entière.
- Pour les contrôleurs de domaine et les serveurs de stratégie réseau, activez les événements requis pour la journalisation. Vous pouvez utiliser les paramètres de sécurité de la Stratégie de groupe pour exécuter cette tâche.

Considérations d'ordre administratif

Les administrateurs de domaine et d'entreprise ont un accès complet à l'administration d'IPAM. Vous pouvez déléguer des fonctions administratives à d'autres utilisateurs ou groupes à l'aide des groupes de sécurité IPAM. La procédure d'installation crée les groupes de sécurité locaux (qui n'ont aucun membre par défaut) sur le serveur IPAM. Les groupes de sécurité locaux fournissent les autorisations qui sont requises pour administrer et utiliser les différents services qu'IPAM utilise.

L'installation d'IPAM crée automatiquement les groupes d'utilisateurs locaux indiqués dans le tableau suivant.

Groupe	Description
Utilisateurs IPAM	Les membres de ce groupe peuvent afficher toutes les informations dans l'inventaire de serveurs IPAM, l'espace d'adressage IP, et les consoles de gestion de serveur IPAM. Ils peuvent afficher les événements opérationnels d'IPAM et du serveur DHCP, mais ils ne peuvent pas afficher les informations de suivi d'adresse IP.
Administrateurs IPAM MSM	Les membres de ce groupe ont tous les privilèges du Groupe d'utilisateurs IPAM, et peuvent effectuer des tâches de surveillance et de gestion d'IPAM.

(suite)

Groupe	Description
Administrateurs IPAM ASM.	Les membres de ce groupe ont tous les privilèges du Groupe d'utilisateurs IPAM et peuvent effectuer des tâches liées à l'espace d'adressage IP d'IPAM.
Administrateurs d'audit IPAM IP	Les membres de ce groupe ont tous les privilèges de Groupe d'utilisateurs IPAM et peuvent afficher les informations de suivi d'adresse IP.
Administrateurs IPAM	Les membres de ce groupe peuvent afficher toutes les informations d'IPAM et effectuer toutes les tâches IPAM.

Migration des données IP existantes dans IPAM

De nombreuses organisations utilisent les feuilles de calcul Microsoft Office Excel® pour documenter l'allocation de l'espace d'adressage IP des adresses statiques et des périphériques réseau. Étant donné que vous devez mettre ces feuilles de calcul à jour manuellement, elles sont sujettes aux erreurs. Vous pouvez migrer les données existantes de ces feuilles de calcul dans IPAM en convertissant les feuilles de calcul en fichiers .csv, puis en important les informations dans IPAM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation des services réseau avancés

Scénario

La société A. Datum s'est développée rapidement au cours des dernières années. La société a déployé plusieurs nouvelles filiales et a sensiblement augmenté le nombre d'utilisateurs dans l'organisation. En outre, elle a augmenté le nombre d'organisations partenaires et de clients qui accèdent aux sites Web et aux applications A. Datum. En raison de cette expansion, la complexité de l'infrastructure réseau a augmenté, et l'organisation doit maintenant accorder plus d'importance à la sécurité au niveau du réseau.

En tant que l'un des principaux administrateurs réseau chez A. Datum, vous êtes chargé de l'implémentation de certaines fonctionnalités avancées dans Windows Server 2012 pour gérer l'infrastructure réseau. Vous devez implémenter de nouvelles fonctionnalités dans DHCP et DNS, avec pour but premier de fournir des niveaux plus élevés de disponibilité tout en augmentant la sécurité de ces services. Vous devez également implémenter IPAM de sorte à pouvoir simplifier et centraliser la gestion de l'utilisation et de la configuration des adresses IP dans un réseau de plus en plus complexe.

Objectifs

- Configurer les paramètres DHCP avancés
- configurer les paramètres DNS avancés ;
- Configurer la gestion des adresses IP

Configuration de l'atelier pratique

Durée approximative : 70 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-SVR2** **22412B-LON-CL1**
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
    - Nom d'utilisateur : **ADATUM\Administrateur**
    - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22412B-LON-SVR1** et **22412B-LON-SVR2**. Ne démarrez pas **22412B-LON-CL1** tant que vous n'avez pas été invité à le faire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration des paramètres avancés du protocole DHCP (Dynamic Host Configuration Protocol)

Scénario

Avec l'expansion du réseau, et les exigences de sécurité et de disponibilité accrues dans la société A. Datum, vous devez implémenter quelques fonctionnalités DHCP supplémentaires. En raison de la récente expansion de l'entreprise, l'étendue DHCP du bureau principal est presque totalement utilisée, vous devez ainsi configurer une étendue globale. En outre, vous devez configurer la protection de nom DHCP et le basculement DHCP.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer une étendue globale
2. Configurer la protection de nom DHCP
3. Configurer et vérifier le basculement DHCP

▶ Tâche 1 : Configurer une étendue globale

1. Sur LON-DC1, configurez une étendue nommée **Etendue1**, avec une plage **192.168.0.50 – 192.168.0.100**, et avec les paramètres suivants :
   - Masque de sous-réseau : **255.255.255.0**
   - Routeur : **192.168.0.1**
   - Suffixe DNS : **Adatum.com**
   - Choisir d'activer l'entendue plus tard
2. Configurez une deuxième étendue nommée **Scope2**, avec une plage **192.168.1.50 – 192.168.1.100** et avec les paramètres suivants :
   - Masque de sous-réseau : **255.255.255.0**
   - Routeur : **192.168.1.1**
   - Suffixe DNS : **Adatum.com**
   - Choisir d'activer l'entendue plus tard
3. Créez une étendue globale appelée **AdatumSuper** qui compte **Etendue1** et **Etendue2** parmi ses membres.
4. Activez l'étendue globale AdatumSuper.

▶ Tâche 2 : Configurer la protection de nom DHCP

- Basculez vers la console DHCP sur LON-DC1 et activez la **Protection de nom DHCP** pour le nœud IPv4.

▶ Tâche 3 : Configurer et vérifier le basculement DHCP

1. Sur LON-SVR1, mettez en marche la console **DHCP** et observez l'état actuel de DHCP. Notez que le serveur est autorisé, mais qu'aucune étendue n'est configurée.
2. Sur LON-DC1, dans la console DHCP, lancez l'**Assistant Configuration du basculement**.

3. Configurez la réplication du basculement avec les paramètres suivants :
   - Serveur partenaire : **172.16.0.21**
   - Nom de la relation : **Adatum**
   - Délai de transition maximal du client (MCLT) : **15 minutes**
   - Mode : **Équilibrage de charge**
   - Pourcentage d'équilibrage de charge : **50%**
   - Intervalle de basculement d'état : **60 minutes**
   - Secret d'authentification des messages partagé : **Pa$$w0rd**
4. Exécutez l'Assistant Configuration du basculement.
5. Sur LON-SVR1, actualisez le nœud **IPv4**. Remarquez que le nœud IPv4 est actif et que l'étendue Adatum est configurée.
6. Démarrez **22412B-LON-CL1**, et connectez-vous en tant qu'**ADATUM\Administrateur**.
7. Configurez LON-CL1 pour obtenir une adresse IP du serveur DHCP.
8. Ouvrez une fenêtre d'invite de commandes et enregistrez l'adresse IP.
9. Basculez vers **LON-DC1** et arrêtez le service du serveur DHCP.
10. Rebasculez vers **LON-CL1** et renouvelez l'adresse IP.
11. Arrêtez le serveur LON-SVR1.
12. Sur LON-DC1, dans la console LON-SVR1, démarrez le service de serveur DHCP.
13. Fermez la console Services.

Résultats : À l'issue de cet exercice, vous aurez configuré une étendue globale, une protection de nom DHCP, et configuré et vérifié le basculement DHCP.

Exercice 2 : Configuration des paramètres DNS avancés

Scénario

Pour augmenter le niveau de sécurité des zones DNS chez A. Datum, vous devez configurer les paramètres de sécurité DNS tels que DNSSEC, pool de sockets DNS et verrouillage de cache. A. Datum entretient une relation professionnelle avec Contoso, Ltd, et hébergera la zone DNS Contoso.com. Les clients d'A. Datum utilisent une application qui accède à un serveur nommé App1 dans la zone Contoso.com à l'aide de son nom NetBIOS. Vous devez vérifier que ces applications peuvent résoudre correctement les noms des serveurs requis. Vous utiliserez une zone GlobalNames pour accomplir ceci.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer DNSSEC
2. Configurer le pool de sockets DNS
3. Configurer le verrouillage de cache DNS
4. Configurer une zone GlobalNames

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer DNSSEC

1. Sur VAN-DC1, démarrez le **Gestionnaire DNS**.
2. Utilisez l'Assistant Signature de zone DNSSEC pour signer la zone **Adatum.com**.
3. Choisissez de personnaliser les paramètres de signature de zone.
4. Assurez-vous que le serveur DNS **LON-DC1** est le maître des clés.
5. Ajoutez la **clé KSK** en acceptant les valeurs par défaut pour la nouvelle clé.
6. Ajoutez la **clé ZSK** en acceptant les valeurs par défaut pour la nouvelle clé.
7. Choisissez d'utiliser **NSCE3** avec les valeurs par défaut.
8. Ne choisissez pas d'activer la distribution des ancres d'approbation pour cette zone.
9. Acceptez les valeurs par défaut pour **signature et interrogation**.
10. Vérifiez que les enregistrements de ressource DNSKEY ont été créés dans la **zone Points d'approbation**.
11. Réduisez la console DNS en icône.
12. Utilisez la Console de gestion des stratégies de groupe, dans l'objet par défaut de stratégie de domaine, pour configurer la table de stratégie de résolution des noms.
13. Créez une règle qui active DNSSEC pour le suffixe Adatum.com et qui exige que les ordinateurs clients DNS vérifient que les données de nom et d'adresse ont été validées.

▶ Tâche 2 : Configurer le pool de sockets DNS

1. Sur LON-DC1, démarrez **Windows PowerShell**.
2. Exécutez la commande suivante pour afficher la taille actuelle du pool de sockets :

```
Get-DNSServer
```

3. Exécutez la commande suivante pour modifier la taille du pool de sockets pour 3 000 :

```
dnscmd /config /socketpoolsize 3000
```

4. Redémarrez le service DNS.
5. Exécutez la commande suivante pour confirmer la nouvelle taille du pool de sockets :

```
Get-DnsServer
```

▶ Tâche 3 : Configurer le verrouillage de cache DNS

1. Exécutez la commande suivante pour afficher la taille actuelle du verrouillage de cache :

```
Get-DnsServer
```

2. Exécutez la commande suivante pour modifier la valeur de verrouillage de cache à 75 pour cent :

```
Set-DnsServerCache –LockingPercent 75
```

3. Redémarrez le service DNS.
4. Exécutez la commande suivante pour confirmer la nouvelle valeur du verrouillage de cache :

```
Get-DnsServer
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer une zone GlobalNames

1. Créez une zone de recherche directe intégrée à Active Directory nommée **Contoso.com** en exécutant la commande suivante :

```
Add-DnsServerPrimaryZone –Name Contoso.com –ReplicationScope Forest
```

2. Exécutez la commande suivante pour activer la prise en charge des zones GlobalName :

```
Set-DnsServerGlobalNameZone –AlwaysQueryServer $true
```

3. Créez une zone de recherche directe intégrée à Active Directory nommée **GlobalNames** en exécutant la commande suivante :

```
Add-DnsServerPrimaryZone –Name GlobalNames –ReplicationScope Forest
```

4. Ouvrez la console du Gestionnaire DNS et ajoutez un nouvel enregistrement d'hôte au domaine Contoso.com nommé **App1** avec l'adresse IP **192.168.1.200**.
5. Dans la zone GlobalNames, créez un nouvel alias nommé **App1** en utilisant le nom de domaine complet **App1.Contoso.com**.
6. Fermez le Gestionnaire DNS et fermez l'invite de commandes.

Résultats : À l'issue de cet exercice, vous aurez configuré DNSSEC, le pool de sockets DNS, le verrouillage de cache DNS et la zone GlobalName.

Exercice 3 : Configuration de IPAM

Scénario

La société A. Datum évalue des solutions pour simplifier la gestion des adresses IP. Depuis l'implémentation de Windows Server 2012, vous avez décidé d'implémenter IPAM.

Les tâches principales de cet exercice sont les suivantes :

1. Installer la fonctionnalité IPAM
2. Configurer des objets de stratégie de groupe en relation avec IPAM
3. Configurer la découverte de serveurs d'administration d'IP
4. Configurer des serveurs gérés
5. Configurer et vérifier une nouvelle étendue DHCP avec IPAM
6. Configurer des blocs d'adresses IP, enregistrer des adresses IP et créer des réservations DHCP et des enregistrements DNS

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Installer la fonctionnalité IPAM

- Sur LON-SVR2, installez la fonctionnalité **Serveur de gestion des adresses IP (IPAM)** à l'aide de l'Assistant Ajout de rôles et de fonctionnalités dans le Gestionnaire de serveur.

▶ Tâche 2 : Configurer des objets de stratégie de groupe en relation avec IPAM

1. Sur LON-SVR2, dans le Gestionnaire de serveur, dans le volet Vue d'ensemble d'IPAM, configurez le serveur IPAM à l'aide de la stratégie de groupe.
2. Entrez **IPAM** comme préfixe du nom d'objet de stratégie de groupe, et configurez IPAM à l'aide de l'Assistant Configuration d'IPAM.

▶ Tâche 3 : Configurer la découverte de serveurs d'administration d'IP

1. Dans le volet Vue d'ensemble d'IPAM, configurez la découverte de serveurs pour le domaine Adatum.
2. Dans le volet Vue d'ensemble d'IPAM, démarrez le processus de découverte de serveurs. Le processus de découverte peut durer 5 à 10 minutes. La barre jaune indique quand la découverte est terminée.

▶ Tâche 4 : Configurer des serveurs gérés

1. Dans le volet Vue d'ensemble d'IPAM, ajoutez les serveurs que vous devez gérer. Vérifiez que l'accès à IPAM est actuellement bloqué.
2. Utilisez Windows PowerShell pour accorder au serveur IPAM l'autorisation de gérer LON-DC1 en exécutant la commande suivante :

```
Invoke-IpamGpoProvisioning –Domain Adatum.com –GpoPrefixName IPAM –IpamServerFqdn
LON-SVR2.adatum.com –DelegatedGpoUser Administrateur
```

3. Définissez l'état de la facilité de gestion sur **Géré**.
4. Basculez vers **LON-DC1** et forcez la mise à jour de la Stratégie de groupe à l'aide de **gpupdate /force**.
5. Revenez à LON-SVR2 et actualisez l'état d'accès au serveur pour LON-DC1 et l'affichage de console du Gestionnaire de serveur. La modification de l'état peut prendre jusqu'à 10 minutes. Au besoin, répétez les deux tâches d'actualisation comme nécessaire jusqu'à ce qu'une coche verte s'affiche à côté de LON-DC1 et que l'accès à IPAM affiche l'état **Débloqué**.
6. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Récupérer les données des serveurs gérés**.

▶ Tâche 5 : Configurer et vérifier une nouvelle étendue DHCP avec IPAM

1. Sur LON-SVR2, utilisez IPAM pour créer une nouvelle étendue DHCP avec les paramètres suivants :
   - Adresse de début d'étendue : **10.0.0.50**
   - Adresse de fin d'étendue : **10.0.0.100**
   - Masque de sous-réseau : **255.0.0.0**
   - Passerelle par défaut : **10.0.0.1**
2. Sur LON-DC1, vérifiez l'étendue dans le MMC de DHCP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UTILISATEUR

▶ Tâche 6 : Configurer des blocs d'adresses IP, enregistrer des adresses IP et créer des réservations DHCP et des enregistrements DNS

1. Sur LON-SVR2, ajoutez un bloc d'adresses IP dans la console IPAM avec les paramètres suivants :
   - ID réseau : **172.16.0.0**
   - Longueur du préfixe : **16**
   - Description : **Siège social**
2. Ajoutez des adresses IP pour le routeur de réseau à l'inventaire d'adresses IP avec les paramètres suivants :
   - Adresse IP : **172.16.0.1**
   - Adresse MAC : **112233445566**
   - Type de périphérique : **Routeurs**
   - Description : **Routeur de siège social**
3. Utilisez la console IPAM pour créer une réservation DHCP comme suit :
   - Adresse IP : **172.16.0.10**
   - Adresse MAC : **223344556677**
   - Type de périphérique : **Hôte**
   - Nom du serveur de réservations : **LON-DC1.Adatum.com**
   - Nom de réservation : **Webserver**
   - Type de réservation : **Les deux**
4. Utilisez la console IPAM pour créer l'enregistrement d'hôte DNS comme suit :
   - Nom de l'unité : **Webserver**
   - Zone de recherche directe : **Adatum.com**
   - Serveur principal de recherche directe : **LON-DC1.adatum.com**
5. Cliquez avec le bouton droit sur l'entrée **IPv4** et créez la réservation DHCP et l'enregistrement d'hôte DNS.
6. Sur LON-DC1, ouvrez la console **DHCP** et confirmez que la réservation a été créée dans l'étendue 172.16.0.0.
7. Sur LON-DC1, ouvrez la console du **Gestionnaire DNS** et confirmez que l'enregistrement d'hôte DNS a été créé.

Résultats : À l'issue de cet exercice, vous aurez installé IPAM et configuré IPAM avec des objets de stratégie de groupe en relation avec IPAM, la découverte de serveurs d'administration d'IP, des serveurs gérés, une nouvelle étendue DHCP, des blocs d'adresses IP, des adresses IP, des réservations DHCP et des enregistrements DNS.

▶ Pour préparer le module suivant

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-SVR2** et **22412B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée :

- Implémentez le basculement DHCP pour vous assurer que les ordinateurs clients peuvent continuer à recevoir les informations de configuration IP en cas de défaillance du serveur.
- Assurez-vous qu'au moins deux serveurs DNS hébergent chaque zone.
- Utilisez IPAM pour contrôler la distribution d'adresses IP et les affectations d'adresses statiques.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les utilisateurs ne peuvent plus accéder au site Web d'un fournisseur auquel ils ont déjà pu accéder.	
Les serveurs gérés ne peuvent pas se connecter au serveur IPAM.	

Questions de contrôle des acquis

Question : Quel est l'un des inconvénients liés à l'utilisation d'IPAM ?

Problèmes réels et scénarios

Question : Certains clients réseau reçoivent une configuration DHCP incorrecte. Quel outil devriez-vous utiliser pour commencer le processus de résolution des problèmes ?

Question : Quelles sont les causes possibles des configurations incorrectes ?

Outils

Outil	Utilisation	Emplacement
Dnscmd	Configurer tous les aspects de gestion de DNS	%systemroot%\System32\dnscmd.exe
Console DHCP	Contrôler tous les aspects de gestion de DHCP d'une interface utilisateur	%systemroot%\System32\dhcpmgmt.msc
Console DNS	Contrôler tous les aspects de gestion de DNS d'une interface utilisateur	%systemroot%\System32\dnsmgmt.msc
Console de gestion des services Internet (IPAM)	Contrôler tous les aspects de gestion d'IPAM	Gestionnaire de serveur

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2

Implémentation des services de fichiers avancés

Table des matières :

Vue d'ensemble du module **2-1**

Leçon 1 : Configuration du stockage iSCSI **2-2**

Leçon 2 : Configuration de la fonctionnalité BranchCache **2-10**

Leçon 3 : Optimisation de l'utilisation du stockage **2-19**

Atelier pratique A : Implémentation des services de fichiers avancés **2-26**

Atelier pratique B : Implémentation de la fonctionnalité BranchCache **2-33**

Contrôle des acquis et éléments à retenir **2-39**

Vue d'ensemble du module

Les configurations d'espace de stockage requises ont évolué depuis la création des partages de fichiers basés sur un serveur. Les systèmes d'exploitation Windows Server® 2012 et Windows® 8 comprennent deux nouvelles fonctionnalités (la déduplication des données et les espaces de stockage) conçues pour réduire l'espace disque requis et gérer efficacement les disques physiques. Ce module fournit une vue d'ensemble de ces fonctionnalités et explique les étapes requises pour les configurer.

Outre la réduction de l'espace disque, la connexion entre le stockage et les disques distants est un autre souci inhérent au stockage. Le stockage iSCSI (Internet Small Computer System Interface) de Windows Server 2012 est une fonctionnalité rentable qui contribue à créer une connexion entre les serveurs et le stockage. Pour implémenter le stockage iSCSI dans Windows Server 2012, vous devez connaître l'architecture et les composants iSCSI. Vous devez également connaître les outils fournis dans Windows Server pour implémenter un stockage de type iSCSI.

Dans les organisations qui possèdent des succursales, il faut tenir compte des liaisons lentes et de la façon de les utiliser efficacement lors de l'envoi des données entre des bureaux. La fonctionnalité Windows BranchCache® proposée avec Windows Server 2012 contribue à résoudre le problème que posent les connectivités lentes. Ce module décrit la fonctionnalité BranchCache et comment la configurer.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- configurer le stockage iSCSI ;
- configurer la fonctionnalité BranchCache ;
- optimiser l'utilisation du stockage ;
- implémenter des services de fichiers avancés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Configuration du stockage iSCSI

Le stockage iSCSI est un moyen simple et peu coûteux de configurer une connexion vers des disques distants. Beaucoup de conditions requises par les applications nécessitent que les connexions de stockage distantes soient redondantes par nature pour obtenir une tolérance aux pannes ou une haute disponibilité. En outre, beaucoup de sociétés disposent déjà de réseaux à tolérance de panne, dans lesquels la redondance est bon marché par rapport aux réseaux de stockage (SAN). Dans cette leçon, vous apprendrez à créer une connexion entre les serveurs et le stockage iSCSI. Vous effectuerez ces tâches à l'aide du stockage iSCSI basé sur IP. Vous apprendrez également à créer des connexions uniques et redondantes à une cible iSCSI. Vous utiliserez à cet effet le logiciel de l'initiateur iSCSI, disponible dans Windows Server 2012.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

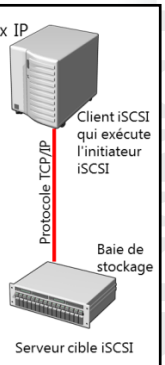
- décrire le stockage iSCSI et ses composants ;
- décrire le serveur cible iSCSI et l'initiateur iSCSI ;
- décrire les options permettant d'implémenter la haute disponibilité pour le stockage iSCSI ;
- décrire les options de sécurité iSCSI ;
- expliquer comment configurer la cible iSCSI ;
- expliquer comment se connecter au stockage iSCSI ;
- décrire les éléments à prendre en compte pour implémenter une solution de stockage iSCSI.

Qu'est-ce qu'iSCSI ?

iSCSI est un protocole qui prend en charge l'accès aux périphériques de stockage SCSI (Small Computer System Interface) sur un réseau TCP/IP. iSCSI véhicule les commandes SCSI standard sur des réseaux IP pour faciliter les transferts de données sur les intranets et gérer le stockage sur de longues distances. Vous pouvez utiliser le protocole iSCSI pour transmettre des données sur des réseaux locaux (LAN), des réseaux étendus (WAN) ou même sur Internet.

iSCSI transmet les commandes SCSI sur les réseaux IP

Composant	Description
Réseau IP	Fournit la haute performance et la redondance
Cibles iSCSI	Est exécuté sur le périphérique de stockage et permet l'accès direct aux disques
Initiateurs iSCSI	Composant logiciel ou carte hôte qui, sur le serveur, fournit l'accès aux cibles iSCSI
IQN	Identificateur globalement unique servant à adresser les initiateurs et les cibles sur un réseau iSCSI



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le protocole iSCSI repose sur une architecture réseau Ethernet standard. Le matériel spécialisé, tel que les adaptateurs de bus hôte (HBA) ou les commutateurs réseau, est facultatif. Le protocole iSCSI utilise la suite TCP/IP (en général le port TCP 3260). Il permet ainsi à deux hôtes de négocier des tâches (l'établissement de session, le contrôle de flux et la taille de paquet, par exemple) et d'échanger ensuite des commandes SCSI à l'aide d'un réseau Ethernet existant. Ce faisant, le protocole iSCSI utilise une architecture de sous-système de bus de stockage local hautes performances répandue et l'émule sur des réseaux LAN et WAN pour créer un réseau SAN. À la différence de certaines technologies SAN, le protocole iSCSI ne requiert aucun câblage spécialisé. Vous pouvez l'exécuter sur l'infrastructure existante de commutation et IP. Toutefois, les performances d'un déploiement SAN iSCSI peuvent être considérablement améliorées si ce déploiement est exécuté sur un réseau ou sous-réseau dédié, comme le recommandent les meilleures pratiques.

 **Remarque :** Bien que vous puissiez utiliser une carte réseau Ethernet standard pour connecter le serveur au périphérique de stockage iSCSI, vous pouvez également utiliser des contrôleurs de bus hôte iSCSI dédiés.

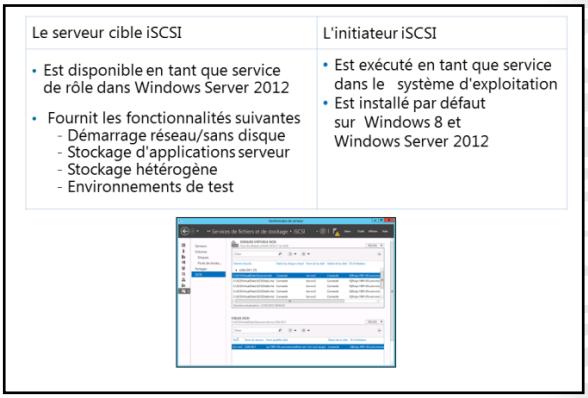
Un déploiement de SAN iSCSI comprend les éléments suivants :

- Réseau TCP/IP. Pour connecter les serveurs au périphérique de stockage, vous pouvez utiliser des cartes d'interface réseau et des commutateurs réseau Ethernet standard. Pour offrir des performances suffisantes, le réseau doit fournir des vitesses d'au moins 1 gigabit par seconde (Gbit/s) et différents chemins d'accès à la cible iSCSI. Une bonne pratique consiste à utiliser un réseau physique et logique dédié pour obtenir un débit rapide et fiable.
- Cibles iSCSI. Il s'agit d'une autre méthode pour accéder au stockage. Les cibles iSCSI présentent ou publient le stockage, comme des contrôleurs pour des lecteurs de disque dur de stockage local. Toutefois, ce stockage n'est pas accessible sur un réseau mais localement. Beaucoup de fournisseurs de stockage implémentent les cibles iSCSI au niveau matériel comme faisant partie du matériel de leur périphérique de stockage. D'autres périphériques ou appareils, tels que les périphériques de Windows Storage Server 2012, implémentent les cibles iSCSI à l'aide d'un pilote logiciel et d'au moins une carte Ethernet. Windows Server 2012 fournit le serveur cible iSCSI, qui est en fait un pilote du protocole iSCSI, en tant que service de rôle.
- Initiateurs iSCSI. La cible iSCSI affiche le stockage pour l'initiateur iSCSI (également appelé le *client*), qui agit en tant que contrôleur de disque local pour les disques distants. Toutes les versions de Windows Server à partir de Windows Server 2008 comprennent l'initiateur iSCSI et peuvent se connecter aux cibles iSCSI.
- Nom IQN (iSCSI Qualified Name). Les IQN sont des identificateurs globalement uniques qui servent à adresser les initiateurs et cibles d'un réseau iSCSI. Lorsque vous configurez une cible iSCSI, vous devez configurer l'IQN des initiateurs iSCSI qui se connecteront à cette cible. Les initiateurs iSCSI utilisent également les IQN pour se connecter aux cibles iSCSI. Toutefois, si la résolution de noms sur le réseau iSCSI est un problème possible, des points de terminaison iSCSI (à la fois cible et initiateur) peuvent toujours être identifiés par leurs adresses IP.

  Question : Pouvez-vous utiliser le réseau TCP/IP interne de votre organisation pour fournir une communication iSCSI ?

Serveur cible iSCSI et initiateur iSCSI

Le serveur cible iSCSI et l'initiateur iSCSI sont décrits ci-dessous.



Serveur cible iSCSI

Le service de rôle de serveur cible iSCSI fournit des sous-systèmes de disques iSCSI de type logiciel indépendants du matériel. Vous pouvez utiliser le serveur cible iSCSI pour créer des cibles iSCSI et des disques virtuels iSCSI. Vous pouvez utiliser ensuite le Gestionnaire de serveur pour gérer ces cibles et disques virtuels iSCSI.

Le serveur cible iSCSI compris dans Windows Server 2012 fournit les fonctionnalités suivantes :

- Démarrage réseau/sans disque. En utilisant des cartes réseau compatibles pour le démarrage ou un chargeur de logiciels, vous pouvez utiliser des cibles iSCSI pour déployer rapidement des serveurs sans disque. En utilisant des disques virtuels de différenciation, vous pouvez économiser jusqu'à 90 pour cent de l'espace de stockage pour les images du système d'exploitation. C'est idéal pour les grands déploiements d'images de système d'exploitation identiques, tels qu'une batterie de serveurs Hyper-V® ou des clusters HPC (High Performance Computing).
- Stockage d'applications de serveur. Certaines applications, telles que Hyper-V et Microsoft® Exchange Server, nécessitent un stockage basé sur les blocs. Le serveur cible iSCSI peut fournir à ces applications un stockage basé sur les blocs disponible en permanence. Étant donné que le stockage est accessible à distance, il peut également combiner le stockage basé sur les blocs pour les sites principaux ou les sites de succursale.
- Stockage hétérogène. Le serveur cible iSCSI prend en charge les initiateurs iSCSI qui ne sont pas basés sur le système d'exploitation Windows. Vous pouvez donc partager le stockage sur des serveurs Windows dans les environnements mixtes.
- Environnements de test. Le rôle de serveur cible iSCSI permet à vos ordinateurs Windows Server 2012 d'être utilisés comme périphériques de stockage par blocs accessibles sur le réseau. Cela est très utile dans les situations dans lesquelles vous souhaitez tester des applications avant de les déployer sur un réseau de stockage SAN.

Les serveurs cibles iSCSI qui fournissent le stockage par blocs utilisent votre réseau Ethernet existant ; aucun matériel supplémentaire n'est requis. Si la haute disponibilité est un critère important, pensez à installer un cluster haute disponibilité. Avec un cluster haute disponibilité, vous aurez besoin d'un stockage partagé pour le cluster, soit un stockage Fibre Channel matériel ou une baie de stockage SAS (Serial Attached SCSI). Le serveur cible iSCSI s'intègre directement à la fonctionnalité de cluster de basculement sous forme de rôle de cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Initiateur iSCSI

Le service d'initiateur iSCSI est un composant standard installé par défaut depuis Windows Server 2008 et Windows Vista®. Pour connecter votre ordinateur à une cible iSCSI, il vous suffit de démarrer le service d'initiateur iSCSI de Microsoft et de le configurer.

Les nouvelles fonctionnalités de Windows Server 2012 incluent :

- L'authentification. Vous pouvez activer le protocole CHAP (Challenge Handshake Authentication Protocol) pour authentifier les connexions d'initiateur, ou le protocole CHAP inversé pour permettre à l'initiateur d'authentifier la cible iSCSI.
- L'ordinateur initiateur de requête d'ID. Cette fonctionnalité n'est prise en charge qu'avec Windows 8 ou Windows Server 2012.

Documentation supplémentaire : Pour plus d'informations sur l'introduction des cibles iSCSI dans Windows Server 2012, reportez-vous à : http://go.microsoft.com/fwlink/?LinkId=270038

Question : Quand devez-vous penser à implémenter le démarrage sans disque sur les cibles iSCSI ?

Options pour l'implémentation de la haute disponibilité iSCSI

En plus de configurer le serveur cible iSCSI de base et les paramètres de l'initiateur iSCSI, vous pouvez intégrer ces services dans des configurations plus avancées.

Les deux technologies servant à implémenter le protocole iSCSI pour la haute disponibilité sont

- MCS. En cas de défaillance, toutes les commandes iSCSI en attente sont réattribuées automatiquement à une autre connexion
- MPIO. Si vous avez plusieurs cartes d'interface réseau dans votre initiateur iSCSI et serveur cible iSCSI, vous pouvez utiliser la fonctionnalité MPIO pour fournir une redondance par basculement en cas de panne de réseau

Configuration d'iSCSI pour la haute disponibilité

La création d'une connexion unique au stockage iSCSI rend ce stockage disponible. Mais il ne rend pas ce stockage hautement disponible. En cas de perte de connexion iSCSI, le serveur perd l'accès à son stockage. Par conséquent, la plupart des connexions de stockage iSCSI sont rendues redondantes au moyen d'une ou deux technologies haute disponibilité : la session à connexions multiples (MCS, Multiple Connected Session) et MPIO (Multipath I/O).

Bien que ces technologies soient similaires dans leur résultat, elles utilisent des approches différentes pour obtenir la haute disponibilité pour les connexions de stockage iSCSI.

MCS est une fonctionnalité du protocole iSCSI qui:

- autorise plusieurs connexions TCP/IP entre l'initiateur et la cible pour la même session iSCSI ;
- prend en charge le basculement automatique. Si une défaillance se produit, toutes les commandes iSCSI en attente sont réattribuées automatiquement à une autre connexion ;
- requiert une prise en charge explicite par des périphériques SAN iSCSI, bien que le rôle de serveur cible iSCSI de Windows Server 2012 la prenne en charge.

La fonctionnalité MPIO fournit la redondance différemment :

- Si vous avez plusieurs cartes d'interface réseau (NIC) dans votre initiateur iSCSI et serveur cible iSCSI, vous pouvez utiliser la fonctionnalité MPIO pour fournir une redondance par basculement lors des pannes de réseau.
- La fonctionnalité MPIO nécessite un DSM (Device Specific Module) pour se connecter à un périphérique SAN tiers connecté à l'initiateur iSCSI. Le système d'exploitation Windows comprend un DSM MPIO par défaut installé sous forme d'une fonctionnalité MPIO dans le Gestionnaire de serveur.
- La fonctionnalité MPIO est largement prise en charge. De nombreux SAN peuvent utiliser le DSM par défaut sans logiciel supplémentaire tandis que d'autres ont besoin de demander un DSM spécialisé à leur fabricant.
- La fonctionnalité MPIO est plus complexe à configurer et n'est pas aussi entièrement automatisé pendant le basculement que la fonctionnalité MCS.

Options de sécurité iSCSI

Puisque le protocole iSCSI permet d'accéder aux dispositifs de stockage via un réseau TCP/IP, il est crucial que vous sécurisiez votre solution iSCSI pour la protéger des utilisateurs malveillants ou des attaques. Vous pouvez atténuer les risques pesant sur votre solution iSCSI en sécurisant différentes couches de l'infrastructure. Le terme *défense en profondeur* est souvent utilisé pour décrire l'utilisation de plusieurs technologies de sécurité à différents points dans toute votre organisation.

Utilisez l'approche de défense en profondeur pour sécuriser les solutions iSCSI

Données	BitLocker, listes de contrôle d'accès, EFS, procédures de sauvegarde/restauration
Application	Renforcement de la sécurité des applications, antivirus
Hôte	Renforcement, authentification, gestion des mises à jour
Réseau interne	Segments réseau, IPsec
Périmètre	Pare-feu
Sécurité physique	Protections, verrous, dispositifs de suivi
Stratégies, procédures et sensibilisation	Documentation sur la sécurité, sensibilisation des utilisateurs

Une stratégie de défense en profondeur inclut les éléments suivants :

- Stratégies, procédures et sensibilisation. Par mesure de sécurité, les mesures relatives aux stratégies de sécurité doivent fonctionner dans le contexte des stratégies de l'organisation. Par exemple, songez non seulement à appliquer une stratégie de mot de passe utilisateur contraignante dans toute l'organisation, mais également une stratégie de mot de passe administrateur encore plus contraignante pour l'accès aux périphériques de stockage iSCSI et aux ordinateurs sur lesquels sont installés les logiciels de gestion iSCSI.
- Sécurité physique. Si n'importe quelle personne non autorisée peut accéder physiquement aux périphériques de stockage iSCSI ou à un ordinateur connecté au réseau, la plupart des autres mesures de sécurité sont inutiles. Vous devez veiller à ce que les périphériques de stockage iSCSI, les ordinateurs qui les gèrent et les serveurs auxquels ils sont connectés soient physiquement sécurisés, et que seul le personnel autorisé puisse y accéder.
- Périmètre. Les réseaux de périmètre marquent la limite entre les réseaux publics et privés. Implémenter des pare-feu et des serveurs proxy inversés dans le réseau de périmètre vous permet de fournir des services d'entreprise plus sécurisés sur le réseau public et d'éviter les attaques potentielles des périphériques de stockage iSCSI depuis Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Réseaux. Lorsque vous connectez des périphériques de stockage iSCSI à un réseau, ils peuvent faire l'objet d'un certain nombre de menaces. Ces menaces comprennent l'écoute illicite, l'usurpation d'identité, le déni de service et les attaques par relecture. Utilisez des fonctionnalités d'authentification telles que le protocole CHAP pour protéger la communication entre les initiateurs et les cibles iSCSI. Vous pourriez également envisager d'implémenter le protocole de sécurité IPSec pour chiffrer le trafic entre les initiateurs et les cibles iSCSI. L'isolation du trafic iSCSI dans son propre réseau local virtuel (VLAN) renforce également la sécurité en évitant que des utilisateurs malveillants connectés au réseau d'entreprise VLAN ne puissent attaquer les périphériques de stockage iSCSI connectés à un réseau VLAN différent. Vous devriez également protéger le matériel réseau (tel que les routeurs et les commutateurs) utilisé par les périphériques de stockage iSCSI contre l'accès non autorisé.
- Hôte. La couche de défense suivante est la couche de protection pour les ordinateurs hôte connectés aux périphériques de stockage iSCSI. Vous devez maintenir la sécurité des ordinateurs en utilisant les dernières mises à jour de sécurité. Vous devriez utiliser uniformément la fonctionnalité Windows Update des systèmes d'exploitation Windows pour tenir votre système d'exploitation à jour. Vous devez également configurer des stratégies de sécurité, comme la complexité des mots de passe, configurer le pare-feu hôte et installer un logiciel antivirus.
- Applications. Les applications ne sont sécurisées que si les dernières mises à jour de sécurité ont été installées. Pour les applications exécutées sur vos serveurs mais qui ne bénéficient pas des mises à jour de Windows Update, vous devriez régulièrement vérifier les mises à jour de sécurité publiées par le revendeur de l'application. Vous devriez également mettre à jour le logiciel à jour iSCSI selon les recommandations des fournisseurs et les meilleures pratiques.
- Données. C'est la couchefinale de sécurité. Pour aider à protéger votre réseau, assurez-vous d'utiliser correctement les droits des utilisateurs de fichiers. Utilisez pour cela la fonctionnalité de chiffrement de lecteur Windows BitLocker® et des listes de contrôle d'accès (ACL), implémentez le chiffrement des données confidentielles avec le système de chiffrement de fichiers EFS et réalisez les copies de sauvegarde régulières des données.

Démonstration : Configuration d'une cible iSCSI

Dans cette démonstration, vous allez apprendre à :

- ajouter le service de rôle du serveur cible iSCSI ;
- créer deux disques virtuels iSCSI et une cible iSCSI.

Procédure de démonstration

Ajouter le service de rôle de serveur cible iSCSI

1. Sur LON-DC1, ouvrez le **Gestionnaire de serveur**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, installez les rôles et fonctionnalités suivantes sur le serveur local et acceptez les valeurs par défaut :
    - **Service de fichiers et de stockage (Installé)\Services de fichiers et iSCSI (Installé)\Serveur cible iSCSI**

Créer deux disques virtuels iSCSI et une cible iSCSI

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**, puis sur **iSCSI**.
2. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
3. Créez un disque virtuel avec les paramètres suivants :
   - Nom : **iSCSIDisk1**
   - Taille de disque : **5 Go**
   - Cible iSCSI : **Nouveau**
   - Nom de la cible : **LON-SVR2**
   - Serveurs d'accès : **172.16.0.22**
4. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis fermez la page **Afficher les résultats**.
5. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
6. Créez un disque virtuel avec les paramètres suivants :
   - Nom : **iSCSIDisk2**
   - Taille de disque : **5 Go**
   - Cible iSCSI : **LON-SVR2**
7. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis fermez la page **Afficher les résultats**.

Démonstration : Connexion au stockage iSCSI

Dans cette démonstration, vous allez apprendre à :

- vous connecter à la cible iSCSI ;
- vérifier la présence du disque iSCSI.

Procédure de démonstration

Procédure de préparation

Avant de commencer cette démonstration, effectuez les étapes suivantes :

1. Sur l'ordinateur hôte, dans la console **Gestionnaire Hyper-V**, ouvrez les paramètres pour l'ordinateur virtuel **22412B-LON-SVR2**.
2. Dans la fenêtre **Paramètres pour 22412B-LON-SVR2**, assurez-vous que les deux cartes réseau héritées sont connectées à **Private Network**.
3. Si l'état d'une carte réseau héritée est défini sur **Non connecté**, connectez-la au réseau virtuel appelé **Private Network**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Se connecter à la cible iSCSI

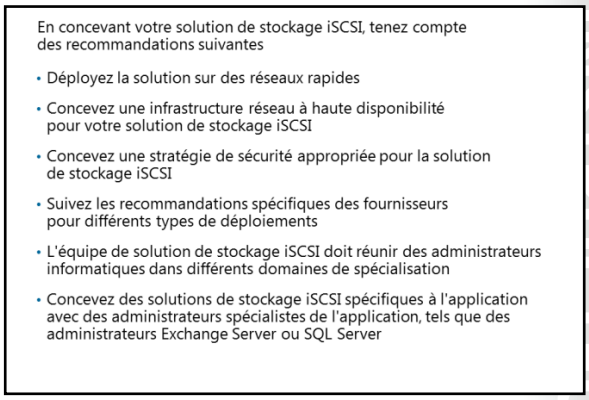
1. Ouvrez une session sur **LON-SVR2** avec le nom d'utilisateur **Adatum\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Ouvrez le **gestionnaire de serveur** et, dans le menu **Outils**, ouvrez **Initiateur iSCSI**.
3. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, définissez les paramètres suivants :
   - Connexion rapide : **LON-DC1**
   - Cibles découvertes : **iqn.1991-05.com.microsoft:lon-dc1-lon-svr2-target**

Vérifier la présence du disque iSCSI

1. Dans Gestionnaire de serveur, dans le menu **Outils**, ouvrez **Gestion de l'ordinateur**.
2. Dans la console Gestion de l'ordinateur, sous **Stockage**, accédez à **Gestion des disques**. Notez que les nouveaux disques sont ajoutés. Ils sont toutefois tous hors connexion et non formatés pour le moment.
3. Fermez la console Gestion de l'ordinateur.

Éléments à prendre en compte pour l'implémentation du stockage iSCSI

En concevant votre solution de stockage iSCSI, tenez compte des recommandations suivantes :



- Déployez la solution iSCSI sur des réseaux d'au moins 1 Gbit/s.
- Une conception haute disponibilité est en effet cruciale pour l'infrastructure réseau, parce que les données sont transférées des serveurs au stockage iSCSI via des périphériques et des composants du réseau. (Les éléments importants concernant la haute disponibilité ont été expliqués plus tôt dans ce module.)
- Concevez une stratégie de sécurité appropriée pour la solution de stockage iSCSI. (Les éléments importants et les recommandations concernant la sécurité ont été expliqués plus tôt dans ce module.)
- Lisez les recommandations spécifiques des fournisseurs pour les différents types de déploiements et d'applications qui utiliseront la solution de stockage iSCSI, comme Exchange Server et Microsoft SQL Server®.
- Le personnel informatique qui concevra, configurera et administrera la solution de stockage iSCSI devra inclure des administrateurs informatiques dans différents domaines de spécialisation, tels que des administrateurs de Windows Server 2012, des administrateurs réseau, des administrateurs de stockage et des administrateurs de sécurité. C'est en effet nécessaire pour que la solution de stockage iSCSI bénéficie de performances et d'une sécurité optimales et pour que les procédures de gestion et d'exécution soient homogènes.
- En concevant une solution de stockage iSCSI, l'équipe de conception devrait également inclure des administrateurs spécifiques à l'application, tels que des administrateurs Exchange Server et SQL Server, de sorte que vous puissiez implémenter la configuration optimale pour la technologie ou la solution en question.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration de la fonctionnalité BranchCache

Les succursales doivent relever des défis de gestion uniques. La connectivité des succursales au réseau d'entreprise est généralement lente et leur infrastructure est limitée pour sécuriser les serveurs. Il est par ailleurs nécessaire de sauvegarder les données gérées dans les succursales distantes, ce qui explique pourquoi les organisations préfèrent centraliser les données lorsque c'est possible. La difficulté consiste donc à fournir un accès efficace aux ressources réseau pour les utilisateurs des succursales. La fonctionnalité BranchCache vous aide à résoudre ces problèmes en mettant les fichiers en cache pour qu'ils n'aient pas à être sans cesse transférés sur le réseau.

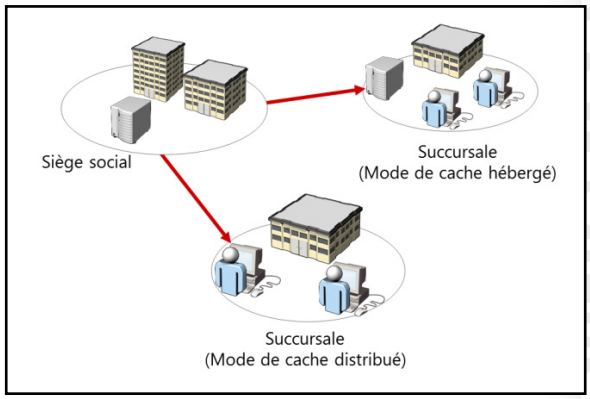
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le fonctionnement de BranchCache ;
- décrire la configuration requise pour BranchCache ;
- expliquer comment configurer les paramètres serveur de BranchCache ;
- expliquer comment configurer les paramètres client de BranchCache ;
- expliquer comment configurer BranchCache ;
- expliquer comment surveiller BranchCache.

Comment fonctionne BranchCache ?

La fonctionnalité BranchCache introduite avec Windows Server 2008 R2 et Windows 7 réduit l'utilisation du réseau sur les connexions WAN entre les succursales et le siège en mettant localement en cache les fichiers fréquemment utilisés sur les ordinateurs d'une succursale. BranchCache améliore la performance des applications qui utilisent l'un des protocoles suivants :



- Protocoles HTTP ou HTTPS. Ces protocoles sont utilisés par les navigateurs Web et d'autres applications.
- Protocole SMB (Server Message Block), y compris le protocole de trafic SMB signé. Ce protocole est utilisé pour accéder à des dossiers partagés.
- Service de transfert intelligent en arrière-plan (BITS). Composant Windows qui distribue le contenu d'un serveur aux clients en utilisant seulement la bande passante réseau inactive. Le service BITS est également un composant utilisé par Microsoft System Center Configuration Manager.

Lorsque le client demande des données, BranchCache les récupère depuis un serveur. Étant donné que BranchCache offre une fonctionnalité de cache passif, celui-ci n'augmente pas l'utilisation du réseau WAN. BranchCache met seulement en cache les requêtes de lecture et n'interfère pas avec un utilisateur qui enregistre un fichier.

BranchCache améliore la réactivité des applications réseau communes qui accèdent à des serveurs intranet à travers des liaisons WAN lentes. Puisque BranchCache ne requiert pas d'infrastructure supplémentaire, vous pouvez améliorer la performance des réseaux distants en déployant Windows 7 ou Windows 8 sur les ordinateurs client et en déployant Windows Server 2008 R2 et Windows Server 2012 sur les serveurs, puis en activant la fonctionnalité BranchCache.

BranchCache fonctionne parfaitement avec les technologies de sécurité du réseau, y compris la technologie SSL (Secure Sockets Layer), la signature SMB et le chiffrement IPsec de bout en bout. Vous pouvez utiliser BranchCache pour réduire l'utilisation de la bande passante réseau et améliorer la performance des applications, même si le contenu est chiffré.

Vous pouvez configurer BranchCache pour utiliser le mode de cache hébergé ou le mode de cache distribué :

- Mode de cache hébergé. Ce mode fonctionne en déployant un ordinateur qui exécute Windows Server 2008 R2 ou une version plus récente en tant que serveur de cache hébergé dans la succursale. Les ordinateurs client localisent l'ordinateur hôte afin de pouvoir récupérer le contenu du cache hébergé lorsque le cache hébergé est disponible. Si le contenu n'est pas disponible dans le cache hébergé, il est récupéré sur le serveur de contenu au moyen d'une liaison WAN, puis transféré dans le cache hébergé pour que les demandes suivantes des clients puissent l'y récupérer.
- Mode de cache distribué. Pour de plus petits bureaux distants, vous pouvez configurer BranchCache en mode de cache distribué sans avoir besoin d'un serveur. Dans ce mode, les ordinateurs client locaux exécutant Windows 7 ou Windows 8 conservent une copie du contenu et le rendent disponible à d'autres clients autorisés qui demandent les mêmes données. Cela évite d'avoir un serveur dans la succursale. Cependant, à la différence du mode de cache hébergé, cette configuration fonctionne uniquement par sous-réseau. En outre, les clients qui hibernent ou sont déconnectés du réseau ne peuvent pas fournir le contenu à d'autres clients.

Remarque : Si vous utilisez BranchCache, vous pouvez utiliser les deux modes dans votre organisation, mais ne pouvez configurer qu'un seul mode par succursale.

La fonctionnalité BranchCache de Windows Server 2012 offre les améliorations suivantes :

- À des fins d'évolutivité, BranchCache permet d'avoir plusieurs serveurs de cache hébergés par emplacement.
- Une nouvelle base de données sous-jacente utilise la technologie de base de données ESE (Extensible Storage Engine) d'Exchange Server. Cela permet à un serveur de cache hébergé d'enregistrer considérablement plus de données (jusqu'à même plusieurs téraoctets).
- Un déploiement plus simple signifie que vous n'avez pas besoin d'un objet de stratégie de groupe (GPO) pour chaque emplacement. Pour déployer BranchCache, vous avez besoin d'un seul objet GPO contenant les paramètres. Cela permet également aux clients de basculer entre le mode de cache hébergé et le mode distribué sans avoir à utiliser d'objets GPO spécifiques au site (ce qui devrait être évité dans plusieurs scénarios) lorsqu'ils passent d'un emplacement à un autre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment les ordinateurs client récupèrent-ils les données en utilisant BranchCache ?

Quand BranchCache est activé sur un ordinateur client et sur un serveur, et quand l'ordinateur client utilise le protocole HTTP, HTTPS ou SMB, l'ordinateur client exécute le processus suivant pour récupérer les données :

1. L'ordinateur client qui exécute Windows 8 se connecte à un serveur de contenu sous Windows Server 2012 au siège social, et demande un contenu de la même façon qu'il le ferait pour récupérer un contenu sans utiliser BranchCache.
2. Le serveur de contenu au siège social authentifie l'utilisateur et vérifie qu'il est autorisé à accéder aux données.
3. Au lieu d'envoyer lui-même le contenu, le serveur de contenu au siège social renvoie des identificateurs ou des hachages du contenu demandé à l'ordinateur client. Le serveur de contenu envoie les données via la même connexion que celle avec laquelle le contenu aurait été normalement envoyé.
4. En utilisant les identificateurs récupérés, l'ordinateur client fait ce qui suit :
   - Si vous configurez l'ordinateur client pour qu'il utilise le cache distribué, il se connecte par multidiffusion au sous-réseau local pour rechercher d'autres ordinateurs client qui ont déjà téléchargé le contenu.
   - Si vous configurez l'ordinateur client pour utiliser le cache hébergé, il recherche le contenu sur le cache hébergé configuré.
5. Si le contenu est disponible dans la succursale, sur un ou plusieurs clients ou sur le cache hébergé, l'ordinateur client récupère les données dans la succursale. L'ordinateur client vérifie également que les données sont à jour et qu'elles n'ont pas été altérées ou corrompues.
6. Si le contenu n'est pas disponible dans le bureau distant, l'ordinateur client le récupère directement sur le serveur via la liaison WAN. L'ordinateur client le rend alors disponible pour d'autres ordinateurs client sur le réseau local (mode de cache distribué) ou l'envoie dans le cache hébergé, où il est mis à disposition d'autres ordinateurs client.

Configuration requise pour BranchCache

BranchCache optimise le trafic entre les sièges sociaux et les succursales. Windows Server 2008 R2, Windows Server 2012 et les ordinateurs client exécutant Windows 7 et Windows 8 peuvent tirer parti d'une utilisation de BranchCache. (Les versions antérieures des systèmes d'exploitation Windows ne proposent pas cette fonctionnalité.) Vous pouvez utiliser BranchCache pour ne mettre en cache que le contenu stocké sur les serveurs de fichiers ou les serveurs Web qui exécutent Windows Server 2008 R2 ou Windows Server 2012.

Configuration requise pour l'utilisation de BranchCache	Conditions requises pour les modes
• Installez la fonctionnalité BranchCache ou la fonctionnalité BranchCache pour Fichiers réseau sur le serveur qui héberge le contenu • Configurez les ordinateurs clients en utilisant soit une stratégie de groupe, soit la commande **netsh**	• En mode de cache distribué, le cache du contenu à la succursale est distribué entre les ordinateurs client • En mode de cache hébergé, le cache du contenu à la succursale est hébergé sur un ou plusieurs ordinateurs qui sont les serveurs de cache hébergé

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration requise pour l'utilisation de BranchCache

Pour utiliser BranchCache pour des services de fichiers, vous devez effectuer les tâches suivantes :

- Installez la fonctionnalité BranchCache ou le service BranchCache pour le rôle Fichiers réseau sur le serveur hôte qui exécute Windows Server 2012.
- Configurez les ordinateurs client en utilisant soit une stratégie de groupe, soit la commande **netsh branchcache set service**.

Si vous souhaitez utiliser BranchCache pour mettre en cache le contenu du serveur de fichiers, vous devez effectuer des tâches suivantes :

- Installez BranchCache pour le service de rôle Fichiers réseau sur le serveur de fichiers.
- Configurez la publication de hachages pour BranchCache.
- Créez des partages de fichiers optimisés par BranchCache.

Si vous souhaitez utiliser BranchCache pour mettre en cache un contenu du serveur Web, vous devez installer la fonctionnalité BranchCache sur le serveur Web. Vous n'avez pas besoin de configurations supplémentaires.

BranchCache est pris en charge sur l'installation complète et l'installation minimale de Windows Server 2012. Par défaut, BranchCache n'est pas installé sur Windows Server 2012.

Configuration requise pour le mode de cache distribué et le mode de cache hébergé

Dans le mode de cache distribué, BranchCache fonctionne sans serveur dédié, mais entre les clients du même site. Si les ordinateurs client sont configurés pour utiliser le mode de cache distribué, n'importe quel ordinateur client peut utiliser un protocole de multidiffusion appelé WS-Discovery pour rechercher localement l'ordinateur qui a déjà téléchargé et mis en cache le contenu. Vous devez configurer le pare-feu client pour activer le trafic entrant, le protocole HTTP et le protocole WS-Discovery.

Les clients rechercheront toutefois un serveur de cache hébergé et, s'ils en découvrent un, ils se configureront eux-mêmes automatiquement comme clients du mode de cache hébergé. Dans le mode de cache hébergé, les ordinateurs client se configurent automatiquement comme clients du mode de cache hébergé et rechercheront le serveur hôte pour pouvoir récupérer le contenu du cache hébergé. Vous pouvez par ailleurs sélectionner une stratégie de groupe pour pouvoir utiliser le nom de domaine complet des serveurs de cache hébergé, ou activer la découverte de cache hébergé automatique par points de connexion de service (SCP). Vous devez configurer un pare-feu pour activer le trafic HTTP entrant du serveur de cache hébergé.

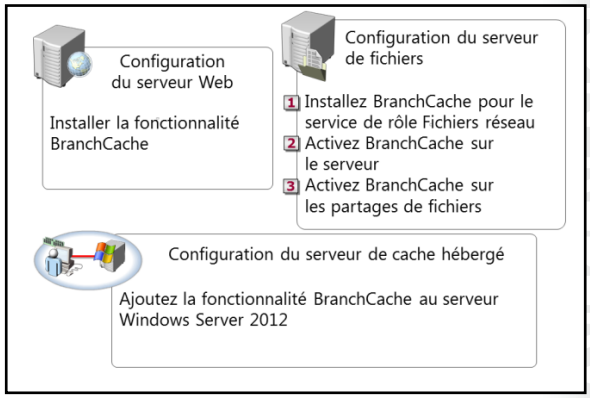
Dans les deux modes de cache, BranchCache utilise le protocole HTTP pour le transfert de données entre les ordinateurs client et l'ordinateur qui héberge les données en mémoire cache.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des paramètres du serveur BranchCache

Vous pouvez utiliser BranchCache pour mettre en cache un contenu Web fourni via le protocole HTTP ou HTTPS. Vous pouvez également utiliser BranchCache pour mettre en cache le contenu d'un dossier partagé fourni via le protocole SMB.

Le tableau suivant dresse la liste des serveurs que vous pouvez configurer pour BranchCache.



Serveur	Description
Serveur Web ou serveur BITS	Pour configurer un serveur Web Windows Server 2012 ou un serveur d'applications qui utilise le protocole BITS, installez la fonctionnalité BranchCache. Vérifiez que le service BranchCache a été démarré. Configurez ensuite les clients qui utiliseront la fonctionnalité BranchCache. Aucune autre configuration du serveur Web n'est nécessaire.
Serveur de fichiers	Vous devez installer la fonctionnalité BranchCache pour le service de rôle Fichiers réseau du rôle serveur Services de fichiers avant de pouvoir activer BranchCache pour un quelconque partage de fichiers. Après avoir installé la fonctionnalité BranchCache du service de rôle Fichiers réseau, utilisez la stratégie de groupe pour activer BranchCache sur le serveur. Vous devez ensuite configurer chaque partage de fichiers pour activer BranchCache.
Serveur de cache hébergé	Pour le mode de cache hébergé, vous devez ajouter la fonctionnalité BranchCache au serveur Windows Server 2012 que vous configurez en tant que serveur de cache hébergé. Pour sécuriser la communication, les ordinateurs client utilisent le protocole TLS (Transport Layer Security) lorsqu'ils communiquent avec le serveur de cache hébergé. Par défaut, BranchCache alloue cinq pour cent de l'espace disque sur la partition active pour héberger des données de cache. Vous pouvez toutefois modifier cette valeur avec la stratégie de groupe ou en exécutant la commande **netsh branchcache set cachesize**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des paramètres du client BranchCache

Il n'est pas nécessaire d'installer la fonctionnalité BranchCache sur les ordinateurs client, car elle est déjà comprise si le client exécute Windows 7 ou Windows 8. Cependant, BranchCache est désactivé par défaut sur les ordinateurs client. Pour activer et configurer BranchCache, vous devez exécuter la procédure suivante :

1. Activez BranchCache.
2. Activez le mode de cache distribué ou le mode de cache hébergé. Les clients Windows 8 peuvent utiliser l'un ou l'autre de façon dynamique.
3. Configurez le pare-feu client pour activer les protocoles BranchCache.

Pour activer et configurer BranchCache, procédez comme suit
1. Activer BranchCache
2. Activez le mode de cache distribué ou le mode de cache hébergé
3. Configurer le pare-feu client

Vous pouvez modifier les paramètres de BranchCache et effectuer des tâches de configuration supplémentaires, comme
- Définir la taille de la mémoire cache
- Définir l'emplacement du serveur de cache hébergé
- Effacer le cache
- Créer et répliquer une clé partagée pour utilisation dans un cluster de serveurs

Activation de BranchCache

Vous pouvez activer la fonctionnalité BranchCache sur les ordinateurs client à l'aide de la stratégie de groupe, Windows PowerShell® ou la commande **netsh branchcache set service**.

Si vous souhaitez activer les paramètres de BranchCache à l'aide de la stratégie de groupe, procédez comme suit pour un objet de stratégie de groupe non basé sur un domaine :

1. Ouvrez la **console de gestion des stratégies de groupe**.
2. Créez un objet de stratégie de groupe qui sera lié à l'unité d'organisation (OU) où sont situés les ordinateurs client.
3. Dans l'objet de stratégie de groupe, suivez le chemin d'accès **Configuration ordinateur\ Stratégies\Modèles d'administration : Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local\Réseau**, puis cliquez sur **BranchCache**.
4. Sélectionnez le paramètre **Activer BranchCache** dans l'objet de stratégie de groupe.

Activation du mode de cache distribué ou hébergé

Vous pouvez configurer le mode de BranchCache sur les ordinateurs client à l'aide de la stratégie de groupe, Windows PowerShell ou la commande **netsh branchcache set service**.

Si vous souhaitez configurer le mode de BranchCache à l'aide de la stratégie de groupe, procédez comme suit pour un objet de stratégie de groupe non basé sur un domaine :

1. Ouvrez la **console de gestion des stratégies de groupe**.
2. Créez un objet de stratégie de groupe qui sera lié à l'unité d'organisation (OU) où sont situés les ordinateurs client.

3. Dans l'objet de stratégie de groupe, suivez le chemin d'accès **Configuration ordinateur\Stratégies\Modèles d'administration : Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local\Réseau**, puis cliquez sur **BranchCache**.
4. Sélectionnez soit le mode de cache distribué, soit le mode de cache hébergé. Vous pouvez également activer à la fois le mode de cache distribué et la découverte automatique de cache hébergé en fonction des paramètres de stratégie de point de connexion de service. Les ordinateurs client fonctionneront en mode de cache distribué, à moins qu'ils ne trouvent un serveur de cache hébergé dans la succursale. S'ils trouvent un serveur de cache hébergé dans la succursale, ils fonctionneront en mode de cache hébergé.

Pour activer BranchCache avec Windows PowerShell, utilisez l'applet de commande **Enable-BCDistributed** ou **Enable-BCHostedServer**. Vous pouvez également utiliser l'applet de commande **Enable-BCHostedClient** pour configurer BranchCache afin qu'il fonctionne en mode de client de cache hébergé.

Par exemple, l'applet de commande suivante active le mode client de cache hébergé en utilisant l'ordinateur SRV1.adatum.com comme serveur de cache hébergé pour des clients Windows 7 et HTTPS.

```
Enable-BCHostedClient –ServerNames SRV1.adatum.com –UseVersion Windows7
```

L'applet de commande suivante active le mode de cache hébergé et inscrit le point de connexion de service dans les services de domaine Active Directory® (AD DS).

```
Enable-BCHostedServer –RegisterSCP
```

L'applet de commande suivante active le mode de cache distribué sur le serveur.

```
Enable-BCDistributed
```

Pour configurer les paramètres de BranchCache avec la commande **netsh branchcache set service**, ouvrez une fenêtre d'invite de commandes et procédez comme suit :

1. Saisissez la syntaxe netsh suivante pour le mode de cache distribué :

```
netsh branchcache set service mode=distributed
```

2. Saisissez la syntaxe netsh suivante pour le mode de cache hébergé :

```
netsh branchcache set service mode=hostedclient location=<serveur de cache hébergé>
```

Configuration du pare-feu client pour activer les protocoles BranchCache

En mode de cache distribué, les clients BranchCache utilisent le protocole HTTP pour le transfert de données entre les ordinateurs client, et le protocole WS-Discovery pour la découverte de contenu mis en cache. Vous devez configurer le pare-feu client pour activer les règles de trafic entrant suivantes :

- BranchCache - Extraction du contenu (utilise HTTP)
- BranchCache - Découverte d'homologue (utilise WSD)

En mode de cache hébergé, les clients BranchCache utilisent le protocole HTTP pour le transfert de données entre les ordinateurs client, mais pas le protocole WS-Discovery. En mode de cache hébergé, vous devriez configurer le pare-feu client pour activer la règle de trafic entrant BranchCache - Extraction du contenu (utilise HTTP).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Tâches de configuration supplémentaires pour BranchCache

Après avoir configuré BranchCache, les clients peuvent accéder aux données en mémoire cache dans les serveurs de contenu sur lesquels BranchCache a été activé, qui sont disponibles localement dans la succursale. Vous pouvez modifier les paramètres de BranchCache et effectuer des tâches de configuration supplémentaires, comme :

- définir la taille de la mémoire cache ;
- définir l'emplacement du serveur de cache hébergé ;
- effacer le cache ;
- créer et répliquer une clé partagée pour utilisation dans un cluster de serveurs.

Démonstration : Configuration de la fonctionnalité BranchCache

Dans cette démonstration, vous allez apprendre à :

- ajouter BranchCache pour le service de rôle Fichiers réseau ;
- configurer BranchCache dans l'Éditeur de stratégie de groupe locale ;
- activer BranchCache pour un partage de fichiers.

Procédure de démonstration

Ajouter BranchCache pour le service de rôle Fichiers réseau

1. Ouvrez une session sur **LON-DC1** et ouvrez le **Gestionnaire de serveur**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, installez les rôles et fonctionnalités suivants sur le serveur local :
    - **Service de fichiers et de stockage (Installé)\Services de fichiers et iSCSI (installés)\ BranchCache pour fichiers réseau**

Activez BranchCache pour le serveur

1. Sur l'écran Accueil, saisissez **gpedit.msc**, puis appuyez sur Entrée.
2. Naviguez jusqu'à **Configuration ordinateur\Modèles d'administration\Réseau\Serveur Lanman**, puis suivez la procédure suivante :
    - Activez **Publication de hachages pour BranchCache**
    - Sélectionnez **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**

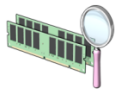
Activer BranchCache pour un partage de fichiers

1. Ouvrez une fenêtre d'**Explorateur de fichiers** et, sur le lecteur C, créez un dossier nommé **Partage**.
2. Configurez les propriétés du dossier **Partage** comme suit :
    - Activez **Partager ce dossier**
    - Cochez **Activer BranchCache** dans **Paramètres hors connexion**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle de la fonctionnalité BranchCache

Les outils d'analyse de BranchCache incluent
- L'applet de commande Windows Powershell Get-BCStatus
- La commande Netsh branchcache shows status
- Observateur d'événements
- Les compteurs de l'Analyseur de performances



Après la configuration initiale, vous souhaitez vérifier que BranchCache est configuré et fonctionne correctement. Vous pouvez utiliser la commande **netsh branchcache show status all** pour afficher l'état de service de BranchCache. Vous pouvez également utiliser l'applet de commande **Get-BCStatus** pour obtenir les informations relatives à l'état et à la configuration de BranchCache. Le client et les serveurs de cache hébergé affichent des informations supplémentaires, telles que l'emplacement du cache local, la taille du cache local et le statut des règles de pare-feu pour les protocoles HTTP et WS-Discovery qu'utilise BranchCache.

Vous pouvez également utiliser les outils suivants pour vérifier le fonctionnement de BranchCache :

- Observateur d'événements. Utilisez cet outil pour surveiller les événements de BranchCache enregistrés dans le journal d'application et le journal des opérations. Le journal d'application est situé dans le dossier Journaux Windows et le journal des opérations dans le dossier Journaux d'application et de service\Microsoft\Windows\BranchCache.
- Compteurs de performance. Utilisez cet outil pour surveiller les compteurs Analyseur de performances de BranchCache. Les compteurs Analyseur de performances de BranchCache sont des outils de débogage utiles pour surveiller l'efficacité et l'intégrité de BranchCache. Vous pouvez également utiliser l'analyse des performances de BranchCache pour connaître la bande passante économisée en mode de cache distribué ou hébergé. Si vous avez implémenté Microsoft System Center 2012 - Operations Manager dans l'environnement, vous pouvez utiliser le pack d'administration BranchCache pour Operations Manager 2012.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Optimisation de l'utilisation du stockage

Chaque organisation enregistre ses données sur des systèmes de stockage différents. Comme ces systèmes de stockage traitent de plus en plus de données à des vitesses plus rapides, les besoins d'espace disque pour stocker ces données ont augmenté. Le grand nombre de fichiers, de dossiers et d'informations, ainsi que la façon dont ils sont stockés, organisés, gérés et maintenus posent un nouveau problème aux organisations. Celles-ci doivent par ailleurs répondre à certaines exigences en matière de sécurité, de conformité et de prévention des vols de données pour les informations confidentielles.

Windows Server 2012 propose de nombreuses technologies qui peuvent aider les organisations à relever les défis que représentent la gestion, la maintenance, la sécurisation et l'optimisation des données stockées sur différents périphériques de stockage. Ces technologies comprennent le Gestionnaire de ressources du serveur de fichiers, l'infrastructure de classification des fichiers et la déduplication des données, qui fournissent chacune de nouvelles fonctionnalités par rapport à Windows Server 2008 R2.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le Gestionnaire de ressources du serveur de fichiers ;
- décrire la classification des fichiers ;
- décrire les règles de classification ;
- expliquer comment configurer la classification des fichiers ;
- décrire les options d'optimisation du stockage dans Windows Server 2012 ;
- expliquer comment configurer la déduplication des données.

Qu'est-ce que le Gestionnaire de ressources du serveur de fichiers ?

Vous pouvez utiliser le Gestionnaire de ressources du serveur de fichiers (FSRM) pour gérer et classer les données stockées sur des serveurs de fichiers. FSRM comprend les fonctionnalités suivantes :

Vous pouvez utiliser le Gestionnaire de ressources du serveur de fichiers pour gérer et classer les données stockées sur des serveurs de fichiers

Fonctionnalités du Gestionnaire de ressources du serveur de fichiers	Nouvelles fonctionnalités du Gestionnaire de ressources du serveur de fichiers
• Infrastructure de classification des fichiers • Tâches de gestion de fichiers • Gestion des quotas • Gestion du filtrage des fichiers • Rapports de stockage	• Contrôle d'accès dynamique • Classification manuelle • Assistance en cas d'accès refusé • Tâches de gestion de fichiers • Classification automatique

- Infrastructure de classification des fichiers. Cette fonctionnalité automatise le processus de classification des données. Vous pouvez appliquer dynamiquement des stratégies d'accès aux fichiers selon leur classification. Les stratégies comprennent, par exemple, le contrôle d'accès dynamique pour limiter l'accès aux fichiers, le chiffrement des fichiers et l'expiration des fichiers. Vous pouvez classer les fichiers automatiquement à l'aide de règles de classification de fichiers, ou manuellement en modifiant les propriétés d'un fichier ou dossier sélectionné. Vous pouvez modifier des propriétés de fichier automatiquement selon le type d'application ou le contenu du fichier, ou en définissant manuellement des options sur le serveur qui déclenchera la classification des fichiers.

- Tâches de gestion de fichiers. Vous pouvez utiliser cette fonctionnalité pour appliquer une stratégie ou action conditionnelle aux fichiers en fonction de leur classification. Les conditions d'une tâche de gestion de fichiers comprennent l'emplacement du fichier, les propriétés de classification, la date à laquelle le fichier a été créé, la dernière date de modification du fichier et la dernière date d'accès au fichier. Les actions qu'une tâche de gestion de fichiers peut effectuer comprennent la capacité de faire expirer des fichiers, de chiffrer des fichiers et d'exécuter une commande personnalisée.
- Gestion des quotas. Cette fonctionnalité sert à limiter l'espace autorisé pour un volume ou un dossier. Vous pouvez automatiquement appliquer des quotas aux nouveaux dossiers qui sont créés sur un volume. Vous pouvez également définir les modèles de quotas que vous pouvez appliquer à de nouveaux volumes ou dossiers.
- Gestion du filtrage des fichiers. Vous pouvez utiliser cette fonctionnalité pour contrôler les types de fichiers que les utilisateurs peuvent stocker sur un serveur de fichiers. Vous pouvez limiter l'extension qui peut être stockée sur vos partages de fichiers. Par exemple, vous pouvez créer un filtre de fichiers qui n'autorise pas les fichiers avec une extension .mp3 à être stockés dans les dossiers partagés personnels sur un serveur de fichiers.
- Rapports de stockage. Vous pouvez utiliser cette fonctionnalité pour identifier des tendances dans l'utilisation du disque et savoir comment vos données sont classées. Vous pouvez également surveiller les tentatives de sauvegarde de fichiers non autorisés par les utilisateurs.

Vous pouvez configurer et gérer FSRM à l'aide du composant logiciel enfichable Gestionnaire de ressources du serveur de fichiers de la console Microsoft Management Console (MMC), ou en utilisant l'interface de ligne de commande Windows PowerShell.

Les fonctionnalités suivantes du gestionnaire FSRM sont nouvelles dans Windows Server 2012 :

- Intégration avec le contrôle d'accès dynamique. Le contrôle d'accès dynamique utilise l'infrastructure de classification des fichiers pour vous aider à contrôler et auditer de façon centralisée l'accès aux fichiers sur vos serveurs de fichiers.
- Classification manuelle. La classification manuelle permet aux utilisateurs de classer les fichiers et dossiers manuellement sans devoir créer des règles de classification automatique.
- Assistance en cas d'accès refusé. Vous pouvez utiliser l'Assistance en cas d'accès refusé pour personnaliser le message d'erreur d'accès refusé qui s'affiche dans Windows 8 Consumer Preview lorsque les utilisateurs n'ont pas accès à un fichier ou à un dossier.
- Tâches de gestion de fichiers. Les mises à jour des tâches de gestion de fichiers comprennent les tâches de gestion de fichiers des services AD DS et AD RMS (Active Directory® Rights Management Services), les tâches continues de gestion de fichiers et l'espace de noms dynamique pour les tâches de gestion de fichiers.
- Classification automatique. Les mises à jour de la classification automatique vous permettent d'avoir un meilleur contrôle de la façon dont les données sont classées sur vos serveurs de fichiers, notamment la classification continue, en utilisant Windows PowerShell pour la classification personnalisée, les mises à jour du classeur de contenu existant et l'espace de noms dynamique pour les règles de classification.

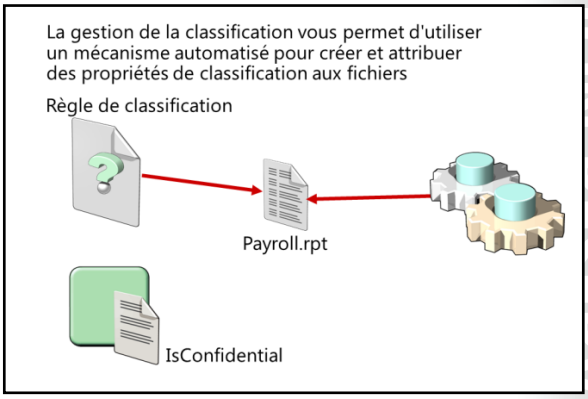
Documentation supplémentaire : Pour plus d'informations sur FSRM, consultez la page Nouveautés du Gestionnaire de ressources du serveur de fichiers à l'adresse http://go.microsoft.com/fwlink/?LinkId=270039.

Question : Utilisez-vous actuellement le Gestionnaire de ressources du serveur de fichiers dans Windows Server 2008 R2 ? Si oui, pour quels domaines l'utilisez-vous ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que la classification des fichiers ?

La classification des fichiers permet aux administrateurs de configurer des procédures automatiques pour définir une propriété souhaitée sur un fichier, en fonction des conditions spécifiées dans les règles de classification. Par exemple, vous pouvez définir la propriété **Confidentialité** sur **Haute** pour tous les documents dont le contenu contient le mot « **secret** ».



Dans Windows Server 2008 R2 et Windows Server 2012, les tâches de gestion de la classification et des fichiers permettent aux administrateurs de gérer des groupes de fichiers selon divers attributs des fichiers et des dossiers. Vous pouvez automatiser les tâches de maintenance des fichiers et des dossiers, comme de nettoyer les données périmées ou protéger les informations confidentielles. Pour cette raison, les tâches de maintenance des fichiers et des dossiers sont plus efficaces que la maintenance du système de fichiers en naviguant dans son affichage hiérarchique.

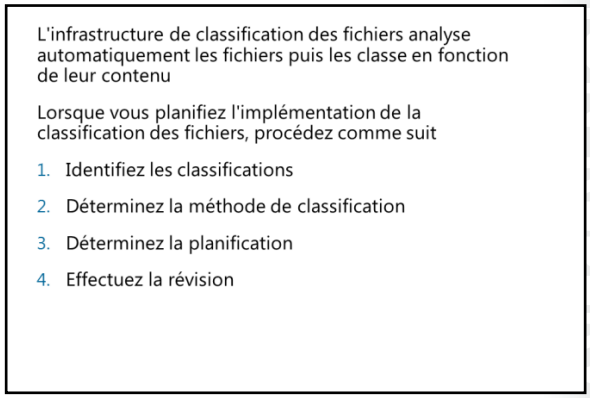
La gestion de la classification est conçue pour simplifier le travail de gestion des données à l'échelle de toute l'organisation. Il existe plusieurs options de classification des fichiers. Dans la plupart des scénarios, la classification se fait manuellement. Dans Windows Server 2012, l'infrastructure de classification des fichiers permet aux organisations de convertir ces processus manuels en stratégies automatisées. Les administrateurs peuvent spécifier des stratégies de gestion des fichiers selon la classification d'un fichier, et appliquer des règles d'entreprise pour gérer les données en fonction de leur valeur.

Vous pouvez utiliser la classification des fichiers pour effectuer les tâches suivantes :

1. Définir des propriétés et des valeurs de classification, que vous pouvez attribuer aux fichiers en exécutant des règles de classification.
2. Créer, mettre à jour et exécuter des règles de classification. Chaque règle attribue une propriété et une valeur prédéfinies uniques aux fichiers dans un répertoire spécifié, en fonction des plug-ins de classification installés.
3. Réévaluer les fichiers déjà classés lorsque vous exécutez une règle de classification. Vous pouvez choisir de remplacer des valeurs de classification existantes ou ajouter une valeur aux propriétés qui prennent en charge de plusieurs valeurs. Vous pouvez également utiliser des règles de classification pour déclasser les fichiers qui ne sont plus dans le critère de classification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les règles de classification ?



L'infrastructure de classification des fichiers utilise des règles de classification pour analyser automatiquement les fichiers et les classer en fonction de leur contenu. Vous configurez les classifications de fichiers dans la console du Gestionnaire de ressources du serveur de fichiers. Les propriétés de classification sont définies de manière centralisée dans AD DS, de sorte que ces définitions puissent être partagées à travers les serveurs de fichiers de l'entreprise. Vous pouvez créer des règles de classification qui analysent des fichiers à la recherche d'une chaîne standard, ou d'une chaîne correspondant à un modèle (expression régulière). Quand un paramètre configuré de classification est détecté dans un fichier, ce fichier est classifié comme configuré dans la règle de classification.

Pour organiser les classifications de fichiers, procédez comme suit :

1. Identifiez la ou les classification(s) que vous souhaitez appliquer aux documents.
2. Déterminez la méthode que vous souhaitez utiliser pour identifier des documents pour la classification.
3. Déterminez la planification des classifications automatiques.
4. Établissez une analyse du bon fonctionnement des classifications.

Une fois que vous avez défini les classifications, vous pouvez organiser l'implémentation du contrôle d'accès dynamique en définissant les expressions conditionnelles qui vous permettront de contrôler l'accès aux documents hautement confidentiels, suivant des attributs d'utilisateur particuliers.

Démonstration : Configuration de la classification des fichiers

Dans cette démonstration, vous allez apprendre à :

- créer une propriété de classification ;
- créer une règle de classification.

Procédure de démonstration

Créer une propriété de classification

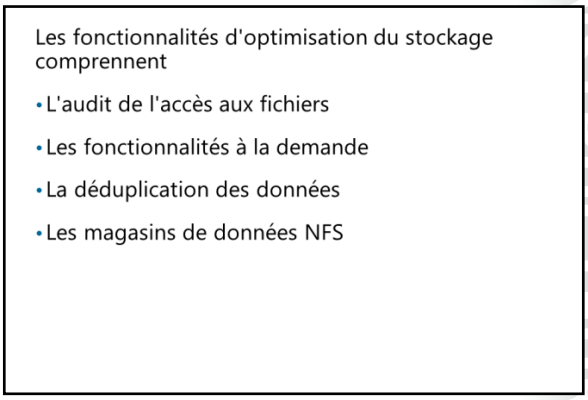
1. Sur LON-SVR1, la console Gestionnaire de serveur doit s'ouvrir automatiquement. À partir du Gestionnaire de serveur, démarrez le **Gestionnaire de ressources du serveur de fichiers**.
2. Dans le Gestionnaire de ressources du serveur de fichiers, créez une propriété locale avec les paramètres suivants :
    - Nom : **Documentation d'entreprise**
    - Type de propriété : **Oui/Non**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le Gestionnaire de ressources du serveur de fichiers, créez une règle de classification avec les paramètres suivants :
   - Onglet **Général**, **Nom de la règle** : **Règle de documents d'entreprise**. Vérifiez que la règle est activée.
   - Onglet **Étendue** : **E:\FichiersAtelier\Documentation d'entreprise**
   - Onglet **Classification,** Méthode de classification : **Classificateur de dossiers**
   - Propriété-Choisissez une propriété à attribuer aux fichiers : **Corporate Documentation**
   - Propriété-Spécifiez une valeur : **Oui**.
   - Onglet **Type d'évaluation**, **Réévaluer les valeurs de propriété existantes** et **Agréger les valeurs**.
4. **Exécutez la classification avec toutes les règles**, puis sélectionnez **Attendre la fin de la classification**.
5. Examinez le **Rapport de classification automatique** qui s'affiche dans Windows Internet Explorer® et vérifiez que le rapport affiche le même nombre de fichiers classés que dans le dossier **Corporate Documentation**.

Options d'optimisation du stockage dans Windows Server 2012

Windows Server 2012 comprend de nouvelles options pour l'optimisation du stockage, qui vous fournissent un moyen efficace pour déployer, administrer et sécuriser vos solutions de stockage. Les fonctionnalités d'optimisation du stockage comprennent ce qui suit :



- Audit de l'accès aux fichiers. Dans Windows Server 2012, l'auditd'accès aux fichiers crée un événement d'audit toutes les fois qu'un utilisateur accède aux fichiers. Par rapport aux versions précédentes de Windows Server, ces données d'événement d'audit contiennent des informations supplémentaires sur les attributs du fichier consulté.
- Fonctionnalités à la demande. Les fonctionnalités à la demande vous permettent d'économiser de l'espace disque en supprimant des fichiers de rôle et de fonctionnalité du système d'exploitation. Si vous devez installer ces rôles et fonctionnalités sur le serveur, les fichiers d'installation seront récupérés depuis des emplacements distants, des supports d'installation ou Windows Update. Vous pouvez supprimer des fichiers de fonctionnalité des ordinateurs physiques et virtuels, des fichiers d'image système Windows (.wim) et des disques durs virtuels hors connexion (VHD).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Déduplication des données. La déduplication des données identifie et supprime les doublons dans les données sans compromettre leur intégrité. La déduplication des données est très évolutive, rentable en ressources et non intrusive. Elle peut fonctionner simultanément sur de grands volumes de données primaires, sans affecter d'autres charges sur le serveur. La déduplication des données a un faible impact sur les charges de travail du serveur en limitant les ressources processeur et mémoire utilisées. Avec les tâches de déduplication des données, vous pouvez planifier à quel moment l'exécuter, spécifier les ressources à dédupliquer et régler avec précision la sélection des fichiers. Lorsqu'elles sont combinées avec la fonctionnalité BranchCache, les mêmes techniques d'optimisation sont appliquées aux données transférées via le réseau WAN à une succursale. Cela accélère les temps de téléchargement des fichiers et réduit la consommation de bande passante.
- Magasin de données NFS. Le magasin de données du système de fichiers réseau (NFS) est l'implémentation serveur NFS des systèmes d'exploitation Windows Server 2012. Dans Windows Server 2012, le système de fichiers réseau prend en charge la haute disponibilité, ce qui signifie que vous pouvez déployer le serveur dans une configuration de clustering avec basculement. Lorsqu'un client se connecte à un serveur NFS dans le cluster de basculement et que ce serveur tombe en panne, le serveur NFS bascule sur un autre nœud du cluster, de sorte que le client peut encore se connecter au serveur NFS.

Démonstration : Configuration de la déduplication des données

Dans cette démonstration, vous allez apprendre à :

- ajouter le service de rôle de déduplication des données ;
- activer la déduplication des données ;
- tester la déduplication des données.

Procédure de démonstration

Ajouter le service de rôle de déduplication des données

1. Ouvrez une session sur **LON-SVR1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Gestionnaire de serveur**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, installez les rôles et fonctionnalités suivants sur le serveur local et acceptez les valeurs par défaut :
    - **Service de fichiers et de stockage (Installé)\Services de fichiers et iSCSI (Installé)\ Déduplication des données**

Activer la déduplication des données

1. Dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Service de fichiers et de stockage**, puis cliquez sur **Volumes**.
2. Dans le volet Volumes, cliquez avec le bouton droit sur le lecteur **E:** et sélectionnez **Configurer la déduplication des données**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Configurez la déduplication des données avec les paramètres suivants :
   - Activer la déduplication des données : **Activé**
   - Dédupliquer les fichiers de plus de (en jours) : **3**
   - Définir la planification de la déduplication : **Activer l'optimisation du débit**
   - Heure de début : **heure actuelle**

Tester la déduplication des données

1. Sur LON-SVR1, copiez le dossier **OBSInstaller.exe** du dossier racine du lecteur E: dans le dossier **E:\LabFiles** .
2. Vérifiez la taille du fichier aux deux emplacements.
3. Dans Windows PowerShell, sur LON-SVR1, saisissez l'applet de commande suivante pour démarrer la tâche de déduplication en mode d'optimisation :

```
Start-DedupJob –Type Optimization –Volume E:
```

4. Une fois la tâche terminée, vérifiez la taille du fichier **OBSInstaller.exe** dans le dossier racine du lecteur E:.
5. Dans la boîte de dialogue **Propriétés** du fichier OBSInstaller.exe, notez les valeurs pour **Taille** et **Taille sur le disque**. La taille sur le disque devrait être beaucoup plus petite qu'elle l'était précédemment.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique A : Implémentation des services de fichiers avancés

Scénario

À mesure que la société A. Datum Corporation s'est développée, ses besoins en matière de gestion du stockage et d'accès aux fichiers partagés ont également évolué. Bien que le coût du stockage ait sensiblement baissé au cours des quelques dernières années, la quantité de données générées par les groupes de l'entreprise a augmenté encore plus vite. Cette organisation envisage d'autres moyens pour réduire le coût de stockage des données sur le réseau et réfléchit aux options disponibles pour optimiser l'accès aux données dans les nouvelles succursales. L'organisation voudrait également s'assurer que les données stockées dans les dossiers partagés soient limitées aux données de l'entreprise, et qu'elles n'incluent pas des types de fichier non autorisés.

En tant que principal administrateur réseau chez A. Datum, vous êtes chargé d'implémenter les nouvelles technologies de stockage de fichiers pour l'organisation. Vous implémenterez le stockage iSCSI pour fournir une option moins compliquée pour déployer de grandes capacités de stockage.

Objectifs

- configurer le stockage iSCSI ;
- configurer l'infrastructure de classification des fichiers.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-SVR2**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

Avant de démarrer les ordinateurs virtuels pour cet atelier pratique, procéder comme suit pour **22412B-LON-DC1** seulement :

1. Sur l'ordinateur hôte, cliquez sur **Gestionnaire Hyper-V** dans la barre des tâches.
2. Dans la console Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Paramètres**.
3. Dans la fenêtre **Paramètres pour 22412B-LON-DC1**, dans le volet gauche, assurez-vous que la première carte réseau héritée est connectée à **Réseau privé** et que la deuxième carte réseau héritée est connectée à **Réseau privé 2**.
4. S'il n'y a qu'une seule carte réseau héritée, cliquez sur **Ajout de matériel** dans le volet gauche, cliquez sur **Carte réseau héritée** dans le volet droit, cliquez sur **Ajouter** puis, dans la liste déroulante **Réseau** du volet droit, sélectionnez **Réseau privé 2**. Cliquez sur **OK**.

 **Remarque :** Vous ne pouvez effectuer l'étape précédente que si LON-DC1 n'a pas été démarré. Si LON-DC1 est déjà démarré, arrêtez-le puis suivez la procédure.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
6. Dans le Gestionnaire Hyper-V, cliquez sur **22412B-LON-DC1** et, dans le volet Actions, cliquez sur **Accueil**.
7. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
8. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
9. Répétez les étapes 6 à 8 pour **22412B-LON-SVR1** et **22412B-LON-SVR2**.

Exercice 1 : Configuration du stockage iSCSI

Scénario

Pour réduire le coût et la complexité de la configuration du stockage centralisé, A. Datum a décidé d'utiliser iSCSI pour fournir le stockage. Pour commencer, vous allez installer et configurer la cible iSCSI, puis configurer l'accès à la cible en configurant les initiateurs iSCSI.

Les tâches principales de cet exercice sont les suivantes :

1. Installer la fonctionnalité de cible iSCSI
2. Configurer les cibles iSCSI
3. Configurer les services MPIO
4. Se connecter aux cibles iSCSI et les configurer

▶ Tâche 1 : Installer la fonctionnalité de cible iSCSI

1. Ouvrez une session sur **LON-DC1** avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Gestionnaire de serveur**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, installez les rôles et fonctionnalités suivants sur le serveur local et acceptez les valeurs par défaut :
   - **Service de fichiers et de stockage (Installé)**\S**ervices de fichiers et iSCSI (Installé)**\ **Serveur cible iSCSI**

▶ Tâche 2 : Configurer les cibles iSCSI

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**, puis sur **iSCSI**.
2. Créez un disque virtuel avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk1**
   - Taille : **5 Go**
   - Cible iSCSI : **Nouveau**
   - Nom de la cible : **lon-dc1**
   - Serveurs d'accès : **172.16.0.22** et **131.107.0.2**
3. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

4. Créez un nouveau disque virtuel iSCSI avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk2**
   - Taille : **5 Go**
   - Cible iSCSI : **lon-dc1**
5. Créez un nouveau disque virtuel iSCSI avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk3**
   - Taille : **5 Go**
   - Cible iSCSI : **lon-dc1**
6. Créez un nouveau disque virtuel iSCSI avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk4**
   - Taille : **5 Go**
   - Cible iSCSI : **lon-dc1**
7. Créez un nouveau disque virtuel iSCSI avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk5**
   - Taille : **5 Go**
   - Cible iSCSI : **lon-dc1**

▶ Tâche 3 : Configurer les services MPIO

1. Ouvrez une session sur **LON-SVR2** avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Sur LON-SVR2, dans le Gestionnaire de serveur, ouvrez la console **Routage et accès distant**.
3. Attendez que l'**Assistant Activation de DirectAccess** s'affiche, puis annulez l'l'Assistant Activation de DirectAccess.
4. Cliquez avec le bouton droit sur **LON-SVR2**, puis cliquez sur **Désactiver le routage et l'accès à distance**. Cliquez sur **Oui**, puis fermez la console Routage et accès distant.

 **Remarque :** Normalement, vous ne désactivez pas Routage et accès distant (RRAS) avant de configurer la fonctionnalité MPIO. Vous le faites ici en raison de la configuration requise pour l'atelier pratique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans Gestionnaire de serveur, démarrez l'Assistant Ajout de rôles et de fonctionnalités et installez la fonctionnalité **MPIO (Multipath I/O)**.
6. Dans Gestionnaire de serveur, dans le menu **Outils**, ouvrez **Initiateur iSCSI** et configurez les éléments suivants :
   - Activez le service **Initiateur iSCSI**.
   - Établissez une **Connexion rapide** avec la cible : **LON-DC1**
7. Dans Gestionnaire de serveur, dans le menu **Outils**, ouvrez **MPIO** et configurez les éléments suivants :
   - Activez **Ajouter la prise en charge des périphériques iSCSI** sur **Découvrir plusieurs chemins**
8. Lorsque l'ordinateur a redémarré, ouvrez une session sur LON-SVR2 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
9. Dans le Gestionnaire de serveur, dans le menu **Outils**, cliquez sur **MPIO** et vérifiez que **ID du matériel de périphérique MSFT2005iSCSIBusType_0x9** est ajouté à la liste.

▶ Tâche 4 : Se connecter aux cibles iSCSI et les configurer

1. Sur LON-SVR2, dans le Gestionnaire de serveur, dans le menu **Outils**, ouvrez **Initiateur iSCSI**.
2. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, effectuez les opérations suivantes :
   - **Déconnectez** toutes les **Cibles**.
   - Cliquez sur **Connexion** et **Activer la prise en charge de plusieurs chemins d'accès**.
   - Définissez les options **Avancé** comme suit :
     - Carte locale : **Initiateur Microsoft iSCSI**
     - IP de l'initiateur : **172.16.0.22**
     - IP du portail cible : **172.16.0.10 / 3260**
   - **Connectez-vous** à une autre cible, **activez la prise en charge de plusieurs chemins d'accès** et configurez les paramètres **Avancé** suivants :
     - Carte locale : **Initiateur Microsoft iSCSI**
     - IP de l'initiateur : **131.107.0.2**
     - IP du portail cible : **131.107.0.1 / 3260**
3. Dans la liste **Cibles**, ouvrez **Périphériques** pour **iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target**, accédez aux informations MPIO, puis vérifiez que dans **Stratégie d'équilibrage de charge**, **Tourniquet** est sélectionné. Vérifiez que deux chemins d'accès sont répertoriés en consultant les adresses IP des deux cartes réseau.

Résultats : À la fin de cet exercice, vous aurez configuré les cibles iSCSI et vous serez connecté à ces cibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration de l'infrastructure de classification des fichiers

Scénario

La société A. Datum a remarqué que beaucoup d'utilisateurs copient la documentation d'entreprise sur les lecteurs mappés de leur serveur de fichiers ou celui du service. En conséquence, il y a beaucoup de différentes versions des mêmes documents sur le réseau. Pour veiller à ce que seule la version la plus récente des documents soit disponible pour la plupart des utilisateurs, vous devez configurer un système de classification des fichiers qui supprimera des fichiers spécifiques des répertoires utilisateurs.

Les tâches principales de cet exercice sont les suivantes :

1. Créer une propriété de classification pour la documentation d'entreprise
2. Créer une règle de classification pour la documentation d'entreprise
3. Créer une règle de classification s'appliquant à un dossier partagé
4. Créer une tâche de gestion de fichiers pour l'expiration des documents d'entreprise
5. Vérifier que les documents d'entreprise sont expirés
6. Pour préparer l'atelier suivant

▶ Tâche 1 : Créer une propriété de classification pour la documentation d'entreprise

1. Sur LON-SVR1, démarrez le **Gestionnaire de ressources du serveur de fichiers** depuis le Gestionnaire de serveur.
2. Dans le Gestionnaire de ressources du serveur de fichiers, sous **Gestion de la classification**, créez une propriété locale avec les paramètres suivants :
   - Nom : **Corporate Documentation**
   - Type de propriété : **Oui/Non**
3. Laissez le Gestionnaire de ressources du serveur de fichiers ouvert.

▶ Tâche 2 : Créer une règle de classification pour la documentation d'entreprise

1. Dans la console du Gestionnaire de ressources du serveur de fichiers, créez une règle de classification avec les paramètres suivants :
   - Onglet **Général**, Nom de la règle : **Règle de documents d'entreprise,** et assurez-vous que la règle est activée.
   - Onglet **Étendue** : **dossier E:\Labfiles\Corporate Documentation**
   - Onglet **Classification** :
     - Méthode de classification : **Classificateur de dossiers**
     - Propriété, Choisissez une propriété à attribuer aux fichiers : **Corporate Documentation**
     - Propriété, Spécifiez une valeur : **Oui**
     - Onglet Type d'évaluation : **Réévaluer les valeurs de propriété existantes** et **Agréger les valeurs**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

2. Sélectionnez à la fois **Exécuter la classification avec toutes les règles** et **Attendre la fin de la classification**.
3. Examinez le Rapport de classification automatique qui s'affiche dans Windows Internet Explorer et vérifiez que le rapport affiche le même nombre de fichiers classés que dans le dossier Documentation d'entreprise.

   Fermez Internet Explorer, mais laissez la console du Gestionnaire de ressources du serveur de fichiers ouverte.

▶ Tâche 3 : Créer une règle de classification s'appliquant à un dossier partagé

1. Dans la console du Gestionnaire de ressources du serveur de fichiers, créez une propriété locale avec les paramètres suivants :
   - Nom : **Expiration Date**
   - Type de propriété : **Date-heure**
2. Dans la console du Gestionnaire de ressources du serveur de fichiers, créez une règle de classification avec les paramètres suivants :
   - Onglet **Général**, Nom de la règle : **Expiration Rule**, et assurez-vous que la règle est activée.
   - Onglet **Portée** : **E:\Labfiles\Corporate Documentation**
   - Onglet **Classification,** Méthode de classification : **Classificateur de dossiers**
   - Propriété, Choisissez une propriété à attribuer aux fichiers : **Expiration Date**
   - Onglet **Type d'évaluation** : **Réévaluer les valeurs de propriété existantes** et **Agréger les valeurs**
3. Sélectionnez à la fois **Exécuter la classification avec toutes les règles** et **Attendre la fin de la classification**.
4. Examinez le Rapport de classification automatique qui s'affiche dans Windows Internet Explorer et vérifiez que le rapport affiche le même nombre de fichiers classifiés que dans le dossier Documentation d'entreprise.
5. Fermez Internet Explorer, mais laissez la console du Gestionnaire de ressources du serveur de fichiers ouverte.

▶ Tâche 4 : Créer une tâche de gestion de fichiers pour l'expiration des documents d'entreprise

- Dans le Gestionnaire de ressources du serveur de fichiers, créez une tâche de gestion de fichiers avec les paramètres suivants :
  - Onglet **Général**, Nom de la tâche : **Expired Corporate Documents**, et assurez-vous que la tâche est activée
  - Onglet **Portée** : **E:\Labfiles\Corporate Documentation**
  - Onglet **Action**, Type : **Expiration de fichier** est sélectionné

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Répertoire d'expiration : **E:\Labfiles\Expired**
- Onglet **Notification** : **Journal des événements** et **Envoyer un avertissement au journal des événements**
- Onglet **Condition,** Nombre de jours depuis la dernière modification au fichier : **1**

Remarque : Cette valeur est fournie aux fins de l'atelier pratique uniquement. Dans un scénario réel, la valeur serait de 365 jours ou plus, selon la stratégie de chaque société.

- Onglet Planification : Hebdomadaire et dimanche
- Laissez le Gestionnaire de ressources du serveur de fichiers ouvert.

▶ Tâche 5 : Vérifier que les documents d'entreprise sont expirés

1. Dans le Gestionnaire de ressources du serveur de fichiers, cliquez sur **Exécuter maintenant une tâche de gestion de fichiers**, puis cliquez sur **Attendre la fin de l'exécution de la tâche**.
2. Examinez le Rapport de tâche de gestion de fichiers qui s'affiche dans Windows Internet Explorer et vérifiez que le rapport affiche le même nombre de fichiers classés que dans le dossier Documentation d'entreprise.
3. Démarrez l'observateur d'événements et ouvrez le **Journal d'événements d'applications** .
4. Examinez les événements portant les numéros **908** et **909**. Notez que 908 – FSRM a démarré une tâche de gestion de fichiers et que 909 – FSRM a terminé une tâche de gestion de fichiers.

Résultats : Après avoir terminé cet exercice, vous aurez configuré une infrastructure de classification des fichiers de sorte que la version la plus récente de la documentation est toujours à la disposition des utilisateurs.

▶ Pour préparer l'atelier suivant

Une fois l'atelier pratique terminé, rétablissez la configuration de 22412B-LON-SVR2. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-SVR2**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.

   Laissez tous les autres ordinateurs virtuels en fonctionnement pour l'atelier suivant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Implémentation de la fonctionnalité BranchCache

Scénario

La société A Datum Corporation a déployé une nouvelle succursale, qui dispose d'un serveur unique. Pour optimiser l'accès aux fichiers dans les succursales, vous devez configurer BranchCache. Pour limiter l'utilisation du réseau WAN à la succursale, vous devez configurer BranchCache pour récupérer les données depuis le siège social. Vous implémenterez également le Gestionnaire de ressources du serveur de fichiers pour aider à optimiser le stockage des fichiers.

Objectifs

- Configurer les serveurs du siège social pour la fonctionnalité BranchCache.
- Configurer les serveurs des succursales pour la fonctionnalité BranchCache.
- Configurer les ordinateurs client pour la fonctionnalité BranchCache.
- Contrôler BranchCache.

Configuration de l'atelier pratique

Durée approximative : 40 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-CL1** **22412B-LON-CL2**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22412B-LON-DC1** et, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22412B-LON-SVR1**, **22412B-LON-CL1**, et **22412B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration des serveurs du siège social pour la fonctionnalité BranchCache

Scénario

Pour configurer la fonctionnalité BranchCache pour vos succursales, vous devez configurer les composants réseau.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer LON-DC1 pour utiliser Windows BranchCache
2. Simuler une liaison lente avec la succursale
3. Activer un partage de fichiers pour BranchCache
4. Configurer les règles de pare-feu des clients pour BranchCache

▶ Tâche 1 : Configurer LON-DC1 pour utiliser Windows BranchCache

1. Basculez vers **LON-DC1**.
2. Ouvrez le Gestionnaire de serveur et installez le service de rôle **BranchCache pour fichiers réseau**.
3. Ouvrez l'Éditeur de stratégie de groupe locale (**gpedit.msc**).
4. Accédez à **Configuration ordinateur/Modèles d'administration/Réseau/Serveur Lanman/ Publication des hachages pour BranchCache** et ouvrez ce paramètre.
5. Activez le paramètre BranchCache puis sélectionnez **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**.

▶ Tâche 2 : Simuler une liaison lente avec la succursale

1. Dans la console de l'Éditeur de stratégie de groupe locale, naviguez jusqu'à **Configuration ordinateur\Paramètres Windows\QoS basée sur la stratégie**.
2. Créez une nouvelle stratégie avec les paramètres suivants :
   - Nom : **Limiter à 100 Kbits/s**
   - Spécifier le taux d'accélération en sortie : **100**
   - Acceptez les valeurs par défaut sur les autres pages de l'Assistant

▶ Tâche 3 : Activer un partage de fichiers pour BranchCache

1. Dans une fenêtre de l'Explorateur de fichiers, créez un nouveau dossier intitulé **C:\Partage**.
2. Partagez ce dossier avec les propriétés suivantes :
   - Nom de partage : **Partage**
   - Autorisations : valeur par défaut
   - Mise en cache : **Activer BranchCache**
3. Copiez **C:\Windows\System32\mspaint.exe** dans le dossier **C:\Partage**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer les règles de pare-feu des clients pour BranchCache

1. Sur LON-DC1, ouvrez **Gestion des stratégies de groupe**.
2. Accédez à **Forêt : Adatum.com\Domaines\Adatum.com\Default Domain Policy** et ouvrez la stratégie pour la modifier.
3. Naviguez jusqu'à **Configuration ordinateur\Stratégies\Paramètres Windows\ Paramètres de sécurité\Pare-feu Windows avec fonctions avancées de sécurité\ Pare-feu Windows avec fonctions avancées de sécurité\Règles de trafic entrant**.
4. Créez une nouvelle règle de trafic entrant avec les propriétés suivantes :
   a. Type de règle : **prédéfini**
   b. Utilisez **BranchCache – Extraction du contenu (utilise HTTP)**
   c. Action : **Autoriser**
5. Créez une nouvelle règle de trafic entrant avec les propriétés suivantes :
   d. Type de règle : **prédéfini**
   e. Utilisez **BranchCache – Découverte d'homologue (utilise WSD)**
   f. Action : **Autoriser**
6. Fermez les consoles Éditeur de gestion des stratégies de groupe et Gestion des stratégies de groupe.

Résultats : À la fin de cet exercice, vous aurez déployé BranchCache, configuré une liaison lente et activé BranchCache sur un partage de fichiers.

Exercice 2 : Configuration des serveurs de succursale pour la fonctionnalité BranchCache

Scénario

L'étape suivante consiste à configurer un serveur de fichiers pour la fonctionnalité BranchCache. Vous installerez la fonctionnalité BranchCache, demanderez un certificat, puis l'associerez à BranchCache.

Les tâches principales de cet exercice sont les suivantes :

1. Installer la fonctionnalité BranchCache sur LON-SVR1
2. Mettre en marche le serveur hôte BranchCache

▶ Tâche 1 : Installer la fonctionnalité BranchCache sur LON-SVR1

- Sur LON- SVR1, dans le Gestionnaire de serveur, ajoutez le service de rôle **BranchCache pour fichiers réseau** et la fonctionnalité **BranchCache**.

▶ Tâche 2 : Mettre en marche le serveur hôte BranchCache

1. Sur LON-DC1, ouvrez Utilisateurs et ordinateurs Active Directory et créez une nouvelle unité d'organisation appelée **BranchCacheHost**.
2. Déplacez **LON-SVR1** dans l'unité d'organisation **BranchCacheHost**.

3. Ouvrez **Gestion des stratégies de groupe** et bloquez l'héritage Objet stratégie de groupe sur l'unité d'organisation **BranchCacheHost**.
4. Redémarrez **LON-SVR1** et ouvrez une session en tant que **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
5. Sur LON-SVR1, ouvrez **Windows PowerShell** et exécutez l'applet de commande suivante :

```
Enable-BCHostedServer
-RegisterSCP
```

6. Sur LON-SVR1, dans Windows PowerShell, exécutez l'applet de commande suivante :

```
Get-BCStatus
```

7. Assurez-vous que la fonctionnalité BranchCache est activée et en cours d'exécution.

Résultats : À la fin de cet exercice, vous aurez activé le serveur BranchCache dans la succursale.

Exercice 3 : Configuration des ordinateurs clients pour la fonctionnalité BranchCache

Scénario

Après avoir configuré les composants du réseau, vous devez vérifier que les ordinateurs client sont configurés correctement. Il s'agit d'une tâche préparatoire à l'utilisation de BranchCache.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les ordinateurs client pour utiliser BranchCache en mode de cache hébergé

▶ Tâche 1 : Configurer les ordinateurs client pour utiliser BranchCache en mode de cache hébergé

1. Sur LON-DC1, ouvrez le Gestionnaire de serveur puis Gestion des stratégies de groupe.
2. Modifiez **Default Domain Policy**.
3. Dans l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\Stratégies\Modèles d'administration\Réseau\BranchCache** et configurez ce qui suit :
   a. Activer BranchCache : **Activé**
   b. Activer la découverte automatique de cache hébergé par point de connexion de service : **Activé**
   c. Configurer BranchCache pour les fichiers réseau : **Activé**
   d. Saisissez la valeur maximum de latence du parcours circulaire du réseau (millisecondes) au-delà de laquelle commence la mise en cache : **0**
4. Démarrez **22412B-LON-CL1**, ouvrez une fenêtre d'invite de commandes et actualisez les paramètres de Stratégie de groupe en utilisant la commande **gpupdate /force**.
5. À l'invite de commandes, saisissez **netsh branchcache show status all**, et appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Vérifiez que BranchCache est **Activé** avec l'état **En cours d'exécution** et que les options de la Stratégie de groupe sont appliquées. Si l'état est défini sur **Arrêté**, répétez les étapes 4 et 5.
7. Démarrez **22412B-LON-CL2**, ouvrez la fenêtre d'invite de commandes et actualisez les paramètres de Stratégie de groupe en utilisant la commande **gpupdate /force**.
8. À l'invite de commandes, saisissez **netsh branchcache show status all**, et appuyez sur Entrée.
9. Vérifiez que BranchCache est **Activé** avec l'état **En cours d'exécution** et que les options de la Stratégie de groupe sont appliquées. Si l'état est défini sur **Arrêté**, répétez les étapes 7 et 8.

Résultats : À la fin de cet exercice, vous aurez configuré les ordinateurs client pour BranchCache.

Exercice 4 : Contrôle de la fonctionnalité BranchCache

Scénario

En conclusion, vous devez tester et vérifier que la fonctionnalité BranchCache fonctionne comme prévu.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer l'Analyseur de performances sur LON-SVR1
2. Configurer les statistiques de performances sur LON-CL1
3. Configurer les statistiques de performances sur LON-CL2
4. Tester la fonctionnalité BranchCache en mode de cache hébergé

▶ Tâche 1 : Configurer l'Analyseur de performances sur LON-SVR1

1. Sur LON-SVR1, ouvrez l'**Analyseur de performances**.
2. Dans la console de l'Analyseur de performance, dans le volet de navigation, sous **Outils d'analyse**, cliquez sur **Analyseur de performances**.
3. Supprimez les compteurs existants, passez en vue du rapport, puis ajoutez les compteurs d'objet **BranchCache** au rapport.

▶ Tâche 2 : Configurer les statistiques de performances sur LON-CL1

1. Basculez vers **LON-CL1** et ouvrez l'**Analyseur de performances**.
2. Dans le volet de navigation de la console Analyseur de performances, sous **Outils d'analyse**, cliquez sur **Analyseur de performances**.
3. Dans l'Analyseur de performances, supprimez les compteurs existants, passez en vue de rapport, puis ajoutez les objets **BranchCache** au rapport.

▶ Tâche 3 : Configurer les statistiques de performances sur LON-CL2

1. Basculez vers **LON-CL2** et ouvrez l'**Analyseur de performances**.
2. Dans la console de l'Analyseur de performance, dans le volet de navigation, sous **Outils d'analyse**, cliquez sur **Analyseur de performances**.
3. Dans l'Analyseur de performances, supprimez les compteurs existants, passez en vue de rapport, puis ajoutez les objets **BranchCache** au rapport.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Tester la fonctionnalité BranchCache en mode de cache hébergé

1. Basculez vers **LON-CL1**.
2. Ouvrez **\\LON-DC1.adatum.com\partage** et copiez **mspaint.exe** sur le Bureau local. Cela peut prendre plusieurs minutes en raison de la liaison lente simulée.
3. Lisez les statistiques de performance sur LON-CL1. Ce fichier a été récupéré depuis LON-DC1 (récupération : octets du serveur). Après que le fichier a été mis en cache localement, il a été transféré au cache hébergé. (récupération : octets traités).
4. Basculez vers **LON-CL2**.
5. Ouvrez **\\LON-DC1.adatum.com\partage** et copiez **mspaint.exe** sur le Bureau local. Ceci ne devrait pas prendre aussi longtemps, car le fichier a été mis en cache.
6. Lisez les statistiques de performance sur LON-CL2. Ce fichier a été obtenu à partir du cache hébergé (récupération : octets du cache).
7. Lisez les statistiques de performance sur LON-SVR1. Ce serveur a fourni les données en mémoire cache aux clients (cache hébergé : offres de segments de fichiers effectuées).

Résultats : À la fin de cet exercice, vous aurez vérifié que BranchCache fonctionne comme prévu.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-CL1** et **22412B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir



Méthode conseillée :

- Lorsque vous envisagez une solution de stockage iSCSI pour votre organisation, consacrez la plus grande partie de votre temps au processus de conception. Le processus de conception est essentiel parce qu'il vous permet d'optimiser la solution pour toutes les technologies qui utiliseront le stockage iSCSI, comme les services de fichier, Exchange Server ou SQL Server. La conception doit également s'adapter à la croissance future des données d'entreprise de votre organisation. Les processus de conception réussis garantissent un déploiement réussi de la solution, qui répondra aux exigences stratégiques de votre organisation.
- Lorsque vous planifiez un déploiement de BranchCache, assurez-vous de travailler en étroite collaboration avec vos administrateurs réseau, afin de pouvoir optimiser le trafic sur le réseau WAN.
- En planifiant la classification des fichiers, veillez à commencer par les exigences stratégiques de votre organisation. Identifiez les classifications que vous appliquerez aux documents, puis définissez une méthode que vous utiliserez pour identifier des documents pour la classification. Avant de déployer l'infrastructure de classification des fichiers, créez un environnement de test et testez les scénarios pour vous assurer que la solution se traduira par un déploiement réussi, et que les exigences stratégiques de votre organisation seront satisfaites.

Questions de contrôle des acquis

Question : En quoi la fonctionnalité BranchCache diffère-t-elle du système de fichiers distribués (DFS) ?

Question : Pourquoi préféreriez-vous implémenter BranchCache en mode de cache hébergé plutôt qu'en mode de cache distribué ?

Question : Pouvez-vous configurer la déduplication des données sur un volume de démarrage ?

Question : Pourquoi implémenteriez-vous une infrastructure de classification des fichiers ?

Problèmes réels et scénarios

Question : Votre organisation envisage de déployer une solution iSCSI. Vous êtes l'administrateur Windows Server 2012 responsable de la conception et du déploiement de la nouvelle solution. Cette nouvelle solution sera utilisée par différents types de technologies, dont le serveur de fichiers Windows Server 2012, Exchange Server et SQL Server. Vous devez relever le défi de concevoir une solution iSCSI optimale, mais en même temps vous n'êtes pas sûr si la solution que vous allez proposer à votre organisation répondra aux exigences de toutes les technologies qui accèderont au stockage iSCSI. Que devez-vous faire ?

Question : Votre organisation envisage de déployer une solution BranchCache. Vous êtes l'administrateur Windows Server 2012 responsable de la conception et du déploiement de la nouvelle solution dans votre organisation. Les directeurs commerciaux de l'organisation sont préoccupés par la sécurité des données qui seront stockées dans les succursales. Ils s'inquiètent également de la façon dont l'organisation gèrera les risques de sécurité tels que l'altération des données, la divulgation d'informations et les attaques par déni de service. Que devez-vous faire ?

Question : Votre organisation utilise de grandes quantités d'espace disque pour le stockage des données et rencontre des difficultés pour organiser et gérer ces données. Votre organisation doit par ailleurs répondre à certaines exigences en matière de sécurité, de conformité et de prévention des vols de données pour les informations confidentielles. Que devez-vous faire ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Outils

Outil	Utilisation	Emplacement
Serveur cible iSCSI	Configurer des cibles iSCSI	Dans le Gestionnaire de serveur, sous Serveurs de fichiers et de stockage
Initiateur iSCSI	Configurer un client pour se connecter à un disque virtuel de cible iSCSI	Dans le Gestionnaire de serveur, dans la zone de liste déroulante Outils
Outil d'évaluation de la déduplication (DDPEval.exe)	Analyser un volume pour découvrir les gains potentiels de la déduplication des données	C:\windows\system32
Gestionnaire de ressources du serveur de fichiers	Ensemble de fonctionnalités qui vous permettent de gérer et classer les données stockées sur des serveurs de fichiers	Gestionnaire de serveur

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3

Implémentation du contrôle d'accès dynamique

Table des matières :

Vue d'ensemble du module **3-1**

Leçon 1 : Vue d'ensemble du contrôle d'accès dynamique **3-2**

Leçon 2 : Planification du contrôle d'accès dynamique **3-9**

Leçon 3 : Déploiement du contrôle d'accès dynamique **3-15**

Atelier pratique : Implémentation du contrôle d'accès dynamique **3-27**

Contrôle des acquis et éléments à retenir **3-37**

Vue d'ensemble du module

Le système d'exploitation Windows Server® 2012 présente une nouvelle fonctionnalité pour améliorer le contrôle d'accès aux ressources basées sur des fichiers et sur des dossiers. Cette fonctionnalité, appelée contrôle d'accès dynamique, étend le contrôle d'accès basé sur les systèmes de fichier NTFS réguliers en permettant aux administrateurs d'utiliser les revendications, les propriétés de ressource, les stratégies et les expressions conditionnelles dans la gestion de l'accès. Dans ce module, vous découvrirez le contrôle d'accès dynamique, comment l'organiser et comment l'implémenter.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire le contrôle d'accès dynamique et ses composants ;
- planifier l'implémentation du contrôle d'accès dynamique ;
- implémenter le contrôle d'accès dynamique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble du contrôle d'accès dynamique

Le contrôle d'accès dynamique est une nouvelle fonctionnalité de Windows Server 2012 que vous pouvez utiliser pour la gestion des accès. Le contrôle d'accès dynamique est une nouvelle manière de sécuriser et contrôler l'accès aux ressources. Avant d'implémenter cette fonctionnalité, vous devrez comprendre son fonctionnement et connaître ses composants. Cette leçon présente une vue d'ensemble sur le contrôle d'accès dynamique.

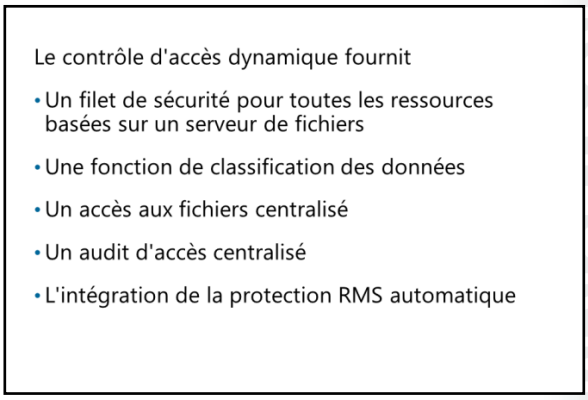
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- définir le contrôle d'accès dynamique ;
- décrire les technologies de base du contrôle d'accès dynamique ;
- comparer le contrôle d'accès dynamique avec des technologies d'autorisation similaires, telles que les autorisations NTFS et les Services RMS (AD RMS) de Active Directory® ;
- définir l'identité ;
- définir les revendications et les types de revendication ;
- définir une stratégie d'accès centralisée.

Qu'est-ce que le contrôle d'accès dynamique ?

Généralement, la plupart des entreprises enregistrent leurs données sur des serveurs de fichiers. Par conséquent, les administrateurs informatiques doivent offrir un niveau de sécurité et un contrôle d'accès appropriés aux ressources du serveur de fichiers. Dans les versions antérieures de Windows Server, les administrateurs informatiques contrôlaient la plupart des accès aux ressources du serveur de fichiers à l'aide des autorisations NTFS et des listes de contrôle d'accès.



Le contrôle d'accès dynamique dans Windows Server 2012 est un nouveau mécanisme de contrôle d'accès destiné aux ressources du système de fichiers. Il permet aux administrateurs de définir des stratégies centrales d'accès aux fichiers, pouvant s'appliquer à chaque serveur de fichiers de l'entreprise. Le contrôle d'accès dynamique intègre un filet de sécurité entre les serveurs de fichiers et entre tous les partages et toutes les autorisations NTFS existants. Il permet également d'assurer que quelle que soit la manière dont le partage et les autorisations NTFS pourraient changer, cette stratégie de remplacement centrale est toujours appliquée. Le contrôle d'accès dynamique combine plusieurs critères dans la décision d'accès. Ceci augmente la liste de contrôle d'accès (ACL) de NTFS, afin que les utilisateurs soient obligés de respecter la stratégie de contrôle d'accès de NTFS et la stratégie d'accès centralisée pour accéder au fichier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le contrôle d'accès dynamique est un moyen flexible pour appliquer et gérer l'accès et l'audit des serveurs de fichiers basés sur un domaine. Le contrôle d'accès dynamique utilise les revendications dans le jeton d'authentification, les propriétés de ressource sur la ressource les et expressions conditionnelles dans l'autorisation et les entrées d'audit. Avec cette combinaison de fonctionnalités, vous pouvez désormais accorder l'accès aux fichiers et dossiers suivant les attributs des services de domaine Active Directory (AD DS).

Le contrôle d'accès dynamique fournit :

- Une fonction de classification des données. Vous pouvez utiliser la classification de fichiers automatique et manuelle pour référencer les données dans des serveurs de fichiers à travers l'entreprise.
- Un fonction de contrôle d'accès aux fichiers. Les stratégies d'accès centralisé permettent aux entreprises de définir, par exemple, les personnes autorisées à accéder aux informations de santé au sein d'une entreprise.
- Une fonction d'audit de l'accès aux fichiers. Vous pouvez utiliser des stratégies centrales d'audit pour la création de rapports de conformité et des analyses d'investigation. Par exemple, vous pouvez identifier qui a accédé aux informations hautement confidentielles.
- L'intégration facultative d'une protection RMS. Vous pouvez utiliser le chiffrement RMS (Rights Management Services) pour les documents Microsoft® Office. Par exemple, vous pouvez configurer RMS pour chiffrer tous les documents contenant des informations sur la loi américaine HIPAA (Health Insurance Portability and Accountability Act).

Le contrôle d'accès dynamique a été conçu pour quatre scénarios :

- Stratégie d'accès centralisée pour l'accès aux fichiers. Permet aux entreprises de définir des stratégies de filet de sécurité conformes à l'entreprise et aux réglementations.
- Audit pour la conformité et l'analyse. Permet d'effectuer un audit ciblé à travers les serveurs de fichiers, pour la création de rapport de conformité et des analyses d'investigation.
- Protection des informations confidentielles. Identifie et protège les informations confidentielles au sein et en dehors d'un environnement Windows Server 2012.
- Action corrective en cas d'accès refusé. Améliore l'expérience d'accès refusé, de manière à réduire la charge de support technique et le temps d'incident lors de la résolution.

Les technologies de base du contrôle d'accès dynamique

Le contrôle d'accès dynamique combine beaucoup de technologies issues de Windows Server 2012, pour fournir une expérience flexible en matière d'autorisation précise et d'audit. Le contrôle d'accès dynamique utilise les technologies suivantes :

- AD DS et ses technologies dépendantes pour la gestion réseau de l'entreprise.
- Le protocole Kerberos version 5 (V5), notamment l'identité composée pour une authentification sécurisée.

Le contrôle d'accès dynamique repose sur de nombreuses technologies de Windows Server 2012, telles que

- AD DS
- Kerberos V5
- La sécurité de Windows
- Les classifications de fichiers
- L'audit
- RMS

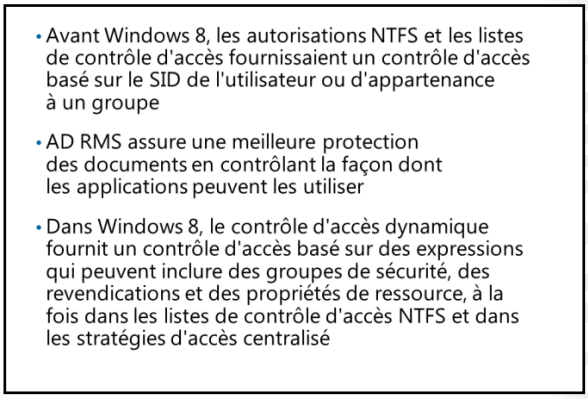
- La sécurité Windows (autorité de sécurité locale (LSA), service d'ouverture de session réseau) pour des transactions sécurisées d'ouverture de session.
- Les classifications des fichiers pour la catégorisation de fichier.
- L'audit, pour une surveillance et une responsabilisation sécurisées.
- RMS pour une protection supplémentaire.

Plusieurs composants et technologies sont mis à jour dans Windows Server 2012 pour prendre en charge le contrôle d'accès dynamique. Les mises à jour les plus importantes sont :

- Le nouveau moteur d'autorisation et d'audit Windows, qui peut traiter des expressions conditionnelles et des stratégies centralisées.
- La prise en charge de l'authentification Kerberos des revendications d'utilisateurs et de périphériques.
- Les améliorations de l'infrastructure de classification des fichiers.
- La prise en charge de l'extensibilité RMS (facultative), afin que les partenaires puissent fournir des solutions pour le chiffrement de format autre que Microsoft Office.

Le contrôle d'accès dynamique comparé à d'autres technologies d'autorisation

Le contrôle d'accès dynamique permet de contrôler l'accès aux ressources basées sur des fichiers. Il étend la fonctionnalité des technologies plus anciennes pour contrôler l'accès aux ressources basées sur des fichiers.



Dans les versions précédentes de Windows Server, le mécanisme de base pour le contrôle d'accès aux fichiers et dossiers était les autorisations NTFS. Les autorisations NTFS et leurs listes de contrôle d'accès permettaient aux administrateurs de contrôler l'accès aux ressources, suivant les identificateurs de sécurité (SID) de nom d'utilisateur ou d'appartenance à un groupe ou le niveau d'accès (par ex. : lecture seule, modification et contrôle total). Cependant, une fois que vous fournissez à quelqu'un l'accès en lecture seule à un document par exemple, vous ne pouvez pas empêcher cette personne de copier le contenu de ce document dans un nouveau document ou de l'imprimer.

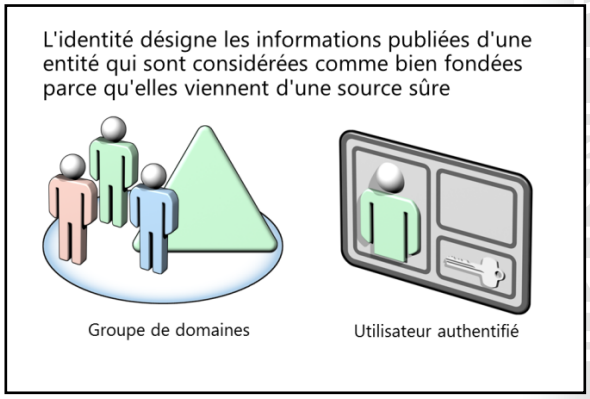
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En implémentant AD RMS, vous pouvez établir un niveau supplémentaire de contrôle de fichier. Ce n'est pas le cas des autorisations NTFS, qui ne prennent pas en charge les applications. En effet, AD RMS définit une stratégie pouvant contrôler l'accès aux documents au sein de l'application que l'utilisateur utilise pour les ouvrir. En implémentant AD RMS, vous permettez aux utilisateurs de protéger des documents dans des applications.

En utilisant des systèmes d'exploitation client Windows antérieures à Windows® 8, vous ne pourrez pas définir l'accès conditionnel aux fichiers à l'aide de NTFS et de AD RMS. Par exemple, vous ne pouvez pas définir des autorisations NTFS de sorte que les utilisateurs puissent accéder à des documents s'ils sont des membres d'un groupe spécifique ou si leurs attributs **EmployeeType** sont définis à **Employé à plein temps**. En outre, vous ne pouvez pas définir des autorisations de sorte que seuls les utilisateurs dont l'attribut de service est rempli avec la même valeur que celui de la ressource puissent accéder au contenu. Cependant, vous pouvez utiliser des expressions conditionnelles pour accomplir ces tâches. Vous pouvez utiliser le contrôle d'accès dynamique pour compter les valeurs d'attribut sur des utilisateurs ou des objets de ressource en fournissant ou en refusant l'accès.

Qu'est-ce que l'identité ?

L'identité est habituellement définie comme un ensemble de données décrivant de manière unique une personne ou une chose (parfois désignée comme *sujet* ou *entité*) et contenant des informations sur les relations du sujet avec d'autres entités. L'identité est généralement vérifiée à l'aide d'une source d'informations sûre.



Par exemple, lorsque vous vous rendez à l'aéroport, vous présentez votre passeport. Votre passeport contient vos nom, adresse, date de naissance et photographie. Chaque élément des données personnelles est une revendication faite à votre sujet, par le pays publiant votre passeport. Votre pays veille à ce que les informations qu'il publie dans un passeport soient exactes concernant le titulaire de passeport. Puisque vous utilisez habituellement le passeport en dehors de votre pays de résidence, les autres pays doivent également pouvoir se fier aux informations de votre passeport. Ils doivent approuver l'organisation qui a publié votre passeport et le considérer comme fiable. C'est ce sentiment de confiance qui permettra aux autres pays de vous accorder l'accès à leurs territoires (pouvant être considérés comme des ressources). Par conséquent, dans cet exemple, pour accéder à des ressources dans d'autres pays, chaque personne doit disposer d'un document (passeport) publié par une source fiable et sûre et contenant les revendications critiques qui décrivent la personne.

Le système d'exploitation Windows Server 2012 utilise un concept semblable concernant l'identité. Un administrateur crée un compte d'utilisateur dans AD DS pour une personne. Le contrôleur de domaine publie les informations du compte utilisateur, telles qu'un identificateur de sécurité et des attributs d'appartenance de groupe. Quand un utilisateur accède à une ressource, Windows Server crée un jeton d'autorisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

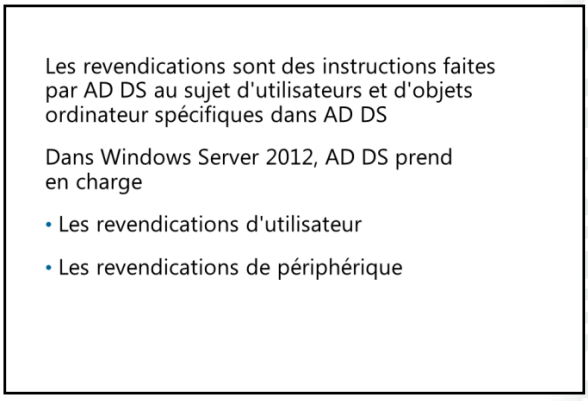
Pour poursuivre l'analogie avec le voyage à l'étranger, vous êtes l'utilisateur et le jeton d'authentification est le passeport. Chaque information unique contenue dans le jeton d'authentification est une revendication faite au sujet de votre compte d'utilisateur. Les contrôleurs de domaine publient et signent ces revendications. Les ordinateurs associés à un domaine et les utilisateurs du domaine font confiance à l'exactitude des informations fournies par les contrôleurs de domaine.

Ainsi, nous pouvons affirmer que l'identité, en ce qui concerne l'authentification et l'autorisation, sont des informations fournies au sujet d'une entité par une source sûre. Par ailleurs, les informations sont considérées comme fiable, puisque la source est approuvée.

Les versions antérieures de Windows Server utilisaient le SID et les groupes de sécurité pour représenter l'identité d'un utilisateur ou d'un ordinateur. Les utilisateurs s'authentifient auprès du domaine avec un nom d'utilisateur et un mot de passe spécifiques. L'unique nom de connexion se traduit par le SID. Le contrôleur de domaine valide le mot de passe et fournit un jeton avec le SID du principal de sécurité, ainsi que les SID de tous les groupes auxquels appartient l'entité. Le contrôleur de domaine revendique que le SID de l'utilisateur est valide et doit servir d'identité à l'utilisateur. Tous les membres du domaine approuvent leur contrôleur de domaine ; ainsi, la réponse est considérée comme fiable.

L'identité ne se limite pas au SID de l'utilisateur. Les applications peuvent utiliser n'importe quelle information concernant l'utilisateur comme une forme d'identité, pourvu que l'application approuve la fiabilité de la source d'informations. Par exemple, de nombreuses applications implémentent le contrôle d'accès basé sur les rôles (RBAC). Le RBAC limite l'accès aux ressources, selon l'appartenance de l'utilisateur à un rôle spécifique. Le serveur Microsoft SharePoint® est un bon exemple de logiciel intégrant la sécurité basée sur les rôles. Windows Server 2012 peut également tirer profit de ces options pour étendre et améliorer a manière dont l'identité est déterminée pour un principal de sécurité.

Qu'est-ce qu'une revendication ?



Windows Server 2008 et Windows Server 2003 utilisent les revendications dans les services ADFS (Active Directory Federation Services ou AD FS). Dans ce contexte, les revendications sont des affirmations concernant l'utilisateur (par ex : nom, identité, touche, groupe, privilège ou fonction) et qui sont comprises par les partenaires dans le cadre d'une fédération AD FS. AD FS fournit également des revendications basées sur AD DS et permet de convertir les données provenant de ces revendications au format SAML (Security Assertions Markup Language). Dans les versions précédentes d'AD FS, les seuls attributs qui pouvaient être récupérés à partir d'AD DS et être incorporés directement à une revendication étaient les informations sur le SID des comptes d'utilisateur et de groupe. Toutes autres informations sur les revendications étaient définies et référencées dans une base de données distincte appelée *magasin d'attributs*. Windows Server 2012 vous permet désormais de lire et d'utiliser n'importe quel attribut directement depuis AD DS. Inutile d'utiliser un magasin d'attributs AD FS distinct pour enregistrer ce type d'informations pour des ordinateurs ou des comptes basés sur Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Par définition, une *revendication* est une affirmation qu'émet AD DS concernant un objet spécifique (généralement un utilisateur ou un ordinateur). Une revendication fournit des informations provenant de la source sûre au sujet d'une entité. Parmi les exemples de revendications figurent le service utilisateur, le niveau de sécurité de l'utilisateur et l'état d'intégrité de l'ordinateur. Toutes ces revendications affirment quelque chose au sujet d'un objet spécifique.

Une entité contient généralement plus d'une revendication. En configurant l'accès aux ressources, il est possible d'utiliser n'importe quelle combinaison de revendications pour autoriser l'accès aux ressources.

Dans Windows Server 2012, le mécanisme d'autorisation est étendu, de manière à prendre en charge des expressions conditionnelles. Vous pouvez désormais utiliser des revendications d'utilisateur et de périphérique pour l'autorisation de fichiers et de dossiers, en plus des autorisations NTFS qui sont basées sur le SID de l'utilisateur ou du groupe. À l'aide des revendications, vous pouvez désormais baser votre décision de contrôle d'accès sur le SID et d'autres valeurs d'attribut. Notez que Windows Server 2012 prend toujours en charge l'appartenance à un groupe pour les décisions d'autorisation.

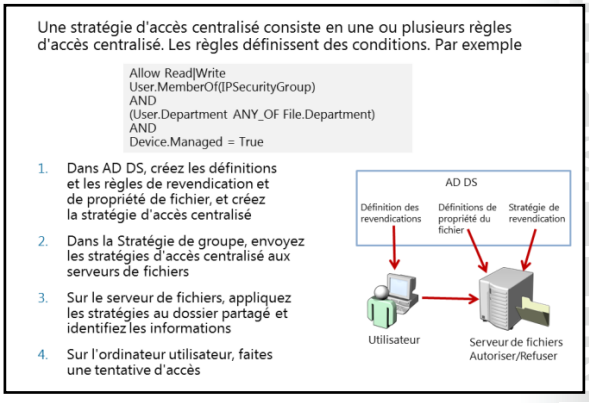
Revendications d'utilisateur

Une *revendication d'utilisateur* est un ensemble d'informations fournies par un contrôleur de domaine Windows Server 2012 au sujet d'un utilisateur. Les contrôleurs de domaine Windows Server 2012 peuvent utiliser la plupart des attributs d'utilisateur AD DS à titre d'informations de revendication. Cela fournit aux administrateurs un large éventail de possibilités pour configurer et utiliser les revendications dans le cadre du contrôle d'accès.

Revendications de périphérique

Une *revendication de périphérique*(souvent appelée *revendication d'ordinateur*)—est un ensemble d'informations fournies par un contrôleur de domaine Windows Server 2012 au sujet d'un périphérique représenté par un compte d'ordinateur dans AD DS. Comme avec des revendications d'utilisateur, les revendications de périphérique peuvent utiliser la plupart des attributs AD DS applicables aux objets ordinateur.

Qu'est-ce qu'une stratégie d'accès centralisé ?



L'une des composantes fondamentales du contrôle d'accès dynamique est la stratégie d'accès centralisée. Cette fonctionnalité de Windows Server 2012 permet aux administrateurs de créer des stratégies pouvant être appliquées à un ou plusieurs serveurs de fichiers. Vous créez des stratégies dans le centre d'administration Active Directory, qui les enregistre alors dans AD DS. Puis, vous les appliquez en utilisant la stratégie de groupe. La stratégie d'accès centralisée contient un ou plusieurs règles de stratégie d'accès centralisée. Chaque règle contient les paramètres qui déterminent l'applicabilité et les autorisations.

Avant de créer une stratégie d'accès centralisée, vous devez créer au moins une règle d'accès centralisée. Les règles d'accès centralisé définissent tous les paramètres et conditions contrôlant l'accès à des ressources spécifiques.

Une règle d'accès centralisée comporte trois parties configurables :

- Nom. Pour chaque règle d'accès centralisée, vous devez configurer un nom descriptif.
- Ressource cible. C'est une condition qui définit les données auxquelles s'applique la stratégie. Vous définissez une condition en spécifiant un attribut et sa valeur. Par exemple, une règle particulière de stratégie centralisée pourrait s'appliquer à n'importe quelles données classées comme sensible.
- Autorisations. C'est une liste d'un ou plusieurs entrées de contrôle d'accès (ACE) visant à définir qui peut accéder aux données. Par exemple, vous pouvez définir l'accès en contrôle total pour un utilisateur dont l'attribut **EmployeeType** est défini sur **ETP** (employé à plein temps). C'est l'élément clé de chaque règle d'accès centralisée. Vous pouvez combiner et regrouper les conditions que vous placez dans la règle d'accès centralisée. Vous pouvez définir les autorisations sur **proposé** (à des fins de transit) ou sur **actuel**.

Vous pouvez penser à la règle d'accès centralisée en vous représentant une exigence d'entreprise décrivant qui peut accéder à un ensemble spécifique d'informations (par ex. informations confidentielles).

Après avoir configuré une ou plusieurs règles d'accès centralisées, ajoutez-les à la stratégie d'accès centralisé, laquelle est ensuite appliquée aux ressources.

La stratégie d'accès centralisée améliore, mais ne remplace pas, les stratégies d'accès locales ou les listes de contrôle d'accès discrétionnaires (DACL) qui sont appliquées aux fichiers et dossiers d'un serveur spécifique. Par exemple, si la liste DACL d'un fichier autorise l'accès à un utilisateur spécifique, mais qu'une stratégie d'accès centralisée appliquée au fichier restreint l'accès à ce même utilisateur, l'utilisateur ne pourra pas obtenir l'accès au fichier. De même, si la stratégie d'accès centralisée autorise l'accès, mais que la liste DACL ne l'autorise pas, alors l'utilisateur ne pourra pas accéder au fichier.

Avant d'implémenter la stratégie d'accès centralisé, procédez aux étapes suivantes :

1. Créez une revendication, puis connectez-la aux utilisateurs ou aux objets ordinateur à l'aide des attributs.
2. Créez les définitions de propriété du fichier.
3. Créez une ou plusieurs règles d'accès centralisé.
4. Créez un objet stratégie d'accès centralisée et définissez ses paramètres.
5. Utilisez la Stratégie de groupe pour déployer la stratégie vers les serveurs de fichiers. Ce faisant, vous mettez au courant des serveurs de fichiers de l'existence d'une stratégie d'accès centralisée dans AD DS.
6. Sur le serveur de fichiers, appliquez cette stratégie à un dossier partagé spécifique.

Vous pouvez également utiliser la boîte à outils de classification de données pour appliquer des stratégies d'accès centralisé automatiquement à travers plusieurs serveurs de fichiers, puis générer un rapport indiquant sur quels partages s'appliquent quelles stratégies.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification du contrôle d'accès dynamique

Le contrôle d'accès dynamique requiert une planification détaillée avant l'implémentation. Vous devez identifier les raisons pour lesquelles votre entreprise souhaite implémenter le contrôle d'accès dynamique et planifier une stratégie d'accès centralisé, des classifications de fichiers, un audit et une assistance en cas d'accès refusé. Dans cette leçon, vous découvrirez comment planifier le contrôle d'accès dynamique.

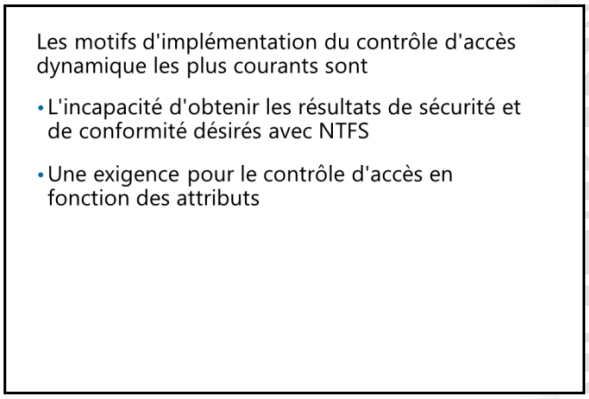
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les motifs d'implémentation du contrôle d'accès dynamique ;
- planifier une stratégie d'accès centralisée ;
- planifier les classifications de fichiers ;
- planifier l'audit d'accès aux fichiers ;
- planifier l'assistance en cas d'accès refusé.

Les motifs d'implémentation du contrôle d'accès dynamique.

Avant d'implémenter le contrôle d'accès dynamique, vous devez identifier clairement les motifs pour lesquels votre entreprise souhaite utiliser cette fonctionnalité. Le contrôle d'accès dynamique doit être bien conçu avant son implémentation. Une implémentation mal organisée peut empêcher certains utilisateurs autorisés d'accéder aux données requises, alors que d'autres utilisateurs non autorisés pourront accéder à des données restreintes.



Les raisons les plus communes justifiant l'implémentation du contrôle d'accès dynamique sont de réduire la complexité des groupes de sécurité, de respecter les règlements de conformité et de protéger les informations confidentielles. En outre, la DAC vous permet d'étendre la fonctionnalité d'un modèle existant de contrôle d'accès. La plupart des entreprises utilisent NTFS et les autorisations de partage pour implémenter le contrôle d'accès pour les ressources de fichiers et de dossiers. Dans la plupart des cas, NFTS est suffisant, mais dans certains cas, cela ne fonctionne pas. Par exemple, vous ne pouvez pas utiliser la liste de contrôle d'accès de NFTS pour protéger une ressource sur un serveur de fichiers. Cela signifie qu'un utilisateur doit être membre des deux groupes à la fois pour accéder à la ressource. Vous devez utiliser le contrôle d'accès dynamique au lieu des méthodes traditionnelles pour l'implémentation du contrôle d'accès, lorsque vous souhaitez utiliser des informations plus spécifiques à des fins d'autorisation. NTFS et les autorisations de partage utilisent uniquement des objets d'utilisateur ou de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planifier une stratégie d'accès centralisé

L'implémentation d'une stratégie d'accès centralisée n'est pas obligatoire pour le contrôle d'accès dynamique. Cependant, pour une configuration cohérente du contrôle d'accès entre tous les serveurs de fichiers, vous devez implémenter au moins une stratégie d'accès centralisée. Ce faisant, vous permettez à tous les serveurs de fichiers dans une portée spécifique d'utiliser une stratégie d'accès centralisée lorsque vous protégez le contenu des dossiers partagés.

Lorsque vous planifiez une stratégie d'accès centralisé, vous devriez

- Identifier les besoins de l'entreprise
- Identifier les ressources à protéger
- Définir les stratégies d'autorisation, telles que définies par vos exigences stratégiques
- Traduire les stratégies d'autorisation en expressions conditionnelles
- Définir les types de revendication, les groupes de sécurité, les propriétés de ressource et les règles

Avant d'implémenter une stratégie d'accès centralisé, créez un plan détaillé comme suit :

1. Identifiez les ressources que vous souhaitez protéger. Si toutes ces ressources sont sur un serveur de fichiers ou dans un seul dossier, l'implémentation d'une stratégie d'accès centralisée n'est peut-être pas nécessaire. Au lieu de cela, vous pouvez configurer l'accès conditionnel sur la liste de contrôle d'accès du dossier. Cependant, si les ressources sont distribuées à travers plusieurs serveurs ou dossiers, vous tirerez avantage à déployer une stratégie d'accès centralisée. Les données pouvant nécessiter une protection supplémentaire peuvent comprendre les données concernant la paie, les données d'antécédents médicaux, les données personnelles des employés et les listes de clients de l'entreprise. Vous pouvez également utiliser le ciblage des règles d'accès centralisées, afin d'identifier les ressources auxquelles vous souhaitez appliquer la stratégie d'accès centralisée.
2. Définissez les stratégies d'autorisation. Ces stratégies sont habituellement définies à partir des besoins de votre entreprise. En voici quelques exemples :
    - Tous les documents dont la confidentialité de propriété est définie sur Haut doivent être disponibles uniquement aux gestionnaires.
    - Les documents de commercialisation de chaque pays doivent être accessibles en écriture uniquement par des employés du service commercial du même pays.
    - Seuls les employés à plein temps doivent pouvoir accéder à la documentation technique des projets précédents.

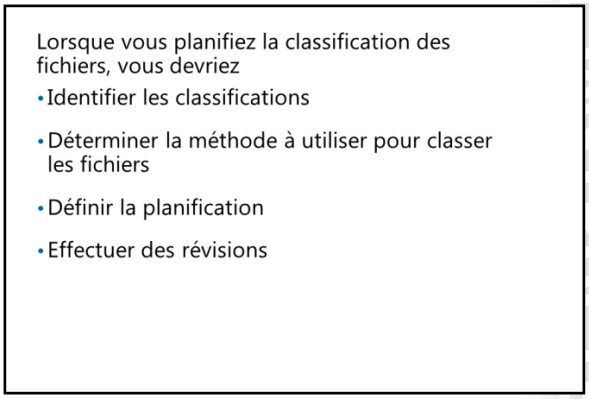
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Traduisez les stratégies d'autorisation dont vous avez besoin par des expressions. Dans le cas du contrôle d'accès dynamique, les expressions sont des attributs associés aux ressources (fichiers et dossiers) et à l'utilisateur ou au périphérique souhaitant accéder aux ressources. Ces expressions énoncent les exigences supplémentaires d'identification qui doivent être respectées pour accéder à des données protégées. Les valeurs associées aux expressions sur la ressource obligent l'utilisateur ou le périphérique à produire la même valeur.
4. Par ailleurs, vous devez décomposer les expressions que vous avez créées et déterminer les types de revendication, groupes de sécurité, propriétés de ressource et revendications de périphérique que vous devez créer pour déployer vos stratégies. En d'autres termes, vous devez identifier les attributs de filtrage d'accès.

Remarque : Vous n'êtes pas censé utiliser les revendications d'utilisateur pour déployer des stratégies d'accès centralisé. Vous pouvez utiliser les groupes de sécurité pour représenter l'identité des utilisateurs. Nous recommandons de commencer par des groupes de sécurité, puisque cela simplifie les conditions initiales de déploiement requises.

Planifier les classifications de fichiers

En organisant votre implémentation du contrôle d'accès dynamique, vous devez inclure les classifications de fichiers. Bien que les classifications de fichiers ne soient pas obligatoires pour le contrôle d'accès dynamique, elles peuvent améliorer l'automatisation de l'ensemble du processus. Par exemple, si vous souhaitez que tous les documents dont la confidentialité est élevée soient accessibles uniquement aux cadres supérieurs, indépendamment du serveur sur lequel les documents existent, vous devez vous demander comment vous identifiez ces documents et comment les classer convenablement.



L'infrastructure de classification des fichiers utilise la classification géolocalisée (puisque la confidentialité de la structure de ce dossier est élevée)— et les règles de classification automatique pour analyser les fichiers automatiquement, puis les classer selon le contenu du fichier. Les propriétés de **Classification** et de **Ressource** sont définies de manière centralisée dans AD DS, de sorte que ces définitions puissent être partagées à travers les serveurs de fichiers de l'entreprise. Vous pouvez créer des règles de classification qui analysent des fichiers à la recherche d'une chaîne standard ou d'une chaîne correspondant à un modèle (expression régulière). Quand un modèle configuré de classification est détecté dans un fichier, ce fichier est classifié comme configuré dans la règle de classification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

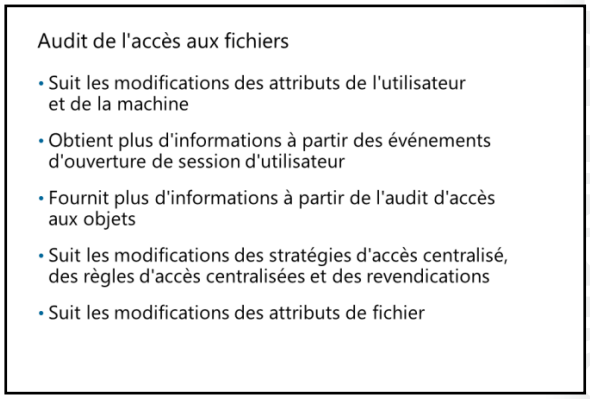
Pour organiser les classifications de fichiers, procédez comme suit :

- Identifiez la ou les classification(s) que vous souhaitez appliquer aux documents.
- Déterminez la méthode que vous utiliserez pour identifier des documents pour la classification.
- Définissez la planification des classifications automatiques.
- Établissez des examens périodiques pour déterminer le succès des classifications.

Vous configurez les classifications de fichiers dans la console du Gestionnaire de ressources du serveur de fichiers.

Une fois que vous avez défini les classifications, vous pouvez organiser l'implémentation du contrôle d'accès dynamique en définissant les expressions conditionnelles qui vous permettront de contrôler l'accès aux documents hautement confidentiels, suivant des attributs d'utilisateur particuliers.

Planifier l'audit de l'accès aux fichiers



Dans Windows Server 2008 R2 et Windows Server 2012, vous pouvez utiliser des stratégies d'audit avancées pour implémenter un audit détaillé et plus précis du système de fichiers. Dans Windows Server 2012, vous pouvez également implémenter l'audit avec le contrôle d'accès dynamique pour utiliser les nouvelles fonctions d'audit de sécurité Windows. À l'aide des expressions conditionnelles, vous pouvez configurer l'audit de sorte qu'il se produise seulement dans des cas spécifiques. Par exemple, il se peut que vous souhaitiez auditer des tentatives d'ouvrir des dossiers partagés par des utilisateurs se trouvant dans des pays autres que le celui où le dossier partagé est localisé. Pour ce faire, implémentez les autorisations proposées dans les règles d'accès centralisées.

L'audit global d'accès aux objets permet aux administrateurs de définir des listes de contrôle d'accès (SACL) au système informatique suivant le type d'objet pour le système de fichiers ou le Registre. La SACL spécifiée est alors appliquée automatiquement à chaque objet de ce type. Vous pouvez utiliser une stratégie d'audit globale d'accès aux objets pour appliquer la stratégie d'audit d'accès aux objets d'un ordinateur, un partage de fichiers ou un Registre, sans configurer ni propager des SACL conventionnelles. La configuration et la propagation d'une SACL est une tâche d'administration complexe difficile à vérifier, en particulier si vous devez faire appel à un auditeur pour vérifier qu'une stratégie de sécurité est appliquée.

Remarque : Les auditeurs peuvent vérifier que chaque ressource du système est protégée par une stratégie d'audit en affichant le contenu du paramètre global de stratégie d'audit d'accès aux objets.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

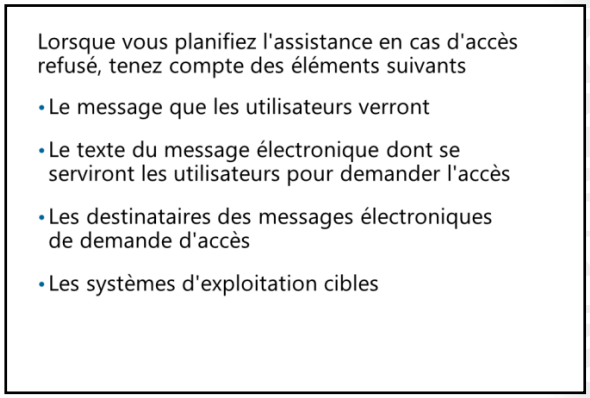
La ressource SACL est également utile pour les scénarios de diagnostic. Par exemple, définir une stratégie d'audit globale d'accès aux objets pour enregistrer toutes les activités d'un utilisateur spécifique ; et activer des stratégies d'audit de défaillances d'accès dans une ressource (telle qu'un système de fichiers ou un Registre) permet d'aider les administrateurs à identifier rapidement l'objet qui dans un système, refuse l'un accès à un utilisateur.

Avant d'implémenter l'audit, vous devez préparer un plan d'audit. Dans le plan d'audit, vous devez identifier les ressources, les utilisateurs et les activités que vous souhaitez suivre. Vous pouvez implémenter l'audit pour plusieurs scénarios, tels que :

- Suivre les modifications des attributs de l'utilisateur et de la machine. Tout comme les fichiers, les utilisateurs et les objets de machine peuvent avoir des attributs et les modifications apportées à ces derniers peuvent affecter l'accès des utilisateurs à ces fichiers. Ainsi, le suivi des modifications apportées aux attributs de l'utilisateur et des machines peut s'avérer intéressant. Les utilisateurs et les objets de machine sont enregistrés dans AD DS, ce qui signifie que vous pouvez suivre leurs attributs en auditant l'accès au service d'annuaire.
- Obtenir plus d'informations à partir des événements d'ouverture de session d'utilisateur. Dans Windows Server 2012, un événement d'ouverture de session d'utilisateur (événement 4624) contient des informations sur l'utilisateur qui a était connecté à l'ordinateur. Vous pouvez afficher ces informations supplémentaires à l'aide des outils de gestion de journal d'audit, afin de relier des événements d'ouverture de session d'utilisateur à des événements d'accès aux objets ; ou en activant le filtrage des événements selon les attributs du fichier et de l'utilisateur.
- Fournir plus d'informations à partir de l'audit d'accès aux objets. Dans Windows Server 2012, les événements 4656 et 4663 d'accès au fichier contiennent maintenant des informations sur les attributs du fichier qui a été consulté. Les outils de filtrage du journal des événements peuvent utiliser ces informations supplémentaires pour vous aider à identifier les événements d'audit les plus appropriés.
- Suivre les modifications des stratégies d'accès centralisé, des règles d'accès centralisées et des revendications. Puisque ces objets sont enregistrés dans AD DS, vous pouvez les auditer exactement comme pour n'importe quel autre objet sécurisable dans AD DS, en auditant l'accès au service d'annuaire.
- Suivre les modifications des attributs de fichier. Les attributs de fichier déterminent que la stratégie d'accès centralisé applique au fichier. Une modification des attributs de fichier peut potentiellement affecter les restrictions d'accès au fichier. Vous pouvez suivre les modifications des attributs de fichier sur n'importe quelle machine en configurant l'audit de changement de politique d'autorisation et l'audit d'accès aux objets pour les systèmes de fichiers. L'événement 4911 est intégré dans Windows Server 2012 pour différencier cet événement des autres événements de changement de politique d'autorisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planifier l'assistance en cas d'accès refusé



L'assistance en cas d'accès refusé, une fonctionnalité du système d'exploitation Windows 8, aide les utilisateurs finaux à déterminer pourquoi ils ne peuvent pas accéder à une ressource. Elle permet également au personnel informatique de diagnostiquer correctement un problème, puis d'orienter sa résolution. Windows Server 2012 vous permet de personnaliser des messages concernant l'accès refusé. Il permet également aux utilisateurs de demander un accès sans contacter l'assistance technique ou l'équipe informatique. En combinaison avec le contrôle d'accès dynamique, l'assistance en cas d'accès refusé peut informer l'administrateur des revendications d'utilisateur et de ressource, permettant à l'administrateur de prendre des décisions informées sur la façon de régler les stratégies et de déterminer les attributs d'utilisateur, par exemple si le service est désigné comme « RH » au lieu de « Ressources Humaines. »

Remarque : Seuls les périphériques Windows 8 prennent en charge l'assistance en cas d'accès refusé.

Pour organiser l'assistance en cas d'accès refusé, vous devez procéder aux étapes suivantes :

- Définissez les messages que les utilisateurs recevront lorsqu'ils tentent d'accéder à des ressources pour lesquelles ils ne possèdent pas les droits d'accès. Le message devrait être informel et facile à comprendre.
- Déterminez si des utilisateurs devrait pouvoir envoyer une demande de l'accès par l'intermédiaire de l'email et si oui, configurez éventuellement le texte qui sera ajouté à leurs messages électroniques.
- Déterminez les destinataires des messages électroniques de demande d'accès. Vous pouvez choisir d'envoyer le courrier électronique aux propriétaires de dossier, aux administrateurs de serveur de fichiers ou à n'importe quel autre destinataire spécifié. Les messages doivent toujours être transmis à la personne appropriée. Si vous disposez d'un outil du support technique ou d'une solution de surveillance prenant en charge les messages électroniques, vous pouvez également diriger ces messages pour générer automatiquement des demandes d'utilisateur dans votre solution d'assistance technique.
- Sélectionnez le système d'exploitation cible. L'assistance en cas d'accès refusé fonctionne uniquement avec Windows 8 ou Windows Server 2012.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Déploiement du contrôle d'accès dynamique

Pour déployer le contrôle d'accès dynamique, vous devez effectuer plusieurs étapes et configurer plusieurs objets. Dans cette leçon, vous découvrirez comment implémenter et configurer le contrôle d'accès dynamique.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les conditions requises pour l'implémentation du contrôle d'accès dynamique ;
- activer l'assistance technique dans AD DS pour le contrôle d'accès dynamique ;
- implémenter des revendications et des objets de propriété de ressource ;
- implémenter les règles d'accès centralisées et les stratégies ;
- implémenter l'audit d'accès aux fichiers ;
- implémenter l'assistance en cas d'accès refusé ;
- implémenter les classifications de fichiers ;
- implémenter les modifications de stratégie d'accès centralisée.

Les prérequis de l'implémentation du contrôle d'accès dynamique

Avant d'implémenter le contrôle d'accès dynamique, vous devez vérifier que vos serveurs respectent certains prérequis. Les autorisations basées sur les revendications requièrent l'infrastructure suivante :

Le contrôle d'accès dynamique est une fonctionnalité spécifique à Windows Server 2012

Pour déployer le contrôle d'accès dynamique, vous devez avoir les technologies suivantes

- Un contrôleur de domaine Windows Server 2012
- Un serveur de fichiers Windows Server 2012
- Un bureau Windows 8 (pour les revendications de périphérique)

- Windows Server 2012, avec la fonction Gestionnaire de ressources du serveur de fichiers (FSRM) activée. Cela doit être installé sur le serveur de fichiers qui hébergera les ressources que le contrôle d'accès dynamique protégera. Le serveur de fichiers qui hébergera le partage doit être un serveur de fichiers Windows Server 2012, de sorte qu'il puisse lire des revendications et des données d'autorisation de périphérique provenant d'un ticket Kerberos v5, traduire les SID et les revendications du ticket en jeton d'authentification, puis comparer les données d'autorisation du jeton avec les expressions conditionnelles du descripteur de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Une mise à jour de schéma ou au moins un contrôleur de domaine Windows Server 2012 pour enregistrer les définitions centrales des propriétés de ressource et des stratégies. Les revendications d'utilisateur ne sont pas requises pour les groupes de sécurité. Si vous utilisez des revendications d'utilisateur, alors au moins un contrôleur de domaine Windows Server 2012 du domaine de l'utilisateur doit être accessible par le serveur de fichiers, afin que le serveur de fichiers puisse récupérer des revendications au nom de l'utilisateur. Si vous utilisez des revendications de périphérique, tous les contrôleurs de domaine du domaine d'utilisateur et de périphérique doivent utiliser le système d'exploitation Windows 8.

 **Remarque :** Seuls les périphériques Windows 8 utilisent les revendications de périphérique.

Le nouveau mécanisme d'autorisation et d'audit requiert des extensions vers AD DS. Ces extensions génèrent le dictionnaire de revendications Windows, emplacement dans lequel les systèmes d'exploitation Windows stockent les revendications pour une forêt Active Directory. L'autorisation des revendications se fonde également sur le centre de distribution de clés (KDC) de Kerberos. Le KDC de Windows Server 2012 contient les améliorations Kerberos requises pour transporter des revendications dans un ticket Kerberos, ainsi qu'une identité composée. Le KDC de Windows Server 2012 comprend également une amélioration pour prendre en charge le blindage Kerberos. Le blindage Kerberos est une implémentation du tunneling sécurisé d'authentification flexible qui fournit un canal protégé entre le client de Kerberos et le KDC.

Les prérequis d'utilisation des revendications sont les suivants :

- Si vous utilisez des revendications à travers une approbation de forêt, vous devez avoir des contrôleurs de domaine Windows Server 2012 dans chaque domaine.
- Si vous utilisez des revendications de périphérique, vous devez avoir un client Windows 8. Les systèmes d'exploitation Windows antérieurs ne prennent pas en charge les revendications de périphérique.

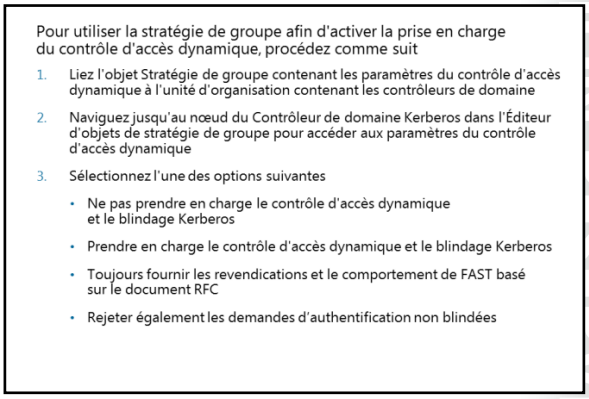
Bien qu'un contrôleur de domaine Windows Server 2012 soit requis en utilisant des revendications d'utilisateur, il n'y a aucune configuration requise pour avoir un domaine et un niveau fonctionnel de forêt pour Windows Server 2012, à moins que vous souhaitiez utiliser les revendications à travers une approbation de forêt. Ceci signifie que vous pouvez également avoir des contrôleurs de domaine sur Windows Server 2008 et Windows Server 2008 R2 avec le niveau fonctionnel de forêt situé sur Windows Server 2008.

 **Remarque :** L'implémentation du contrôle d'accès dynamique dans un environnement avec plusieurs forêts requiert des spécifications d'installation supplémentaires.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Activer l'assistance technique dans AD DS pour le contrôle d'accès dynamique

Une fois les spécifications logicielles remplies pour activer la prise en charge du contrôle d'accès dynamique, vous devez activer la prise en charge des revendications du KDC de Windows Server 2012. La prise en charge Kerberos pour le contrôle d'accès dynamique fournit un mécanisme afin d'inclure la revendication d'utilisateur et les informations d'autorisation d'un périphérique dans un jeton d'authentification Windows. Les contrôles d'accès exécutés sur les ressources (telles que des fichiers ou dossiers) utilisent ces informations d'autorisation pour vérifier l'identité.



Vous devez d'abord utiliser la stratégie de groupe pour activer le contrôle d'accès dynamique dans AD DS. Puisque ce paramètre est spécifique aux contrôleurs de domaine, vous pouvez créer un nouvel objet de stratégie de groupe (GPO) puis lier le paramètre à l'unité d'organisation (OU) des contrôleurs de domaine ou modifier le GPO des contrôleurs de domaine par défaut qui sont déjà liés à cette unité d'organisation.

N'importe quelle méthode vous choisissez, vous devriez ouvrir **Éditeur d'objet de stratégie de groupe**, développez **Configuration ordinateur**, développez **Stratégies**, développez **Modèles d'administration**, développez **Système**, puis développez **Contrôleur de domaine Kerberos**. Dans ce nœud, ouvrez un paramètre appelé **Prendre en charge le contrôle d'accès dynamique et le blindage Kerberos**.

Pour configurer le contrôle d'accès dynamique et le paramètre de stratégie de blindage Kerberos, choisissez une des quatre options listées ci-dessous :

- Ne pas prendre en charge le contrôle d'accès dynamique et le blindage Kerberos
- Prendre en charge le contrôle d'accès dynamique et le blindage Kerberos
- Toujours fournir les revendications et le comportement de FAST basé sur le document RFC
- Rejeter également les demandes d'authentification non blindées

La prise en charge des revendications et du blindage Kerberos est désactivée par défaut, ce qui est équivalent à ne pas configurer le paramètre de stratégie ou à le configurer sur Ne pas prendre en charge le contrôle d'accès dynamique et le blindage Kerberos.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le paramètre Prendre en charge le contrôle d'accès dynamique et la stratégie de blindage Kerberos permet de configurer le contrôle d'accès dynamique et le blindage Kerberos dans un environnement en mode Mixte(lorsqu'il y a un mélange de contrôleurs de domaine Windows Server 2012 et de contrôleurs de domaine exécutant des versions antérieures de Windows Server). Pour activer les revendications de périphérique, vous devez également autoriser les revendications des clients Windows 8.

Utilisez les paramètres de stratégie restants si tous les contrôleurs de domaine sont des contrôleurs de domaine Windows Server 2012 et que le niveau fonctionnel du domaine est configuré à Windows Server 2012. Le paramètre de stratégie Toujours fournir les revendications et le comportement RAPIDE de RFC et le paramètre de stratégie Échouer également les demandes d'authentification non blindées permettent d'activer le contrôle d'accès dynamique et le blindage Kerberos pour le domaine. Cependant, le dernier paramètre de stratégie exige que tous les services d'authentification et les communications de service d'accord de tickets (TGS, Ticket-Granting Service) Kerberos utilisent le blindage Kerberos. Les contrôleurs de domaine Windows Server 2012 lisent cette configuration tandis que d'autres contrôleurs de domaine ignorent ce paramètre.

Implémenter des revendications et des objets de propriété de ressource

Après avoir activé la prise en charge du contrôle d'accès dynamique dans AD DS, vous devez ensuite créer et configurer des revendications et des objets de propriété de ressource.

Les expressions conditionnelles peuvent inclure à la fois des revendications et des objets de propriété de ressource

Revendications	• Créées pour les utilisateurs et les ordinateurs • Ont des attributs comme source • Créées en utilisant le centre d'administration Active Directory ou Windows PowerShell
Objets de propriété de ressource	• Créés pour les ressources • Ont des propriétés comme source • Créés en utilisant le centre d'administration Active Directory ou Windows PowerShell

Créer et configurer des types de revendication

Pour créer et configurer des revendications, vous utilisez principalement le centre d'administration Active Directory. Vous utilisez le centre d'administration Active Directory pour créer des revendications basées sur des attributs, qui sont le type de revendication le plus commun. Cependant, vous pouvez également utiliser le module Active Directory pour Windows PowerShell® pour créer des revendications basées sur des certificats. Toutes les revendications sont enregistrées dans la partition de configuration dans AD DS. Puisque c'est une partition à l'échelle de la forêt, tous les domaines de la forêt partagent le dictionnaire de revendications ; et les contrôleurs de domaine affichent les informations de revendication lors de l'authentification de l'utilisateur et de l'ordinateur.

Pour créer des revendications basées sur des attributs dans le centre d'administration Active Directory, naviguez vers le nœud du contrôle d'accès dynamique, puis ouvrez le conteneur des Types de revendication. Par défaut, aucun type de revendication n'est défini ici. Dans le volet Actions, vous pouvez cliquer sur **Créer un type de revendication** pour afficher la liste d'attributs. Ces attributs servent de source aux valeurs de revendications. Quand vous créez une revendication, vous associez la revendication avec l'attribut spécifique. La valeur de cet attribut est renseignée comme valeur de revendication. Par conséquent, il est crucial que les informations contenues dans les attributs d'Active Directory servant de source aux types de revendication soient exactes ou restent vierge, car elles seront utilisées pour le contrôle d'accès de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Quand vous sélectionnez l'attribut que vous souhaitez utiliser pour créer une revendication, vous devez également fournir un nom pour la revendication. Le nom suggéré pour la revendication est toujours identique au nom de l'attribut sélectionné. Cependant, vous pouvez également fournir un autre nom ou un nom plus explicite pour la revendication. Éventuellement, vous pouvez fournir des valeurs suggérées pour une revendication. Ce n'est pas obligatoire, mais c'est recommandé, parce que cela peut réduire la possibilité d'erreurs.

Vous pouvez également spécifier un ID de revendication. Cette valeur est générée automatiquement, mais il se peut que vous souhaitiez spécifier l'ID de revendication si vous définissez la même revendication pour plusieurs forêts et que vous souhaitez que l'ID soit identique.

 **Remarque :** Les types de revendication proviennent des attributs d'AD DS. Pour cette raison, vous devez configurer les attributs de votre ordinateur et de vos comptes d'utilisateurs dans AD DS avec les informations appropriées pour l'utilisateur ou l'ordinateur respectif. Les contrôleurs de domaine Windows Server 2012 n'émettent pas une revendication pour un type de revendication basé sur des attributs lorsque l'attribut de l'entité de sécurité de l'authentification est vide. Suivant la configuration des attributs de l'objet de propriété de la ressource du fichier de données, une valeur Null dans une revendication peut avoir comme conséquence de refuser l'accès des données protégées du contrôle d'accès dynamique à un utilisateur.

Créer et configurer des propriétés de ressource

Bien que les propriétés de ressource soient au noyau du contrôle d'accès dynamique, vous devriez les implémenter après avoir défini l'utilisateur et les revendications de périphérique. Souvenez-vous que si une revendication ne correspond à pas la valeur de propriété spécifiée de la ressource, il se peut que l'accès aux données soit interdit. Par conséquent, renverser l'ordre d'implémentation risquerait malencontreusement de bloquer l'accès aux données aux utilisateurs qui devraient pouvoir y accéder.

Quand vous utilisez des revendications ou des groupes de sécurité pour contrôler l'accès aux fichiers et aux dossiers, vous devez également fournir les informations supplémentaires pour ces ressources. Vous faites ceci en configurant les objets de propriété de ressource. Vous gérez des propriétés de ressource dans le conteneur de propriétés de ressource, qui est situé dans le nœud dynamique de contrôle d'accès au centre d'administration Active Directory. Vous pouvez créer vos propres propriétés de ressource ou utiliser une propriété préconfigurée, telle que **Projet**, **Service** et **Utilisation de dossier**. Tous les objets de propriété de ressource prédéfinis sont désactivés par défaut. Si vous souhaitez utiliser l'un d'entre eux, vous devez d'abord les activer. Si vous souhaitez créer votre propre objet de propriété de ressource, vous pouvez indiquer le type de propriété et les valeurs autorisées ou suggérées.

Quand vous créez des objets de propriété de ressource, vous pouvez sélectionner des propriétés à inclure dans les fichiers et dossiers. Pendant l'évaluation et l'audit du fichier, le système d'exploitation Windows utilise les valeurs de ces propriétés, ainsi que les valeurs provenant des revendications de l'utilisateur et du périphérique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Après avoir configuré les revendications de l'utilisateur et du périphérique, ainsi que les propriétés de ressource, vous devez ensuite protéger les fichiers et dossiers à l'aide des expressions conditionnelles qui évaluent les revendications de l'utilisateur et du périphérique par rapport à des valeurs constantes ou des valeurs contenues dans les propriétés de ressource. Pour ce faire, procédez par l'une des trois manières suivantes :

- Si vous souhaitez inclure uniquement des dossiers spécifiques, vous pouvez utiliser l'éditeur avancé de paramètres de sécurité pour créer des expressions conditionnelles directement dans le descripteur de sécurité.
- Pour inclure plusieurs (ou tous les) serveurs de fichiers, vous pouvez créer des règles de stratégie d'accès centralisé, puis lier ces règles aux objets de la stratégie centralisée. Vous pouvez alors utiliser la stratégie de groupe pour déployer les objets de stratégie centralisée vers les serveurs de fichiers, puis configurer le partage de manière à utiliser l'objet de stratégie centralisée. Cependant, utiliser des stratégies d'accès centralisé est la méthode la plus efficace pour sécuriser des fichiers et des dossiers. Ce point est expliqué plus en détail dans la prochaine rubrique.
- Vous pouvez utiliser des classifications de fichiers pour inclure certains fichiers avec un ensemble de propriétés plus commun à travers plusieurs dossiers ou fichiers.

Vous pouvez utiliser des revendications et des objets de propriété de ressource ensemble dans des expressions conditionnelles. Windows Server 2012 et Windows 8 prennent en charge une ou plusieurs expressions conditionnelles dans une entrée d'autorisation. Les expressions conditionnelles ajoutent simplement une autre couche applicable à l'entrée d'autorisation. Les résultats de toutes les évaluations d'expressions conditionnelles doivent afficher **Vrai** pour que Windows accorde l'entrée d'autorisation pour l'autorisation. Par exemple, supposez que vous définissez une revendication nommée Service, pour un utilisateur (avec un attribut de source « service ») et que vous définissez un objet de propriété de ressource nommé Serv. Vous pouvez désormais définir une expression conditionnelle indiquant que l'utilisateur peut accéder à un dossier (avec les objets de propriété de ressource appliqués) seulement si la valeur de l'attribut Service de l'utilisateur est égale à la valeur de la propriété Serv. du dossier. Notez que si l'objet de propriété de ressource Serv. n'a pas été appliqué au(x) fichier(s) en question ou Serv. est une valeur Null, alors l'utilisateur sera autorisé à accéder aux données.

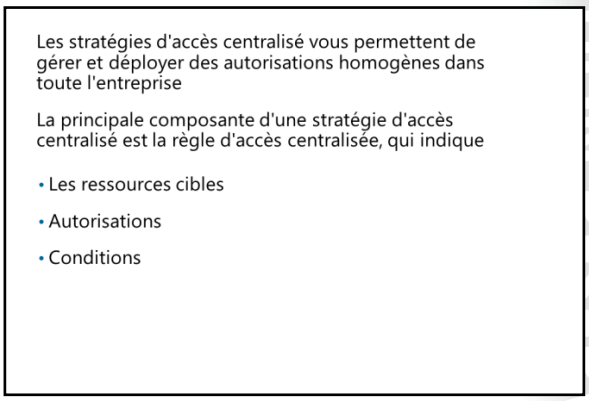
 **Remarque :** L'accès n'est pas contrôlé par la revendication, mais par l'objet de propriété de ressource. La revendication doit fournir la valeur correcte correspondant aux configurations requises définies par l'objet de propriété de ressource. Si l'objet de propriété de ressource n'implique aucun attribut particulier, les attributs supplémentaires de revendication associés à l'utilisateur ou ai périphérique sont ignorés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémenter des règles et des stratégies d'accès centralisées

Les stratégies d'accès centralisé vous permettent de gérer et de déployer une autorisation cohérente dans toute l'entreprise à l'aide des règles d'accès centralisées et des objets de stratégie d'accès centralisée.



Les stratégies d'accès centralisé agissent comme des réseaux de sécurité qu'une entreprise applique à travers ses serveurs. Vous utilisez la stratégie de groupe pour déployer une stratégie d'accès centralisée et vous appliquez manuellement les stratégies à tous les serveurs de fichiers Windows Server 2012 qui utiliseront le contrôle d'accès dynamique. Une stratégie d'accès centralisée vous permet de déployer une configuration cohérente à travers plusieurs serveurs de fichiers. En outre, vous pouvez utiliser la boîte à outils de classification de données pour appliquer une stratégie d'accès centralisé partagée à travers plusieurs serveurs de fichiers indiquant les stratégies d'accès centralisées appliquées aux partages.

La composante principale d'une stratégie d'accès centralisée est la règle d'accès centralisée. Les objets d'une stratégie d'accès centralisée représentent une collection de règles d'accès centralisées. Avant de créer une stratégie d'accès centralisé, vous devrez créer une règle d'accès centralisée, parce que les stratégies sont composées des règles.

Une règle d'accès centralisée contient plusieurs critères que le système d'exploitation Windows utilise lorsqu'il évalue l'accès. Par exemple, une règle d'accès centralisée peut utiliser des expressions conditionnelles pour cibler des fichiers et des dossiers spécifiques. Chaque règle d'accès centralisée a une condition qui détermine les informations ciblées par la règle et les listes d'entrée d'autorisation à utiliser pour gérer les entrées d'autorisation actuelles ou proposées. Vous pouvez également renvoyer la liste d'entrée d'autorisation actuelle de la règle à sa dernière liste connue d'entrées d'autorisation. Chaque règle d'accès centralisée peut appartenir à un ou plusieurs objets de stratégie d'accès centralisée.

Configuration des règles d'accès centralisé

En général, vous créez et configurez les règles d'accès centralisés dans le centre d'administration Active Directory. Cependant, vous pouvez également utiliser Windows PowerShell pour effectuer la même tâche.

Pour créer une nouvelle règle d'accès centralisé, procédez comme suit :

1. Fournissez un nom et une description pour la règle. Vous devez également choisir de protéger la règle contre la suppression accidentelle.
2. Configurez les ressources cibles. Dans le centre d'administration Active Directory, utilisez la section Ressources cibles pour créer une étendue pour la règle d'accès. Vous créez l'étendue à l'aide des propriétés de ressource d'une ou plusieurs expressions conditionnelles. Vous souhaitez créer une condition cible selon l'exigence d'entreprise qui pilote cette règle. Par exemple, Resource.Compliancy=HIPAA. Pour simplifier le processus, vous pouvez conserver la valeur par défaut (Toutes les ressources) et appliquer un filtrage de ressource le cas échéant. Vous pouvez joindre les expressions conditionnelles à l'aide des opérateurs logiques, tels que **ET** et **OU**. En outre, vous pouvez regrouper des expressions conditionnelles pour combiner les résultats de deux expressions conditionnelles jointes ou davantage. La section Ressources cibles affiche l'expression conditionnelle actuellement configurée, utilisée pour contrôler l'applicabilité de la règle.

3. Configurez les autorisations avec l'une des options suivantes :

   - **Utiliser les autorisations suivantes en tant qu'autorisations proposées**. Sélectionnez cette option pour ajouter les entrées d'autorisation de la liste d'autorisations à la liste d'entrées d'autorisation proposées pour la règle d'accès centralisée récemment créée. Vous pouvez combiner la liste d'autorisations proposée avec l'audit du système de fichiers pour modeler l'accès effectif des utilisateurs à la ressource, sans avoir à modifier les entrées d'autorisation de la liste d'autorisations actuelle. Les autorisations proposées génèrent un événement d'audit spécial dans le journal des événements, décrivant l'accès effectif proposé pour les utilisateurs.

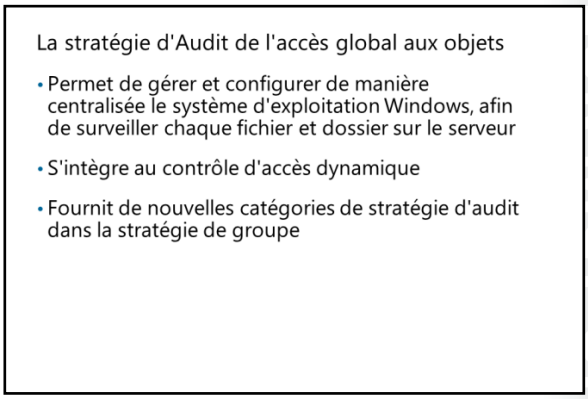
 **Remarque :** Les autorisations proposées ne s'appliquent pas aux ressources ; elles existent uniquement pour la simulation.

   - **Utiliser les autorisations suivantes en tant qu'autorisations actuelles**. Sélectionnez cette option pour ajouter les entrées d'autorisation de la liste d'autorisations à la liste d'entrées d'autorisation actuelle pour la règle d'accès centralisée récemment créée. La liste d'autorisations actuelle représente les autorisations supplémentaires que le système d'exploitation Windows considère lorsque vous déployez la règle d'accès centralisée vers un serveur de fichiers. Les règles d'accès centralisées ne remplacent pas la sécurité existante. En prenant des décisions d'autorisation, Windows évalue les entrées d'autorisation de la liste d'autorisations actuelle de la règle d'accès centralisée, NTFS et les listes d'autorisations de partage.

Une fois que vous êtes satisfait de vos autorisations proposées, vous pouvez les convertir en des autorisations actuelles. Autrement, vous pouvez utiliser des autorisations actuelles dans un environnement de test et l'accès effectif comme spécifié dans l'onglet **Sécurité avancée** pour modeler la manière dont la stratégie s'applique à différents utilisateurs.

Implémenter l'audit d'accès aux fichiers

La fonctionnalité d'audit global d'accès aux objets de Windows 8 et Windows Server 2012 vous permet de configurer l'audit d'accès aux objets de chaque fichier et dossier du système de fichiers d'un ordinateur. Vous utilisez cette fonctionnalité pour gérer et configurer de manière centralisée les systèmes d'exploitation Windows, afin de surveiller chaque fichier et dossier de l'ordinateur. Pour activer l'audit d'accès aux objets dans les versions précédentes de Windows Server, vous devez configurer cette option dans les stratégies d'audit de base (dans les GPO) et activer l'audit d'un principal de sécurité spécifique du SACL de l'objet. Parfois, cette approche ne permet pas de rapprocher facilement les stratégies (par ex. : « Enregistrer toutes les activités d'écriture administrative sur les serveurs contenant des données financières ») parce que vous pouvez activer l'enregistrement d'audit d'accès aux objets au niveau de l'objet, mais pas au niveau du serveur. La nouvelle catégorie d'audit dans Windows Server 2008 R2 et Windows Server 2012 permet aux administrateurs de gérer l'audit d'accès aux objets en utilisant une portée beaucoup plus large.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le contrôle d'accès dynamique vous permet de créer des stratégies d'audit ciblées en utilisant les propriétés de ressource et les expressions, selon les revendications d'utilisateur et d'ordinateur. Par exemple, vous pouvez créer une stratégie d'audit pour suivre toutes les opérations de **Lecture** et d'**Écriture** sur les fichiers hautement confidentiels, par des employés dont l'attribut **Niveau d'autorisation élevé** ne contient pas la valeur appropriée. Vous pouvez écrire des stratégies d'audit basées sur des expressions directement sur un fichier ou dossier ;ou de manière centralisée via la stratégie de groupe, en utilisant l'audit global d'accès aux objets. Avec cette approche, vous n'empêchez pas l'accès non autorisé ; au lieu de cela, vous enregistrez les tentatives d'accès au contenu par des personnes non autorisées.

Vous configurez l'audit global d'accès aux objets quand vous activez l'audit d'accès aux objets et l'audit global d'accès aux objets. L'activation de cette fonctionnalité active l'audit de l'ordinateur qui applique le paramètre de stratégie. Cependant, la seule activation de l'audit ne génère pas toujours des événements d'audit. La ressource—dans ce cas, des fichiers et dossiers—doit contenir des entrées d'audit dans sa liste de contrôle d'accès.

Vous devez configurer l'audit global d'accès aux objets de votre entreprise à l'aide de la stratégie de sécurité d'un objet de stratégie de groupe basé sur un domaine. Les deux paramètres de stratégie de sécurité requis pour activer l'audit global d'accès aux objets sont situés dans les emplacements suivants :

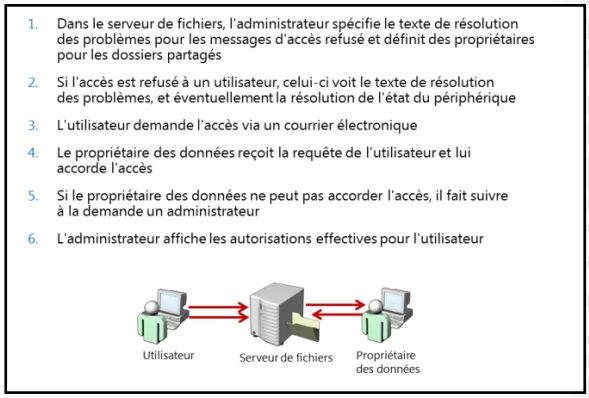
- Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies d'audit avancées\Stratégies d'audit\Accès aux objets\Auditer le système de fichiers.
- Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies d'audit avancées\Stratégie d'audit\Audit global d'accès aux objets\Système de fichiers

L'audit global d'accès aux objets comprend une sous-catégorie pour le système de fichiers et le Registre. Tous les événements d'audit d'accès au fichier comprennent également les valeurs de propriété de ressource dans les événements d'audit, de sorte que vous puissiez utiliser ces valeurs pour la création de rapport avancée tel que « qui a consulté toutes les données de finances. » Pour ce faire, utilisez des outils tels que Microsoft System Center pour rassembler tous les événements dans une base de données SQL centrale et générer des rapports selon ces événements.

 **Remarque :** Si une liste SACL de fichiers ou de dossiers ainsi qu'une stratégie d'audit globale d'accès aux objets (ou une liste SACL de paramètres du Registre unique et une stratégie d'audit globale d'accès aux objets) sont configurés sur un ordinateur, la liste SACL effective est dérivée en combinant la liste SACL de fichiers ou de dossiers et la stratégie d'audit globale d'accès aux objets. Cela signifie qu'un événement d'audit est généré si une activité correspond à la liste SACL de fichiers ou de dossiers ou à la stratégie d'audit globale d'accès aux objets. Si plusieurs stratégies d'audit globales sont configurées pour le même serveur, les stratégies d'audit sont combinées à une stratégie d'audit globale pour ce serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémenter l'assistance en cas d'accès refusé



L'erreur d'accès refusé est l'une des plus communes que les utilisateurs reçoivent lorsqu'ils essayent d'accéder à un fichier ou dossier sur un serveur de fichiers distant. En général, cette erreur se produit quand un utilisateur essaye d'accéder à une ressource sans avoir les autorisations appropriées pour le faire ; ou à cause d'une mauvaise configuration des autorisations ou des listes de contrôle d'accès aux ressources. La mauvaise implémentation du contrôle d'accès dynamique peut créer des complications supplémentaires. Par exemple, les utilisateurs disposant des autorisations requises se verront refuser l'accès, si un attribut particulier de leur compte est mal épelé.

Quand les utilisateurs reçoivent cette erreur, ils essayent en général de contacter l'administrateur pour obtenir l'accès. Cependant, les administrateurs n'approuvent généralement pas l'accès aux ressources, alors ils redirigent les utilisateurs à quelqu'un d'autre pour approbation.

Dans Windows Server 2012, il y a une nouvelle fonctionnalité pour aider les utilisateurs et les administrateurs dans de telles situations. Cette fonctionnalité est appelée assistance en cas d'accès refusé. L'assistance en cas d'accès refusé aide les utilisateurs à répondre aux problèmes d'accès refusé, sans impliquer le personnel informatique. Pour ce faire, elle fournit des informations au sujet du problème et dirige les utilisateurs vers la personne appropriée.

Action corrective en cas d'accès refusé

La fonctionnalité d'assistance en cas d'accès refusé propose trois moyens de résoudre les problèmes impliquant des erreurs d'accès refusé :

- Mise à jour automatique. Les administrateurs peuvent créer des messages personnalisés d'accès refusé, écrits par l'administrateur du serveur. À l'aide des informations contenues dans ces messages, les utilisateurs peuvent tenter de résoudre eux-mêmes les cas d'accès refusé. Le message peut également comprendre les URL qui dirigent les utilisateurs vers des sites Web d'auto-mise à jour fournis par l'entreprise. Par exemple, l'URL pourrait diriger l'utilisateur vers la modification du mot de passe d'une application ou vers le téléchargement d'une copie actualisée du logiciel côté client.
- Mise à jour par le propriétaire de données. Les administrateurs peuvent définir des propriétaires pour les dossiers partagés. Cela permet aux utilisateurs d'envoyer des messages électroniques aux propriétaires de données afin de demander un accès. Par exemple, si par erreur, un utilisateur n'est pas inclus dans un groupe de sécurité ou si l'attribut du service de l'utilisateur est mal épelé, le propriétaire de données pourra ajouter l'utilisateur au groupe. Si le propriétaire de données ignore comment accorder l'accès à l'utilisateur, il peut transférer ces informations à l'administrateur informatique compétent. C'est pratique parce que le nombre de demandes d'assistance transmises au bureau de support de la part des utilisateurs devrait être limité aux cas particuliers ou aux cas difficiles à résoudre.

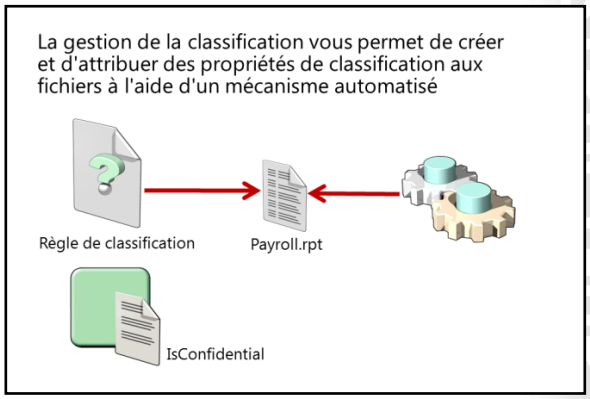
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Mise à jour par les administrateurs d'assistance technique et du serveur de fichiers. Si les utilisateurs ne peuvent pas régler eux-mêmes les problèmes et que les propriétaires de données ne peuvent pas non plus résoudre le problème, alors les administrateurs peuvent résoudre les problèmes en accédant à une interface utilisateur, afin de consulter les autorisations effectives pour l'utilisateur. Les exemples de cas dans lesquels un administrateur doit être impliqué, sont les cas où les attributs de revendications ou les attributs d'objet de ressource sont définis de manière inexacte ou contiennent des informations erronées ; ou lorsque les données elles-mêmes semblent corrompues.

Vous utilisez la stratégie de groupe pour activer la fonctionnalité d'assistance en cas d'accès refusé. Ouvrez l'éditeur d'objet de stratégie de groupe et naviguez à**Configuration ordinateur\Stratégies\Modèles d'administration\Système\Assistance en cas d'accès refusé**. Dans le nœud d'assistance en cas d'accès refusé, vous pouvez activer l'assistance en cas d'accès refusé ; et vous pouvez également fournir les messages personnalisés aux utilisateurs. Autrement, vous pouvez également utiliser la console Gestionnaire de ressources du serveur de fichiers pour activer l'assistance en cas d'accès refusé. Cependant, si l'assistance en cas d'accès refusé est activée dans la stratégie de groupe, les paramètres appropriés de la console Gestionnaire de ressources du serveur de fichiers sont désactivés pour la configuration.

Vous pouvez également utiliser la page **Propriétés de gestion** du gestionnaire de ressources du serveur de fichiers pour configurer un message personnalisé d'assistance en cas d'accès refusé pour une arborescence de dossiers particulière du serveur (par ex. : un message par partage).

Implémenter des classifications de fichiers



Pour implémenter le contrôle d'accès dynamique efficacement, il faut avoir défini correctement les revendications et les propriétés de ressource. Bien que les revendications soient définies par les attributs d'un utilisateur ou d'un périphérique, les propriétés de ressource sont le plus souvent créées et définies manuellement. Les classifications de fichiers permettent aux administrateurs de définir des procédures automatiques, afin d'établir une propriété souhaitée sur le fichier, en fonction des conditions spécifiées dans une règle de classification. Par exemple, vous pouvez définir la propriété **Confidentiality** sur **Haut** sur tous les documents dont le contenu contient le mot « secret. » Vous pourrez alors utiliser cette propriété dans le contrôle d'accès dynamique pour spécifier que seuls les employés dont l'attribut **employeetype** est défini à **Gestionnaire** peuvent accéder à ces documents.

Dans Windows Server 2008 R2 et Windows Server 2012, les tâches de gestion de la classification et des fichiers permettent aux administrateurs de gérer des groupes de fichiers selon divers attributs des fichiers et des dossiers. Avec ces tâches, vous pouvez automatiser les tâches de maintenance des fichiers et des dossiers (par ex. : le nettoyage les données périmées ou la protection des informations confidentielles).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

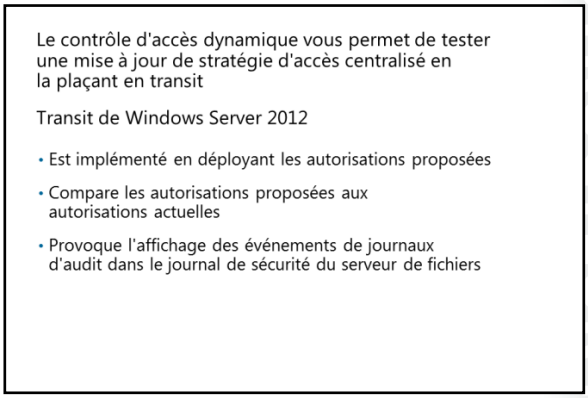
La gestion de la classification est conçue pour simplifier le travail et la gestion des données à l'échelle de l'entreprise. Il existe plusieurs options de classification des fichiers. Dans la plupart des scénarios, vous classez les fichiers manuellement. Dans Windows Server 2008 R2, l'infrastructure de classification des fichiers permet aux entreprises de convertir ces processus manuels en stratégies automatisées. Les administrateurs peuvent spécifier des stratégies de gestion des fichiers selon la classification d'un fichier, puis appliquer des règles d'entreprise pour gérer les données en fonction d'une valeur.

Vous pouvez utiliser la classification des fichiers pour effectuer les tâches suivantes :

- Définir des propriétés et des valeurs de classification, que vous pouvez ensuite attribuer aux fichiers en exécutant des règles de classification.
- Classer un dossier, afin que tous les fichiers contenus dans l'arborescence du dossier héritent de la classification.
- Créer, mettre à jour et exécuter des règles de classification. Chaque règle attribue une propriété et une valeur prédéfinies uniques aux fichiers dans un répertoire spécifié, en fonction des plug-ins de classification installés.
- Réévaluer les fichiers déjà classés lorsque vous exécutez une règle de classification. Vous pouvez choisir de remplacer des valeurs de classification existantes ou ajouter une valeur aux propriétés qui prennent en charge de plusieurs valeurs. Vous pouvez également déclasser les fichiers qui ne sont plus dans les critères de classification.

Implémenter des modifications de stratégie d'accès centralisé

Après avoir implémenté le contrôle d'accès dynamique, vous devez apporter quelques modifications. Par exemple, il se peut que vous deviez mettre à jour des expressions conditionnelles ou que vous souhaitiez modifier des revendications. Cependant, vous devez organiser soigneusement toutes les modifications par rapport aux composants du contrôle d'accès dynamique.



Modifier une stratégie d'accès centralisée peut considérablement affecter l'accès. Par exemple, une modification pourrait potentiellement accorder plus d'accès que désiré ou trop restreindre une stratégie, ce qui entraînerait un nombre excessif d'appels d'assistance technique. Nous vous conseillons de tester les modifications avant d'implémenter une mise à jour de stratégie d'accès centralisée.

Pour ce faire, Windows Server 2012 a introduit le concept de transit. Le transit permet aux utilisateurs de vérifier les mises à jour de leurs stratégies proposées avant de les appliquer. Pour utiliser le transit, déployez la stratégie proposée avec les stratégies appliquées. Cependant, vous n'accordez pas réellement des autorisations d'accès ou des refus d'accès. Au lieu de cela, le système d'exploitation Windows enregistre un événement d'audit (événement 4818) lorsque le résultat du contrôle d'accès qui utilise la stratégie étagée diffère du résultat d'un contrôle d'accès qui utilise la stratégie appliquée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation du contrôle d'accès dynamique

Scénario

L'équipe de recherche du groupe A. Datum Corporation est impliquée dans une mission confidentielle qui crée un chiffre d'affaires conséquent à l'entreprise. En outre, d'autres groupes de A. Datum, tel que le service exécutif, enregistrent fréquemment des fichiers contenant des informations vitales pour l'entreprise sur les serveurs de fichiers de société. Le département sécurité souhaite vérifier que ces fichiers confidentiels sont accessibles uniquement au personnel autorisé et que tout accès à ces fichiers soit audité.

En tant qu'un administrateur réseau principal chez A. Datum, vous êtes responsable de répondre à ces exigences de sécurité en implémentant le contrôle d'accès dynamique sur les serveurs de fichiers. Vous travaillerez étroitement avec les groupes d'entreprises et le département sécurité afin d'identifier les fichiers à sécuriser, ainsi que les personnes qui peuvent y accéder. Vous implémenterez ensuite le contrôle d'accès dynamique selon les exigences de l'entreprise.

Objectifs

- Planifier l'implémentation du contrôle d'accès dynamique
- Configurer les revendications d'utilisateurs et de périphériques
- Configurer les définitions des propriétés de ressource
- Configurer les règles d'accès centralisées et les stratégies d'accès centralisé
- Valider et mettre à jour le contrôle d'accès dynamique
- Implémenter de nouvelles stratégies de ressources

Configuration de l'atelier pratique

Durée approximative : 90 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-CL1** **22412B-LON-CL2**
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22412B-LON-SVR1**.
6. Ne commencez pas **22412B-LON-CL1** et **22412B-LON-CL2** avant d'y être invité.

Exercice 1 : Planification de l'implémentation du contrôle d'accès dynamique

Scénario

La société A. Datum doit s'assurer que les documents utilisés par l'équipe de recherche et le service exécutif sont sécurisés. La plupart des fichiers utilisés par ces services sont actuellement enregistrés dans les dossiers partagés consacrés à ces services, mais les documents confidentiels apparaissent parfois dans d'autres dossiers partagés. Seuls les membres de l'équipe de recherche doivent pouvoir accéder aux dossiers de l'équipe de recherche ; et seuls les gestionnaires de service doivent pouvoir accéder aux documents hautement confidentiels.

Le département sécurité est également mis au courant lorsque les gestionnaires accèdent à des fichiers via leur ordinateur personnel, qui peuvent ne pas être hautement sécurisés. Par conséquent, vous devez créer un plan pour sécuriser les documents, quel que soit l'endroit où ils sont localisés ; et vérifier que les documents peuvent être consultés uniquement à partir des ordinateurs autorisés. Les ordinateurs autorisés des gestionnaires sont membres du groupe de sécurité ManagersWks.

Le service de support technique enregistre qu'un nombre élevé d'appels est généré par des utilisateurs qui ne peuvent pas accéder aux ressources. Vous devez implémenter une fonctionnalité qui aide les utilisateurs à mieux comprendre les messages d'erreur et leur permettra de demander l'accès automatiquement.

Les tâches principales de cet exercice sont les suivantes :

1. Planifier le déploiement du contrôle d'accès dynamique
2. Préparer AD DS pour prendre en charge le contrôle d'accès dynamique

▶ Tâche 1 : Planifier le déploiement du contrôle d'accès dynamique

- Selon le scénario, décrivez comment vous concevrez le Contrôle d'accès dynamique pour remplir les conditions du contrôle d'accès.

▶ Tâche 2 : Préparer AD DS pour prendre en charge le contrôle d'accès dynamique

1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Créez une nouvelle unité d'organisation nommée **Test**.
3. Déplacez les objets d'ordinateur **LON-CL1**, **LON-CL2** et **LON-SVR1** vers **Test unité d'organisation**.
4. Dans LON-DC1, depuis le Gestionnaire de serveur, ouvrez la **Console de gestion des stratégies de groupe**.
5. Enlevez le paramètre **Bloquer l'héritage** qui est appliqué à **Unité d'organisation des gestionnaires**. Faites cela pour enlever le paramètre d'héritage de bloc utilisé dans un module postérieur du cours.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Modifiez l'objet de stratégie de groupe **stratégie de domaine par défaut**.
7. Dans l'Éditeur de gestion des stratégies de groupe, dans Configuration ordinateur, développez **Stratégies**, **Modèles d'administration**, **Système** et cliquez sur **KDC**.
8. Activez le paramètre de stratégie **soutien KDC pour les revendications, l'authentification composée et le blindage Kerberos**.
9. Dans la section **Options**, cliquez sur **Pris en charge**.
10. Dans LON-DC1, actualisez la stratégie de groupe.
11. Ouvrez Utilisateurs et ordinateurs Active Directory et dans le conteneur **Utilisateurs**, créez un groupe de sécurité nommé **ManagersWKS**.
12. Ajoutez **LON-CL1** au groupe **ManagersWKS**.
13. Vérifiez que l'utilisateur **Aidan Delaney** est un membre du service **Gestionnaires** et que **Allie Bellew** est membre du service de **Recherches**. Les entrées de service doivent être renseignées dans l'attribut approprié pour chaque profil d'utilisateur.

Résultats : Après avoir terminé cet exercice, vous aurez organisé le déploiement du contrôle d'accès dynamique et préparé AD DS pour l'implémentation du contrôle d'accès dynamique.

Exercice 2 : Configuration des revendications d'utilisateurs et de périphériques

Scénario

La première étape d'implémentation du contrôle d'accès dynamique est la configuration des revendications des utilisateurs et des périphériques qui accèdent aux fichiers. Dans cet exercice, vous examinerez les revendications par défaut, puis vous créerez de nouvelles revendications selon les attributs du service et la description d'ordinateur. Pour les utilisateurs, vous créerez une revendication pour un attribut de service. Pour les ordinateurs, vous créerez une revendication pour un attribut de description.

Les tâches principales de cet exercice sont les suivantes :

1. Examiner les types de revendication par défaut
2. Configurer des revendications pour des utilisateurs
3. Configurer des revendications pour des périphériques

▶ Tâche 1 : Examiner les types de revendication par défaut

1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez le **Centre d'administration Active Directory**.
2. Dans le Centre d'administration Active Directory, cliquez sur le nœud **Contrôle d'accès dynamique**.
3. Ouvrez le conteneur **Type de revendication** et vérifiez qu'aucune revendication par défaut n'est définie.
4. Ouvrez le conteneur **Propriétés de ressource** et notez que toutes les propriétés sont désactivées par défaut.
5. Ouvrez le conteneur **Resource Property Lists**, puis ouvrez les propriétés de **Global Resource Property List**.
6. Dans la section **Global Resource Property List**, examinez les propriétés de ressources disponibles et cliquez sur **Annuler**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer des revendications pour des utilisateurs

1. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**.
2. Ouvrez le conteneur **Type de revendication** et créez un nouveau type de revendication d'utilisateurs et d'ordinateurs, à l'aide des paramètres suivants :
   - Attribut de la source : **department**
   - Nom complet : **department**

▶ Tâche 3 : Configurer des revendications pour des périphériques

1. Dans le Centre d'administration Active Directory, dans le volet Tâches, cliquez sur **Nouveau**, puis sur **Type de revendication**.
2. Créez un nouveau type de revendication pour les ordinateurs, à l'aide des paramètres suivants :
   - Attribut de la source : **description**
   - Nom complet : **description**

Résultats : Après avoir terminé cet exercice, vous aurez examiné les types de revendication par défaut, configuré les revendications d'utilisateurs et les revendications de périphériques.

Exercice 3 : Configuration des définitions des propriétés de ressource

Scénario

La deuxième étape d'implémentation du contrôle d'accès dynamique est la configuration des listes de propriété de ressource et des définitions de propriété de ressource. Une fois que vous aurez terminé ceci, vous devez établir une nouvelle règle de classification afin de classer tous les fichiers contenant le mot « secret ». Vous devez attribuer la valeur Haut pour la **Confidentialité** de ces fichiers. Vous devez également attribuer la propriété du service au dossier qui appartient à l'équipe de recherche.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les définitions des propriétés de ressource
2. Classer les fichiers
3. Affecter des propriétés à un dossier

▶ Tâche 1 : Configurer les définitions des propriétés de ressource

1. Dans le Centre d'administration Active Directory, cliquez sur **Contrôle d'accès dynamique**, puis ouvrez le conteneur **Resource Properties**.
2. Activez les propriétés de ressource **Department** et **Confidentiality**.
3. Ouvrez les Propriétés de la propriété **Department**.
4. Ajoutez **Research** comme valeur suggérée.
5. Ouvrez **Global Resource Property List**, assurez-vous que **Department** et **Confidentiality** sont compris dans la liste, puis cliquez sur **Annuler**.
6. Fermez le Centre d'administration Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Classer les fichiers

1. Sur LON-SVR1, ouvrez le **Gestionnaire de ressources du serveur de fichiers**.
2. Actualisez **Propriétés de classification** et vérifiez que les propriétés **Confidentiality** et **Department** sont dans la liste.
3. Créez une règle de classification avec les valeurs suivantes :
   - Nom : **Définir la confidentialité**
   - Portée : **C:\Docs**
   - Méthode de classification : **Classifieur de contenus**
   - Propriété : **Confidentiality**
   - Valeur : **High**
   - Paramètres de classification : **Chaîne « secret »**
   - Type d'évaluation : **Ré-évaluez les valeurs de propriété existantes**, puis cliquez sur **Remplacer la valeur existante**
4. Exécutez la règle de classification.
5. Ouvrez une fenêtre de l'**Explorateur de fichiers**, accédez au dossier **C:\Docs**, puis ouvrez la fenêtre **Propriétés** des fichiers **Doc1.txt**, **Doc2.txt** et **Doc3.txt**.
6. Vérifiez les valeurs de **confidentialité**. La confidentialité de Doc1.txt et Doc2.txt doivent être définies à **High**.

▶ Tâche 3 : Affecter des propriétés à un dossier

1. Sur LON-SVR1, ouvrez l'**Explorateur de fichiers**.
2. Accédez à **C:\Research**, et ouvrez ses propriétés.
3. Dans l'onglet **Classification**, définissez la valeur **Service** sur **Research**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré des propriétés de ressource pour des fichiers, classifié des fichiers et attribué des propriétés à un dossier.

Exercice 4 : Configuration des règles d'accès central et des stratégies d'accès centralisées

Scénario

Maintenant que vous avez configuré vos définitions de propriété de ressource, vous devez configurer les règles d'accès centralisées et les stratégies qui lieront les revendications et les définitions de propriété.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer des règles d'accès centralisé
2. Créer une stratégie d'accès centralisé
3. Publier une stratégie d'accès centralisée à l'aide de la stratégie de groupe
4. Appliquer la stratégie d'accès centralisée aux ressources
5. Configurer les paramètres d'action corrective en cas d'accès refusé

▶ Tâche 1 : Configurer des règles d'accès centralisé

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Cliquez sur **Contrôle d'accès dynamique**, puis ouvrez le conteneur **Central Access Rules**.
3. Créez une nouvelle règle d'accès centralisée avec les valeurs suivantes :
   - Nom : **Correspondance de service**
   - Ressource cible : **utilisez la condition Ressource-Department-Est égal à-Research**
   - Autorisations actuelles :
     - Supprimez les **Administrateurs**
     - Ajoutez des **Utilisateurs authentifiés**,
     - Modifiez par la condition **Utilisateur-Service de société-Est égal à-Ressource-Department**
4. Créez une autre règle d'accès centralisée avec les valeurs suivantes :
   - Nom : **Accéder aux documents confidentiels**
   - Ressource cible : **utilisez la condition Ressource-Confidentiality-Est égal à-Valeur-High**
   - Autorisations actuelles :
     - Supprimez les **Administrateurs**
     - Ajoutez des **Utilisateurs authentifiés**
     - Modifiez et définissez la première condition à : **Utilisateur-Groupe-Membre** de **chaque-Valeur-Managers**
   - Autorisations : Définissez la deuxième condition à : **Périphérique-Groupe-Membre** de **chaque-Valeur-ManagersWKS**

▶ Tâche 2 : Créer une stratégie d'accès centralisé

1. Sur LON-DC1, dans le centre d'administration Active Directory, créez une nouvelle **Central Access Policies** avec les valeurs suivantes :
   - Nom : **Protéger les documents confidentiels**
   - Règles comprises : **Accéder aux documents confidentiels**
2. Créez une autre stratégie d'accès centralisée avec les valeurs suivantes :
   - Nom : **Correspondance de service**
   - Règles comprises : **Correspondance de service**
3. Fermez le Centre d'administration Active Directory.

▶ Tâche 3 : Publier une stratégie d'accès centralisée à l'aide de la stratégie de groupe

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez la **console Gestion de stratégie de groupe.**
2. Créez un nouvel objet de stratégie de groupe nommé **Stratégie de DAC** et dans le domaine **Adatum.com**, liez-le au **Test UO**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Modifiez la stratégie de DAC, accédez à **Configuration ordinateur /Stratégies/Paramètres Windows/Paramètres de sécurité/Système de fichiers**, puis cliquez avec le bouton droit sur **Stratégie d'accès centralisée**.
4. Cliquez sur **Gérer les stratégies d'accès centralisées**.
5. Cliquez sur **Correspondance de service** et sur **Protéger les documents confidentiels**, cliquez sur **Ajouter**, puis cliquez sur **OK**.
6. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.

▶ Tâche 4 : Appliquer la stratégie d'accès centralisée aux ressources

1. Sur LON-SVR1, utilisez Windows PowerShell pour actualiser la stratégie de groupe sur LON-SVR1.
2. Ouvrez l'**Explorateur de fichier**s et accédez au dossier **C:\Docs**.
3. Appliquez la stratégie centralisée **Protéger les documents confidentiels** au dossier **C:\Docs**.
4. Accédez au dossier **C:\Research**.
5. Appliquez la stratégie centralisée **Correspondance de service** au dossier **C:\Research**.

▶ Tâche 5 : Configurer les paramètres d'action corrective en cas d'accès refusé

1. Sur LON-DC1, ouvrez la **Console de gestion des stratégies de groupe** et accédez aux **Objets de stratégie de groupe**.
2. Modifiez la **Stratégie DAC**.
3. Dans le nœud **Configuration ordinateur**, accédez à **Stratégies\Modèles d'administration\ Système**, puis cliquez sur **Assistance en cas d'accès refusé**.
4. Dans le volet droit, double-cliquez sur **Personnaliser le message des erreurs d'accès refusé**.
5. Dans la fenêtre Personnaliser le message pour les erreurs d'accès refusé, cliquez sur **Activé**.
6. Dans la zone de texte **Afficher le message suivant aux utilisateurs auxquels l'accès est refusé**, saisissez **Votre accès est refusé en raison de la stratégie d'autorisation. Veuillez demander un accès**.
7. Activez la case à cocher **Permettre aux utilisateurs de demander une assistance**, puis cliquez sur **OK**.
8. Double-cliquez sur **Activer l'assistance en cas d'accès refusé pour tous les types de fichiers**, activez-la, puis cliquez sur **OK**.
9. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.
10. Basculez vers LON-SVR1 et actualisez la Stratégie de groupe.

Résultats : Après avoir complété cet exercice, vous aurez configuré des règles d'accès centralisées et des stratégies d'accès centralisé pour le contrôle d'accès dynamique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 5 : Validation et mise à jour du contrôle d'accès dynamique

Scénario

Pour vérifier que les paramètres du Contrôle d'accès dynamique sont configurés correctement, vous devez pratiquer divers scénarios d'accès. Vous examinerez les utilisateurs et périphériques approuvés, ainsi que les utilisateurs et périphériques non approuvés. Vous validerez également la configuration de mise à jour d'accès.

Les tâches principales de cet exercice sont les suivantes :

1. Valider la fonctionnalité de contrôle d'accès dynamique

▶ Tâche 1 : Valider la fonctionnalité de contrôle d'accès dynamique

1. Démarrez et connectez-vous à **LON-CL1** en tant que **Adatum\April** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur la mosaïque **Bureau**, puis ouvrez l'**Explorateur de fichiers**.
3. Accédez à **\\LON-SVR1\Docs** et vérifiez que vous pouvez ouvrir uniquement Doc3.
4. Essayez d'accéder à **\\LON-SVR1\Research**. Vous ne devriez pas pouvoir y accéder.
5. Déconnectez-vous de LON-CL1.
6. Connectez-vous sur **LON-CL1** en tant que **Adatum\Allie** avec le mot de passe **Pa$$w0rd**.
7. Ouvrez l'**Explorateur de fichiers**, et tentez d'accéder à **\\LON-SVR1\Research**. Vous devriez pouvoir y accéder et ouvrir les fichiers qui s'y trouvent.
8. Déconnectez-vous de LON-CL1.
9. Connectez-vous sur **LON-CL1** en tant que **Adatum\Aidan** avec le mot de passe **Pa$$w0rd**.
10. Ouvrez l'**Explorateur de fichiers** et tentez d'accéder à **\\LON-SVR1\Docs**. Vous devriez pouvoir ouvrir tous les fichiers contenus dans ce dossier.
11. Déconnectez-vous de LON-CL1.
12. Démarrez et connectez-vous à **LON-CL2** en tant que **Adatum\Aidan** avec le mot de passe **Pa$$w0rd**.
13. Ouvrez l'**Explorateur de fichiers** et tentez d'accéder à **\\LON-SVR1\Docs**. Vous ne devriez pas pouvoir consulter Doc1 et Doc2, parce que LON-CL2 n'est pas autorisé à consulter les documents secrets.

Résultats : Après avoir terminé cet exercice, vous aurez validé la fonctionnalité de contrôle d'accès dynamique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 6 : Implémentation de nouvelles stratégies de ressource

Scénario

L'étape finale d'implémentation du contrôle d'accès dynamique est de tester l'effet de l'implémentation d'une nouvelle stratégie de ressource.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le transit pour une stratégie d'accès centralisé
2. Configurer des autorisations intermédiaires
3. Vérifier le transit
4. Utiliser des autorisations effectives pour tester le contrôle d'accès dynamique

▶ Tâche 1 : Configurer le transit pour une stratégie d'accès centralisé

1. Sur LON-DC1, ouvrez **Gestion des stratégies de groupe**.
2. Ouvrez l'**Éditeur de gestion des stratégies de groupe** pour la **Stratégie DAC**.
3. Accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\ Configuration avancée de la stratégie d'audit\Stratégies d'audit**, puis cliquez sur **Accès à l'objet**.
4. Double-cliquez sur **Auditer la stratégie d'accès centralisée intermédiaire**, activez les trois cases à cocher, puis cliquez sur **OK**.
5. Double-cliquez sur **Auditer le système de fichiers**, activez les trois cases à cocher, puis cliquez sur **OK**.
6. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.

▶ Tâche 2 : Configurer des autorisations intermédiaires

1. Sur LON-DC1, ouvrez le **Centre d'administration Active Directory**, puis ouvrez les propriétés pour la règle d'accès centralisée **Correspondance de service**.
2. Dans la section **Autorisations proposées**, configurez la condition des **Utilisateurs authentifiés** comme suit **Utilisateur-Service de société-Est égal à-Valeur-Marketing**.
3. Sur LON-SVR1, actualisez les autorisations.

▶ Tâche 3 : Vérifier le transit

1. Connectez-vous sur **LON-CL1** en tant que **Adatum\Adam** avec le mot de passe **Pa$$w0rd**.
2. Dans l'Explorateur de fichiers, essayez d'accéder à **\\LON-SVR1\Research**, et aux fichiers qu'il contient.
3. Basculez vers **LON-SVR1**.
4. Ouvrez l'**Observateur d'événements**, ouvrez **Sécurité**, puis recherchez et examinez les événements avec l'ID **4818**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Utiliser des autorisations effectives pour tester le contrôle d'accès dynamique

1. Sur LON-SVR1, ouvrez les propriétés du dossier **C:\Research**.
2. Ouvrez les Options **avancées** de **Sécurité**, puis cliquez sur **Accès effectif**.
3. Cliquez sur **Sélectionner un utilisateur**.
4. Dans la fenêtre Sélectionner des utilisateurs, Ordinateur, Compte de service ou Groupe, saisissez **April**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
5. Cliquez sur **Afficher l'accès effectif**.
6. Vérifiez les résultats. L'utilisateur ne devrait pas avoir accès à ce dossier.
7. Cliquez sur **Inclure une revendication utilisateur**.
8. Dans la liste déroulante, cliquez sur **Service de société**.
9. Dans la zone de texte **Valeur**, saisissez **Research**.
10. Cliquez sur **Afficher l'accès effectif**. L'utilisateur devrait maintenant y avoir accès.
11. Fermez toutes les fenêtres.

Résultats : À la fin de cet exercice, vous aurez implémenté de nouvelles stratégies de ressource.

▶ Pour préparer le module suivant

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-CL1** et **22412B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée :

- Utilisez des stratégies d'accès centralisé au lieu de configurer des expressions conditionnelles sur les ressources.
- Activez les paramètres d'assistance en cas d'accès refusé.
- Testez toujours les modifications que vous avez apportées aux règles d'accès centralisées et aux stratégies d'accès centralisé avant de les implémenter.
- Utilisez les classifications de fichiers pour attribuer des propriétés aux fichiers.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les revendications ne sont pas remplies avec les valeurs appropriées.	
Une expression conditionnelle bloque l'accès.	

Questions de contrôle des acquis

Question : Qu'est-ce qu'une revendication ?

Question : Quel est le rôle des stratégies d'accès centralisé ?

Question : Qu'est-ce que l'assistance en cas d'accès refusé ?

Outils

Outil	Utilisation	Emplacement
Centre d'administration Active Directory	Administrer et créer des revendications, des propriétés de ressource, des règles et des stratégies	Outils d'administration
Console de gestion des stratégies de groupe (GPMC, Group Policy Management Console)	Gérer une stratégie de groupe	Outils d'administration
Éditeur de gestion des stratégies de groupe	Modifier des objets de stratégie de groupe (GPO)	GPMC

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4

Implémentation des déploiements de services de domaine Active Directory distribués

Table des matières :

Vue d'ensemble du module **4-1**

Leçon 1 : Vue d'ensemble des déploiements AD DS distribués **4-2**

Leçon 2 :Déploiement d'un environnement AD DS distribué **4-8**

Leçon 3 : Configuration d'approbations AD DS **4-18**

Atelier pratique : Implémentation des déploiements AD DS distribués. **4-25**

Contrôle des acquis et éléments à retenir **4-29**

Vue d'ensemble du module

Pour la plupart des organisations,le déploiement de services de domaine Active Directory® (AD DS) est le composant le plus important de l'infrastructure informatique. Quand les organisations déploient AD DS ou n'importe quel autre service lié à Active Directory–dans Windows Server® 2012, ils déploient un service central d'authentification et d'autorisation qui permet l'accès par authentification unique (SSO) à de nombreux autres services et applications en réseau dans l'organisation. AD DS permet également la gestion basée sur la politique de l'entreprise pour l'utilisateur et les comptes d'ordinateur.

La plupart des organisations déploie un domaine AD DS unique. Cependant, certaines organisations nécessitent un déploiement AD DS plus complexe qui peut comprendre plusieurs domaines ou forêts.

Ce module traite des composants clés d'un environnement complexe AD DS ainsi que de l'installation et de la configuration d'un déploiement AD DS complexe.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- Décrire les composants des déploiements AD DS distribués.
- Expliquer comment déployer un déploiement AD DS distribué.
- Expliquer comment configurer des approbations d'AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble des déploiements AD DS distribués

Avant de commencer la configuration d'un déploiement AD DS complexe, il est important de connaître les composants constitutifs de la structure AD DS, et la manière dont ils interagissent entre eux pour pouvoir fournir un environnement informatique évolutif et sécurisé. La leçon commence par l'examen des divers composants d'un environnement AD DS, puis explore les raisons pour lesquelles une organisation peut choisir de déployer un environnement AD DS complexe.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les composants d'un environnement AD DS.
- Expliquer comment les domaines et les forêts AD DS constituent des limites en termes de sécurité et d'administration.
- Décrire pourquoi il peut être nécessaire d'avoir plus d'un domaine dans un environnement AD DS.
- Expliquer pourquoi il peut être nécessaire d'avoir plus d'une forêt dans un environnement AD DS.
- Expliquer l'importance du système DNS (Domain Name System) dans une structure AD DS complexe.

Discussion : Vue d'ensemble des composants AD DS

Un environnement AD DS comporte différents composants. Il est important de comprendre la raison d'être de chaque composant, et la manière dont ils interagissent les uns avec les autres.

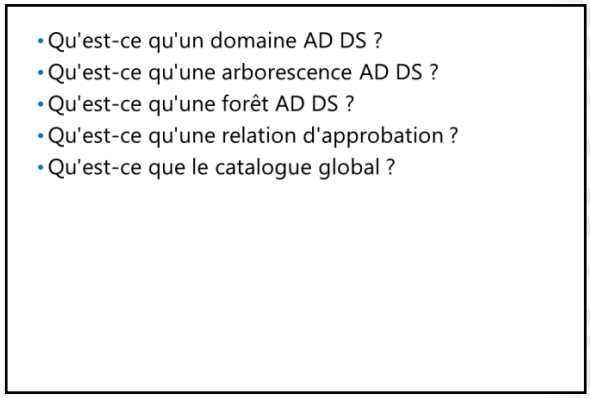
Question : Qu'est-ce qu'un domaine AD DS ?

Question : Qu'est-ce qu'une arborescence de domaine AD DS ?

Question : Qu'est-ce qu'une forêt AD DS ?

Question : Que sont les relations d'approbation ?

Question : Qu'est-ce que le catalogue global ?



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des limites de domaine et de forêt dans une structure AD DS

Les domaines et les forêts AD DS fournissent différents types de limites à l'intérieur d'un déploiement AD DS. La bonne compréhension des différents types de limites est essentielle à la gestion d'un environnement AD DS complexe.

Objet AD DS	Type de limite
Domaine	Réplication de partition de domaine
	Autorisations administratives
	Application de la stratégie de groupe
	Audit
	Stratégies de mot de passe et de compte
	Réplication de zone de domaine DNS
Forêt	Limite de sécurité
	Réplication de partition de schéma
	Réplication de partition de configuration
	Réplication de catalogue global
	Réplication de zone DNS de forêt

Limites de domaine AD DS

Le domaine AD DS présente les limites suivantes :

- Limite de réplication pour la partition de domaine. Tous les objets AD DS d'un domaine unique sont enregistrés dans la partition de domaine dans la base de données AD DS sur chaque contrôleur de domaine du domaine. Le processus de réplication garantit que toutes les mises à jour sont répliquées à tous les autres contrôleurs de domaine du même domaine. Les données du domaine de partition ne sont pas répliquées dans les contrôleurs de domaine appartenant à d'autres forêts.
- Limite d'administration. Par défaut, un domaine AD DS comprend plusieurs groupes, tels que le groupe Administrateurs du domaine, dont les membres ont le contrôle administratif total du domaine. Vous pouvez également attribuer des autorisations administratives à des comptes d'utilisateurs et des groupes à l'intérieur des domaines. Excepté le groupe Administrateurs de l'entreprise dans le domaine racine de forêt, les comptes d'administrateur n'ont aucun droit administratif dans d'autres domaines de forêt ou dans d'autres forêts.
- Limite de l'application d'une stratégie de groupe. Des stratégies de groupe peuvent être liées aux niveaux suivants : local, site, domaine, et unité d'organisation (OU). Mises à part les stratégies de groupe s'appliquant au niveau du site, l'étendue des stratégies de groupe est le domaine AD DS. Il n'y a pas d'héritage des stratégies de groupe d'un domaine AD DS à l'autre, même si un domaine AD DS est inférieur à un autre dans une arborescence de domaine.
- Limite d'audit. L'audit est géré de manière centrale à l'aide des objets de stratégie de groupe (GPO). L'étendue maximum de ces paramètres est le domaine AD DS. Il est possible d'avoir les mêmes paramètres d'audit dans différents domaines AD DS, mais dans ce cas, ils doivent être gérés séparément dans chaque domaine.

- Limites de stratégie de mot de passe et de compte. Par défaut, les stratégies de mot de passe et de compte sont définies au niveau du domaine et appliquées à tous les comptes de domaine. Alors qu'il est possible de configurer des stratégies de mot de passe précises pour configurer différentes stratégies pour les utilisateurs spécifiques d'un domaine, l'application des stratégies de mot de passe et de compte est limitée à ce seul domaine.
- Limite de réplication pour des zones DNS de domaine. Lors de la configuration des zones DNS dans un environnement AD DS, vous avez la possibilité de configurer des zones intégrées–Active Directory. Ceci signifie qu'au lieu que les enregistrements DNS soient stockés localement sur chaque serveur DNS sous forme de fichiers texte, ils sont stockés et répliqués dans la base de données AD DS. L'administrateur peut alors décider de répliquer les informations DNS à tous les contrôleurs de domaine du domaine (indépendamment du fait qu'elles soient ou pas sur les serveurs DNS), à tous les contrôleurs de domaine qui sont des serveurs DNS du domaine, ou à tous les contrôleurs de domaine qui sont des serveurs DNS de la forêt. Par défaut, quand vous déployez le premier contrôleur de domaine dans un domaine d'AD DS, et configurez ce serveur en tant que serveur DNS, deux partitions distinctes de réplication sont créées. Elles sont appelées : domainDnsZones et forestDnsZones. La partition de domainDnsZones contient les enregistrements DNS spécifiques au domaine, et n'est répliquée qu'aux autres serveurs DNS qui sont également des contrôleurs de domaine AD DS du domaine.

Limites de forêt AD DS

Les actes de la forêt AD DS fournissent les limites suivantes :

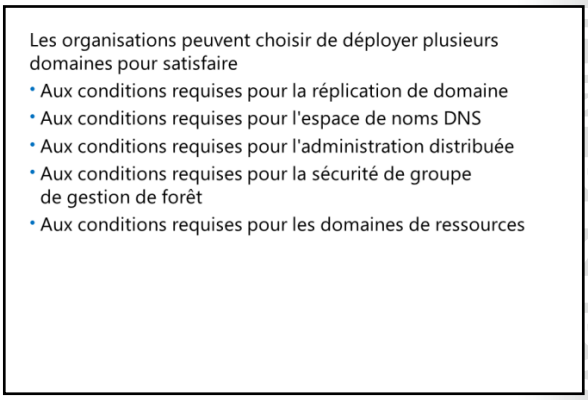
- Limite de sécurité. La limite de forêt est une limite de sécurité parce que par défaut, aucun compte en dehors de la forêt n'a quelque autorisation administrative que ce soit à l'intérieur de la forêt.
- Limite de réplication pour la partition de schéma. La partition de schéma contient les règles et la syntaxe applicables à la base de données AD DS. Elle est répliquée sur tous les contrôleurs de domaine de la forêt AD DS.
- Limite de réplication pour la configuration de partition. La partition de configuration contient les détails de la structure de domaine AD DS, dont : les domaines, contrôleurs de domaine, partenaires de réplication, site et informations de sous-réseau, et autorisation de protocole DHCP (Dynamic Host Configuration Protocol) ou la configuration du contrôle d'accès dynamique. La partition de configuration contient également des informations sur les applications intégrées à la base de données AD DS. Exchange Server 2010 en est un exemple. Cette partition est répliquée à tous les contrôleurs de domaine dans la forêt.
- Limite de réplication pour le catalogue global. Le catalogue global est la liste en lecture seule contenant chaque objet appartenant à la forêt AD DS. Pour que sa taille reste gérable, le catalogue global contient seulement quelques attributs pour chaque objet. Le catalogue global est répliqué sur tous les contrôleurs de domaine qui sont aussi des serveurs de catalogue global dans la forêt.
- Limite de réplication pour les zones DNS de forêt. La partition forestDnsZones est répliquée sur tous les contrôleurs de domaine qui sont aussi des serveurs DNS dans l'ensemble de la forêt. Cette zone contient des enregistrements importants pour l'activation de la résolution de noms DNS à l'échelle de la forêt.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pourquoi implémenter plusieurs domaines ?

Beaucoup d'organisations peuvent fonctionner convenablement avec un seul domaine AD DS. Cependant, certaines organisations nécessitent le déploiement de plusieurs domaines. Parmi ces besoins, peuvent se trouver :



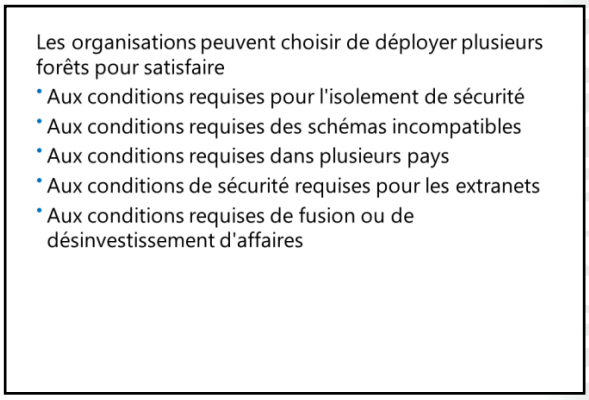
- Les conditions requises pour la réplication de domaine. Certaines organisations ont plusieurs grands bureaux connectés les uns aux autres par des réseaux étendus lents ou peu fiables (Wan). Les connexions réseau nécessitent une bande passante suffisamment large pour prendre en charge la réplication AD DS de la partition de domaine. Il peut être alors judicieux d'installer un domaine AD DS séparé dans chaque bureau.
- Les conditions requises pour l'espace de noms DNS. Certaines organisations nécessitent plusieurs espaces de noms DNS dans une forêt AD DS. C'est en général le cas quand une société en acquiert une autre, ou fusionne avec une autre organisation, et qu'il y a besoin de conserver les noms de domaine de l'environnement existant. Même s'il est alors possible de fournir plusieurs noms d'utilisateur principal (UPN) aux utilisateurs d'un domaine, beaucoup d'organisations choisissent plutôt de déployer plusieurs domaines.
- Les conditions requises pour l'administration distribuée. Il se peut que des organisations aient des exigences stratégiques ou des configurations requises de sécurité d'entreprise qui font qu'elles sont organisées selon un modèle d'administration décentralisée. Le déploiement d'un domaine séparé peut permettre l'autonomie administrative des organisations. Avec ce type de déploiement, les administrateurs de domaine ont un contrôle total de leurs domaines.

Remarque : Le déploiement de domaines distincts entraîne l'autonomie administrative, pas l'isolement administratif. La seule façon de garantir l'isolement administratif est de déployer une forêt distincte.

- Les conditions requises pour la sécurité de groupe de gestion de forêt. Certaines organisations choisissent de déployer un domaine racine dédié ou vide. C'est un domaine qui n'a pas d'autre compte d'utilisateur que les comptes par défaut du domaine racine de forêt. Le domaine racine de forêt AD DS comporte deux groupes—le groupe Administrateurs du schéma et le groupe Administrateurs de l'entreprise—qui n'existent que dans ce domaine de forêt AD DS. Ces groupes ayant des droits étendus dans la forêt AD DS, il peut être préférable de restreindre l'utilisation de ces groupes en n'utilisant le domaine racine de forêt AD DS que pour leur stockage.
- Conditions requises pour les domaines de ressources. Certaines organisations déploient des domaines de ressources pour déployer des applications spécifiques. Avec ce type de déploiement, tous les comptes d'utilisateurs sont situés dans un domaine, tandis que les serveurs d'applications et les comptes d'administration d'applications sont déployés dans un domaine distinct. Ceci permet aux administrateurs d'application d'avoir des autorisations administratives pour tout le domaine dans le domaine de ressources sans activer d'autorisation dans le domaine contenant les comptes d'utilisateurs normaux.

Pourquoi implémenter plusieurs forêts ?

Les organisations peuvent parfois demander à ce que leur AD DS contienne plus d'une forêt. Il y a plusieurs raisons pour lesquelles une forêt AD DS peut ne pas être insuffisante :



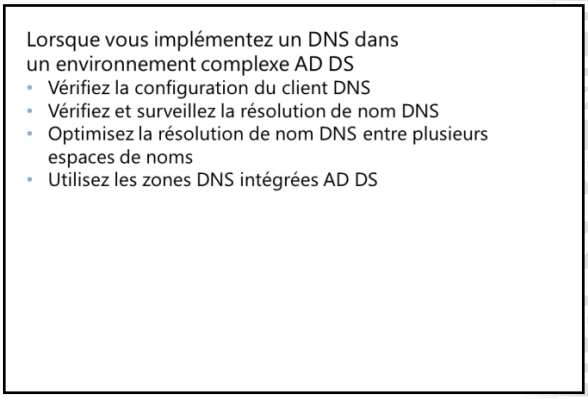
- Des conditions requises pour l'isolement de sécurité. Quand une organisation a besoin de l'isolement administratif entre deux parties, elle doit déployer plusieurs forêts AD DS. Des forêts AD DS distinctes sont souvent déployées par des sous-traitants du gouvernement dans le secteur de la défense et d'autres organisations où l'isolement de sécurité est une configuration requise.
- Schémas incompatibles. Certaines organisations ont besoin de plusieurs forêts parce qu'elles ont besoin de schémas incompatibles ou des schémas incompatibles modifient les processus. Le schéma est partagé entre tous les domaines dans une forêt.
- Conditions requises dans plusieurs pays. Certains pays ont des règlements stricts concernant la propriété ou la gestion des entreprises sur leur sol. Une forêt distincte AD DS peut satisfaire la condition d'isolement administratif requise par la législation.
- Conditions de sécurité requises pour les extranets. Certaines organisations disposent de plusieurs serveurs déployés dans un réseau de périmètre. Ces serveurs peuvent avoir besoin d'AD DS pour authentifier des comptes d'utilisateurs, ou peuvent l'utiliser pour appliquer les stratégies sur les serveurs dans le réseau de périmètre. Pour garantir autant que possible la sécurité de l'extranet AD DS, les organisations configurent souvent une forêt distincte AD DS dans le réseau de périmètre.
- Conditions requises de fusion ou de désinvestissement d'affaires. Une des raisons les plus communes pour lesquelles les organisations disposent de plusieurs forêts AD DS est la fusion d'affaires. Quand des organisations fusionnent, ou qu'une organisation en achète une autre, la configuration requise pour fusionner les forêts AD DS déployées dans les deux organisations doit être évaluée. La fusion des forêts AD DS procure les avantages liés à une collaboration et une administration simplifiées. Cependant, si les deux groupes de l'organisation vont continuer à être gérés séparément, et s'il y a peu de besoins de collaboration, fusionner les deux forêts peut ne pas valoir la peine. En particulier, s'il y a quelque projet que ce soit de vendre une partie de la société, il est préférable de maintenir les deux organisations en tant que forêts distinctes.

Méthode conseillée : La meilleure pratique consiste en choisir la conception la plus simple atteignant le but recherché. En effet, une telle structure est moins coûteuse à implémenter et plus simple à gérer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configurations requises de DNS pour les environnements complexes AD DS

AD DS a besoin de DNS pour fonctionner correctement, et l'implémentation de DNS dans un environnement multidomaines ou à forêts multiples exige un niveau supplémentaire de planification.



Lors du déploiement d'une structure DNS de prise en charge d'un environnement AD DS complexe, vous devez répondre à des exigences dans plusieurs domaines de configuration :

- Vérifiez la configuration du client DNS. Configurez tous les ordinateurs du domaine AD DS avec au moins deux adresses de serveurs DNS fonctionnels. Tous les ordinateurs doivent avoir une bonne connectivité réseau avec les serveurs DNS.
- Vérifiez et surveillez la résolution de nom DNS. Vérifiez que tous vos ordinateurs, y compris les contrôleurs de domaine, peuvent effectuer avec succès des recherches DNS pour tous les contrôleurs de domaine de la forêt. Les contrôleurs de domaine doivent pouvoir se connecter à d'autres contrôleurs de domaine pour répliquer avec succès des modifications faites sur AD DS. Les ordinateurs clients doivent pouvoir localiser des contrôleurs de domaine à l'aide des enregistrements de service SRV, et doivent pouvoir régler les noms de contrôleurs de domaine en fonction des adresses IP. Dans un environnement multi domaines ou multi forêts, les ordinateurs clients peuvent avoir besoin de localiser les ordinateurs de domaine de n'importe quel domaine pour pouvoir valider les approbations lors de l'accès aux ressources d'un autre domaine.
- Optimisez la résolution de nom DNS entre plusieurs espaces de noms. Quand les organisations déploient plusieurs arborescences dans une forêt AD DS, ou quand elles déploient plusieurs forêts, la résolution de noms est plus compliquée parce que plusieurs espaces de noms de domaine doivent être gérés. Utilisez les fonctionnalités DNS telles que le transfert conditionnel, les zones de stub, et la délégation pour optimiser le processus de résolution des noms d'ordinateur pour l'ensemble des espaces de noms.
- Utilisez les zones DNS intégrées AD DS. Quand vous configurez une zone DNS en tant qu'AD DS intégré, les informations DNS sont enregistrées dans AD DS et répliquées par le processus normal de réplication AD DS. Cela optimise le processus de réplication des modifications dans toute la forêt. Vous pouvez également configurer l'étendue de la réplication pour les zones DNS. Par défaut, des enregistrements DNS spécifiques au domaine seront répliqués à d'autres contrôleurs de domaine qui sont également des serveurs DNS du domaine. Des enregistrements DNS qui activent des recherches inter domaines sont enregistrés dans la zone _msdcs.forestrootdomainname et sont répliqués aux contrôleurs de domaine qui sont également des serveurs DNS de l'ensemble de la forêt. Cette configuration par défaut ne doit pas être modifiée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Déploiement d'un environnement AD DS distribué

Certaines organisations doivent déployer plusieurs domaines ou même plusieurs forêts. Le déploiement de contrôleurs de domaine AD DS dans cette situation n'est pas beaucoup plus compliqué que celui de contrôleurs de domaine dans un environnement à domaine unique, mais il y a quelques points particuliers dont il faut tenir compte.

Dans cette leçon, vous allez apprendre comment déployer un environnement AD DS complexe, et voir comment faire la mise à niveau d'une version précédente d'AD DS.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Expliquer comment installer un contrôleur de domaine dans un nouveau domaine d'une forêt.
- Décrire les niveaux fonctionnels de domaine AD DS.
- Décrire les niveaux fonctionnels de forêt AD DS.
- Expliquer comment faire la mise à niveau d'une version précédente d'AD DS à la version Windows Server 2012.
- Expliquer comment migrer d'une version précédente d'AD DS à la version Windows Server 2012.

Démonstration : Installer un contrôleur de domaine dans un nouveau domaine d'une forêt.

Dans cette démonstration, vous allez apprendre à :

- configurer un contrôleur de domaine AD DS ;
- accéder au contrôleur de domaine AD DS.

Procédure de démonstration

Configurez LON-SVR1 en tant que contrôleur de domaine AD DS dans atl.adatum.com

1. Ouvrez une session sur **LON-DC1** en tant qu' **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-DC1, dans le Gestionnaire de serveurs, utilisez l'assistant d'installation AD DS pour installer à distance AD DS sur LON-SVR1.
3. Utilisez l'assistant d'installation AD DS pour installer et configurer LON-SVR1 comme contrôleur de domaine AD DS dans un nouveau domaine, atl.adatum.com.

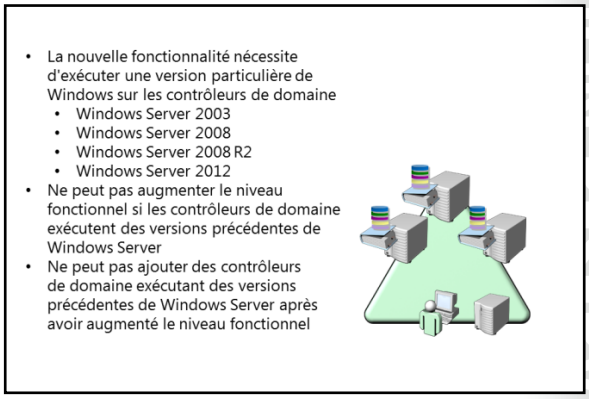
Accédez à LON-SVR1 en tant qu'ADATUM\Administrateur

1. Sélectionnez les options d'installation de DNS et du catalogue global, et définissez le mot de passe pour le compte administrateur de mode de restauration des services d'annuaire.
2. Redémarrez et connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**, sur le contrôleur de domaine AD DS nouvellement créé, **LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Niveaux fonctionnels de domaine AD DS

Les domaines AD DS peuvent s'exécuter à différents niveaux fonctionnels. En général, la mise à niveau du domaine à un niveau fonctionnel supérieur va introduire des fonctionnalités supplémentaires. Certains niveaux fonctionnels du domaine sont listés dans le tableau suivant.



Niveau fonctionnel de domaine	Fonctionnalités
Microsoft Windows® 2000 Server natif	• Groupes universels • Groupes d'imbrication • Historique d'identificateur de sécurité (SID) • Installer des contrôleurs de domaine à partir d'un support : Installez à partir de supports permet l'installation d'un contrôleur de domaine AD DS sans incidence sur la connexion réseau, car la majorité de la nouvelle base de données AD DS est restaurée localement à partir d'une copie de sauvegarde ntdsutil sur une clé USB ou un lecteur DVD. Après que le nouveau contrôleur de domaine AD DS est installé et redémarré, il utilise le réseau pour récupérer AD DS en lançant les mises à jour qui ont été faites depuis le moment où la copie de sauvegarde ntdsutil a été faite. **Remarque :** Des contrôleurs de domaine de Windows Server 2012 ne peuvent pas être installés dans un domaine qui s'exécute au niveau de Windows 2000 Server natif.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Niveau fonctionnel de domaine	Fonctionnalités
Windows Server 2003	• **LastLogonTimestamp** est un attribut qui se souvient de la dernière ouverture de session de domaine des utilisateurs, et la réplique sur d'autres contrôleurs de domaine AD DS dans le domaine AD DS. • La délégation contrainte rend cela possible pour que les applications tirent profit de la délégation sécurisée des informations d'identification de l'utilisateur à l'aide de l'authentification basée sur Kerberos. • L'authentification sélective permet de spécifier quels utilisateurs et groupes sont autorisés à s'authentifier auprès des serveurs spécifiques de ressources dans une forêt d'approbation. • Vous pouvez enregistrer des zones DNS dans des partitions d'application, ce qui permet qu'elles soient répliquées sur les contrôleurs de domaine qui sont également des serveurs DNS dans le domaine, ou même dans la forêt. • Des attributs de groupe et d'autres attributs à valeurs multiples sont répliqués au niveau d'attribut, au lieu du niveau d'objet. Dans les versions précédentes AD DS, l'appartenance au groupe était considérée comme une partie de l'objet, et le groupe était répliqué en tant qu'objet unique. Cela voulait dire que si deux administrateurs modifiaient leur adhésion au même groupe pendant la même période de réplication, c'était la dernière écriture qui l'emportait. Les premières modifications apportées étaient perdues, parce que la nouvelle version du groupe remplaçait entièrement la précédente. Avec la réplication à valeurs multiples, l'appartenance au groupe est traitée au niveau de l'attribut, et donc toutes les mises à jour d'origine sont fusionnées ensemble. Cela réduit également considérablement le trafic de réplication qui avait alors lieu. Cela présente l'avantage supplémentaire de supprimer la restriction précédente d'appartenance au groupe, restriction qui limitait le nombre maximum de membres à 5000.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Niveau fonctionnel de domaine	Fonctionnalités
Windows Server 2008	• La réplication de système de fichiers DFS (Distributed File System) représente un service de réplication de fichiers plus efficace et plus fiable pour les dossiers SYSVOL. La réplication DFS peut remplacer le service de réplication de fichiers NT, NTFRS (NT File Replication Service). • Un grand nombre d'informations d'ouverture de session interactive est enregistré pour chaque utilisateur, pas seulement le moment de la dernière ouverture de session. • Les paramètres précis de mot de passe permettent la définition de stratégies de compte pour des utilisateurs et des groupes, et remplacent les paramètres par défaut de domaine pour ces utilisateurs ou membres de groupe. • Les bureaux virtuels personnels sont disponibles pour que les utilisateurs se connectent, à l'aide de RemoteApp et de Bureau à distance. • Les services de chiffrement avancés AES (Advanced Encryption Standard) (AES 128 et 256) sont pris en charge pour Kerberos. • Les contrôleurs de domaine en lecture seule (RODC) constituent une manière sécurisée et économique de fournir des services d'ouverture de session AD DS sur des sites distants, sans enregistrer d'informations confidentielles (telles que des mots de passe) dans les environnements non fiables. • Le groupe et d'autres attributs à multi valeurs sont répliqués au niveau de la valeur, au lieu d'être répliqués ensemble (ce qui a supprimé la limite de 5000 utilisateurs par groupe).
Windows Server 2008 R2	• L'assurance de mécanisme d'authentification, qui rassemble les informations sur la méthode d'ouverture de session d'un utilisateur, peut être utilisée en conjonction avec l'authentification de l'application—par exemple, avec des services AD FS (Active Directory Federation Services). Autre exemple : un utilisateur ouvrant une session à l'aide d'une carte à puce peut se voir accorder l'accès à plus de ressources que s'il se connecte à l'aide d'un nom d'utilisateur et d'un mot de passe. • Les comptes de services gérés permettent la gestion des mots de passe du compte par le système d'exploitation Windows, et la gestion des noms principaux de service (SPN).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

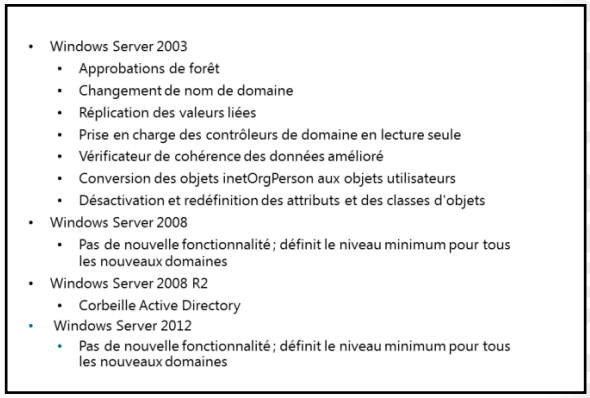
Niveau fonctionnel de domaine	Fonctionnalités
Windows Server 2012	Le niveau fonctionnel du domaine de Windows Server 2012 n'implémente pas de nouvelles fonctionnalités du niveau fonctionnel de Windows 2008 R2, à une exception près : Si la prise en charge du centre de distribution de clés (KDC) des réclamations, l'authentification composée, et le blindage Kerberos sont configurés pour **Toujours fournir les réclamations** ou **Rejeter les demandes d'authentification non blindées**, ces fonctionnalités ne seront pas activées tant que le domaine n'est pas défini au niveau de Windows Server 2012.

Remarque : D'une manière générale, il n'est pas possible de restaurer des niveaux fonctionnels de domaine AD DS. Cependant, dans Windows Server 2012 et Windows Server 2008 R2, vous pouvez restaurer à un niveau minimum de Windows Server 2008, tant que vous n'activez pas des fonctionnalités facultatives (telles que la Corbeille). Si vous avez implémenté une fonctionnalité qui n'est disponible qu'à un niveau fonctionnel du domaine supérieur, vous ne pouvez pas restaurer à un état antérieur.

Documentation supplémentaire : Pour en savoir plus au sujet des niveaux fonctionnels de domaine AD DS, référez-vous à Comprendre les niveaux fonctionnels des services de domaine Active Directory à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=270028.

Niveaux fonctionnels de forêt AD DS

La forêt AD DS peut s'exécuter à différents niveaux fonctionnels. Parfois l'élévation du niveau fonctionnel de la forêt AD DS rend disponibles des fonctionnalités supplémentaires. Les fonctionnalités supplémentaires les plus apparentes viennent avec la mise à niveau fonctionnelle de la forêt de Windows Server 2003. Les fonctionnalités supplémentaires qui sont rendues disponibles avec Windows Server 2003 comprennent :



- Approbations de forêt. Les forêts AD DS peuvent avoir des approbations définies entre elles, ce qui active le partage des ressources. Il existe des approbations totales et des approbations sélectives.
- Réplication des valeurs liées. Cette fonctionnalité a amélioré la réplication de Windows 2000 Server, et a amélioré la gestion de l'appartenance à un groupe.
- Algorithmes améliorés de calcul de réplication AD DS. Le vérificateur de cohérence des données (KCC) et l'utilisation du générateur de topologie d'intersite (ISTG) ont amélioré les algorithmes pour accélérer le calcul de l'infrastructure de réplication AD DS, et permettent des calculs de liaison entre sites beaucoup plus rapides.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Prise en charge des contrôleurs de domaine en lecture seule. Les RODC sont pris en charge au niveau fonctionnel de la forêt de Windows Server 2003. Le RODC doit s'exécuter sous Windows Server 2008 ou une version plus récente.
- Conversion des objets inetOrgPerson aux objets utilisateurs. Vous pouvez convertir une instance d'un objet inetOrgPerson, utilisé pour la compatibilité avec certains services d'annuaire autre que Microsoft, dans une instance d'utilisateur de classe. Vous pouvez également convertir un objet utilisateur à un objet inetOrgPerson.
- Désactivation et redéfinition des attributs et des classes d'objets. Bien que vous ne puissiez pas supprimer un attribut ou une classe d'objets dans le schéma au niveau fonctionnel de Windows Server 2003, vous pouvez désactiver ou redéfinir des attributs ou des classes d'objets.

Le niveau fonctionnel de la forêt de Windows Server 2008 n'ajoute pas de nouvelles fonctionnalités au niveau de la forêt. Le niveau fonctionnel de la forêt de Windows Server 2008 R2 ajoute la fonctionnalité Corbeille Active Directory. Cette fonctionnalité permet la restauration des objets Active Directory supprimés.

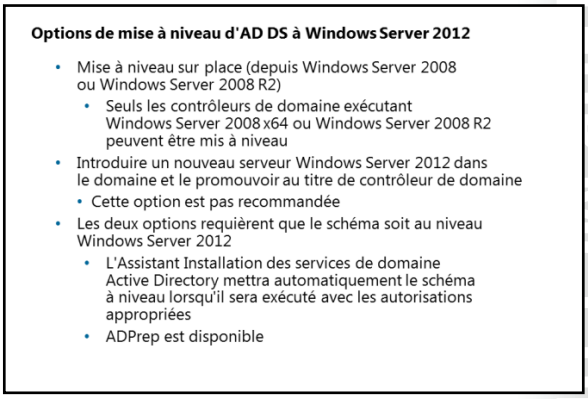
Bien que le niveau fonctionnel de la forêt de Windows Server 2008 R2 AS DS ait introduit la Corbeille AD DS, celle-ci devait être gérée avec Windows PowerShell. Cependant, la version des outils d'administration de serveur distant (Remote Server Administration Tools) (RSAT) qui vient avec Windows Server 2012 a la capacité de gérer la Corbeille AD DS à l'aide d'outils d'interface utilisateur graphique (GUI).

Le niveau fonctionnel de la forêt de Windows Server 2012 n'ajoute pas de nouvelles fonctionnalités au niveau de la forêt. En élevant le niveau fonctionnel de la forêt, vous limitez les niveaux fonctionnels possibles de domaine, des domaines que vous ajoutez à la forêt. Par exemple, si vous définissez le niveau fonctionnel de forêt pour Windows Server 2012, il est impossible d'ajouter un nouveau domaine qui s'exécute au niveau fonctionnel de domaine de Windows Server 2008 R2.

Mise à niveau d'une version antérieure d'AD DS à Windows Server 2012

Pour mettre une version antérieure AD DS au niveau de Windows Server 2012 AD DS, vous pouvez utiliser l'une ou l'autre des deux méthodes suivantes :

- Mettre le système d'exploitation au niveau de Windows Server 2012sur les contrôleurs de domaine existants.
- Introduire les serveurs de Windows Server 2012 en tant que contrôleurs de domaine dans le domaine existant. Vous pouvez alors désaffecter les contrôleurs de domaine AD DS qui exécutent des versions antérieures d'AD DS.



La mise à niveau de systèmes d'exploitation - en particulier sur des serveurs qui fonctionnent depuis plusieurs années - étant souvent difficile, nous préférons la deuxième méthode. En effet, avec l'installation de nouveaux contrôleurs de domaine qui s'exécutent sous Windows Server 2012, vous aurez une installation entièrement nouvelle du système d'exploitation Windows Server 2012.

Vous pouvez déployer des serveurs de Windows Server 2012 comme serveurs membres dans un domaine avec des contrôleurs de domaine exécutant Windows Server 2003 ou une version plus récente. Cependant, avant que vous puissiez installer le premier contrôleur de domaine qui exécute Windows Server 2012, vous devez mettre le schéma à niveau. Dans les versions d'AD DS antérieures à Windows Server 2012, l'outil adprep.exe était exécuté pour effectuer les mises à niveau de schéma. Lors du déploiement de nouveaux contrôleurs de domaine de Windows Server 2012 dans un domaine existant, si vous avez ouvert une session avec un compte membre des administrateurs du schéma et des groupes Administrateurs de l'entreprise, l'Assistant d'installation des services de domaine Active Directory met automatiquement à niveau le schéma de forêt AD DS.

Remarque : Windows Server 2012 continue de fournir une version 64 bits d'ADPrep de manière à ce que vous puissiez exécuter Adprep.exe séparément. Par exemple, si l'administrateur qui installe le premier contrôleur de domaine de Windows Server 2012 n'est pas membre du groupe Administrateurs de l'entreprise, vous devrez exécuter la commande séparément. Vous ne devez exécuter adprep.exe que si vous prévoyez une mise à niveau sur place pour le premier contrôleur de domaine de Windows Server 2012 dans le domaine.

Le processus de mise à niveau

Pour mettre à niveau le système d'exploitation d'un contrôleur de domaine, de Windows Server 2008 à Windows Server 2012 :

1. Insérez le disque d'installation de Windows Server 2012, et exécutez l'**Installation**.
2. Après la page de sélection de la langue, cliquez sur **Installer maintenant**.
3. Après la fenêtre de sélection du système d'exploitation et la page d'acceptation de licence, dans la fenêtre Quel type d'installation souhaitez-vous ?**,** cliquez sur **Mise à niveau : Installer Windows et conserver les fichiers, les paramètres, et les applications**.

De cette manière, l'AD DS du contrôleur de domaine est mis à niveau vers AD DS de Windows Server 2012. Au rang des meilleures pratiques, il est recommandé de vérifier les compatibilités de matériel et de logiciel avant d'effectuer une mise à niveau. Après la mise à niveau du système d'exploitation, pensez à mettre vos pilotes et autres services à jour (tels que les agents de surveillance), et vérifiez la présence de mises à jour des applications Microsoft et des logiciels autres que Microsoft.

Remarque : La mise à niveau peut être faite directement de Windows Server 2008 ou Windows Server 2008 R2 à Windows Server 2012. Pour mettre à niveau les serveurs qui exécutent une version de Windows Server antérieure à Windows Server 2008, il faut soit effectuer une mise à niveau intermédiaire à Windows Server 2008 ou Windows Server 2008 R2, soit effectuer une installation entièrement nouvelle. Veuillez remarquer que les contrôleurs de domaine de Windows Server 2012 AD DS peuvent coexister comme contrôleurs de domaine dans le même domaine que des contrôleurs de domaine Windows Server 2003 ou d'une version plus récente.

Le processus de nouvelle installation

Pour introduire une nouvelle installation de Windows Server 2012 en tant que membre du domaine :

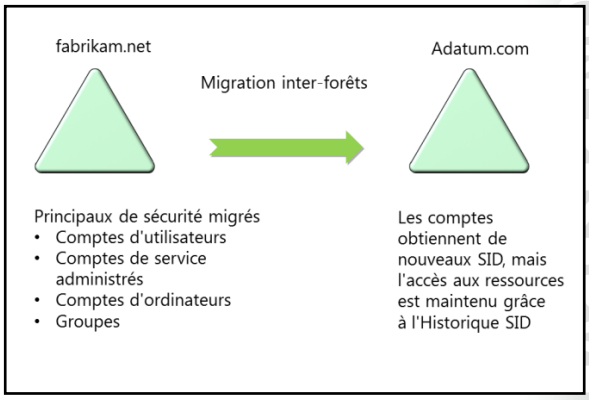
1. Déployez et configurez une nouvelle installation de Windows Server 2012, puis rattachez-le au domaine.
2. À l'aide de Gestionnaire de serveurs, faites du nouveau serveur un contrôleur de domaine dans le domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Faire la migration vers Windows Server 2012 AD DS à partir d'une version antérieure

Dans le cadre du déploiement d'AD DS, il est possible que vous choisissiez de restructurer votre environnement pour les raisons suivantes :

- Pour optimiser la structure logique d'AD DS. Dans certaines organisations, l'entreprise a connu des changements importants depuis le premier déploiement d'AD DS. Le domaine AD DS ou la structure de la forêt ne répond peut-être donc plus aux exigences stratégiques.
- Pour réaliser une fusion, une acquisition, ou un désinvestissement d'affaires.



Une restructuration implique une migration des ressources entre les domaines AD DS soit dans la même forêt soit dans des forêts différentes. Dans AD DS, il n'est pas possible de détacher un domaine d'une forêt pour l'attacher à une autre. Vous pouvez renommer et réorganiser des domaines dans une forêt dans certaines circonstances, mais il n'y a pas de moyen de fusionner facilement des domaines à l'intérieur d'une forêt ou entre différentes forêts. La seule option de restructuration d'un domaine de la sorte est de déplacer tous les comptes et ressources d'un domaine vers l'autre.

Microsoft fournit l'Outil de Migration Active Directory (ADMT) pour déplacer les comptes utilisateur, de groupe et d'ordinateur d'un domaine à l'autre, et pour migrer les ressources du serveur. Si elle est effectuée soigneusement, la migration peut être réalisée sans perturber l'accès utilisateur aux ressources nécessaires à son travail. L'outil de migration ADMT fournit une interface graphique utilisateur et une interface de scripts, et prend en charge les tâches suivantes pour réaliser la migration de domaine :

- Migration de compte d'utilisateur
- Migration de compte de groupe
- Migration de compte d'ordinateur
- Migration de compte de service
- Migration des relations d'approbation
- Migration de répertoire du Serveur Exchange
- Traduction de la sécurité sur des comptes d'ordinateur migrés
- Fonctionnalités de création de rapports pour l'affichage des résultats de la migration
- Fonctionnalité d'annulation de la dernière migration et de nouvel essai de la dernière migration

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Étapes de prémigration

Avant d'effectuer la migration, vous devez effectuer plusieurs tâches de préparation des domaines sources et cibles. Ces tâches sont les suivantes :

- Pour les ordinateurs membres du domaine qui ont une version de Windows antérieure à Windows Vista® Service Pack 1 (SP1) ou Windows Server 2008 R2, configurez un registre sur le contrôleur de domaine cible AD DS pour permettre l'exécution des algorithmes de chiffrement compatibles avec le système d'exploitation Microsoft Windows NT® Server 4.0.
- Activez les règles de pare-feu sur les contrôleurs de domaine AD DS sources et cibles pour rendre possible le partage de fichier et d'imprimante.
- Préparez les domaines AD DS sources et cibles pour gérer la manière dont les utilisateurs, les groupes et les profils utilisateurs sont traités.
- Créez un plan de restauration.
- Établissez les relations d'approbation requises pour la migration.
- Configurez les domaines AD DS sources et cibles pour activer la migration de l'historique SID.
- Spécifiez les comptes de services destinés à la migration.
- Exécutez un test de la migration, et corrigez toutes les erreurs rapportées.

Restructuration inter-forêts avec ADMT

Une restructuration inter-forêts implique le déplacement des ressources à partir des domaines sources appartenant à d'autres forêts que celles du domaine cible. Pour pouvoir utiliser ADMT afin d'effectuer une restructuration inter-forêts, suivez les étapes ci-dessous :

1. Créez un plan de restructuration. Un plan approprié est essentiel au succès du processus de restructuration. Suivez les étapes suivantes pour créer un plan de restructuration :
    a. Déterminez le processus de migration des comptes.
    b. Attribuez des emplacements aux objets et le mappage des emplacements.
    c. Développez un plan de test.
    d. Créez un plan de restauration.
    e. Créez un plan de communication.
2. Préparez les domaines sources et cibles. La préparation des domaines sources et cibles dans le cadre du processus de restructuration se fait en effectuant les tâches suivantes :
    a. Assurez-vous du chiffrement 128 bits pour tous les contrôleurs de domaine.
    Windows Server 2000 Service Pack 3 (SP3) et les versions plus récentes prennent en charge de manière native le chiffrement 128 bits. Si vous disposez de systèmes d'exploitation plus anciens, vous devrez télécharger et installer un pack de chiffrement différent.
    b. Établissez les relations d'approbation requises. Vous devez configurer une relation d'approbation au minimum à sens unique entre les domaines sources et cibles.
    c. Établissez les comptes de migration. ADMT utilise des comptes de migration pour migrer des objets des domaines sources aux domaines cibles. Assurez-vous que ces comptes disposent des autorisations nécessaires pour déplacer et modifier des objets sur les domaines sources et cibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

d. Déterminez si ADMT traite l'historique SID automatiquement, ou si vous allez configurer manuellement les domaines sources et cibles.

e. Assurez-vous que la configuration de la structure de l'unité d'organisation du domaine cible est correcte. Assurez-vous que vous configurez les droits administratifs et l'administration déléguée appropriés dans le domaine cible.

f. Installez ADMT dans le domaine cible.

g. Activez la migration des mots de passe.

h. Exécutez une migration de test avec un petit groupe de comptes de test.

3. Migrez les comptes. Pour effectuer la migration des comptes, procédez comme suit :

   a. Faites la transition des comptes de service.

   b. Migrez les groupes globaux.

   c. Migrez les comptes. Migrez les comptes d'utilisateur et d'ordinateur par lots pour surveiller la progression de la migration. Si vous migrez des profils locaux, migrez d'abord les ordinateurs concernés, puis les comptes d'utilisateurs associés.

4. Migrez les ressources. Migrez les ressources du domaine restantes en procédant comme suit :

   a. Migrez les stations de travail et les serveurs membres.

   b. Migrez les groupes locaux de domaine.

   c. Migrez les contrôleurs de domaine.

5. Finalisez la migration. Finalisez la migration et effectuez le nettoyage en procédant comme suit :

   a. Transférez les processus d'administration au domaine cible.

   b. Assurez-vous qu'il y a au moins deux contrôleurs de domaine fonctionnels dans le domaine cible. Sauvegardez ces contrôleurs de domaine.

   c. Désaffectez le domaine source.

L'attribut d'historique SID

Il est possible qu'au cours de la migration vous ayez déplacé les comptes d'utilisateur et de groupe dans le nouveau domaine mais que les ressources auxquelles les utilisateurs ont besoin d'accéder soient toujours dans l'ancien domaine. Lorsque vous migrez un compte d'utilisateur, AD DS lui attribue un nouveau SID. La ressource du domaine source autorisant les accès sur base du SID de l'utilisateur dans le domaine source, jusqu'à ce que la ressource soit déplacée dans le nouveau domaine, l'utilisateur ne peut pas utiliser le nouveau SID pour y accéder.

Pour remédier à cela, vous pouvez configurer l'ADMT pour migrer le SID du domaine source, puis enregistrez le SID dans un attribut appelé **historique SID**. Quand l'attribut **historique**-**SID** est renseigné, le SID précédent de l'utilisateur est utilisé pour accorder l'accès aux ressources dans le domaine source.

Documentation supplémentaire :

- Vous pouvez télécharger la version 3.2 de l'outil de migration Active Directory sur http://go.microsoft.com/fwlink/?LinkId=270029.
- Vous pouvez télécharger le manuel de l'outil de migration Active Directory sur http://go.microsoft.com/fwlink/?LinkId=270045.

Leçon 3
Configuration d'approbations AD DS

Les relations d'approbation AD DS activent l'accès aux ressources dans un environnement complexe AD DS. Quand vous déployez un domaine unique, vous pouvez facilement accorder l'accès aux utilisateurs et aux groupes du domaine aux ressources du domaine. Quand vous implémentez plusieurs domaines ou forêts, vous devez vérifier que les relations d'approbation appropriées sont en place pour activer le même accès aux ressources. Cette leçon décrit le fonctionnement des relations d'approbation dans un environnement AD DS, ainsi que leur configuration de manière à répondre aux exigences stratégiques de l'organisation.

Objectifs de la leçon

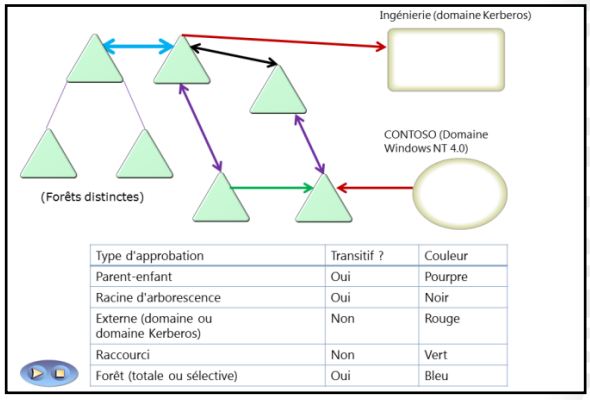
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les possibilités de configuration de relations d'approbation dans un environnement Windows Server 2012.
- Expliquer comment les relations d'approbation fonctionnent dans une forêt AD DS.
- Expliquer comment les relations d'approbation fonctionnent entre plusieurs forêts AD DS.
- Décrire la configuration des paramètres avancés des relations d'approbation.

Expliquer la configuration d'une approbation de forêt.

Vue d'ensemble de différents types de relation d'approbation AD DS

Dans une forêt multi domaines AD DS, des relations bidirectionnelles d'approbation transitive sont générées automatiquement entre les domaines AD DS, de sorte qu'il y ait un chemin d'accès possible à l'approbation entre tous les domaines AD DS. Toutes les approbations créées automatiquement dans la forêt sont transitives. Cela signifie que si le domaine A approuve le domaine B et que le domaine B approuve le domaine C, alors le domaine A approuve le domaine C.



Type d'approbation	Transitif ?	Couleur
Parent-enfant	Oui	Pourpre
Racine d'arborescence	Oui	Noir
Externe (domaine ou domaine Kerberos)	Non	Rouge
Raccourci	Non	Vert
Forêt (totale ou sélective)	Oui	Bleu

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

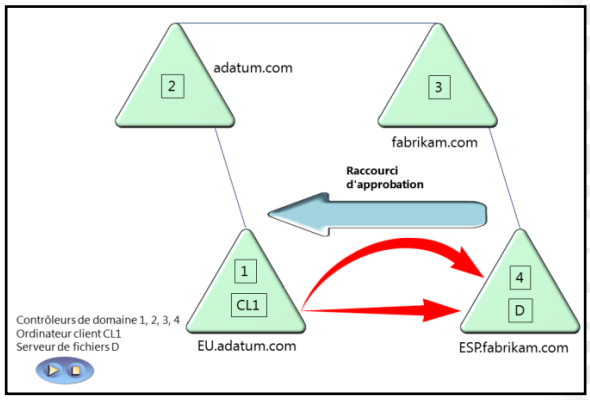
Il est possible de déployer d'autres types de relation d'approbation. Le tableau suivant décrit les principaux types de relation d'approbation.

Type d'approbation	Transitivité	Direction	Description
Parent et enfant	Transitive	Bidirectionnelle	Quand un nouveau domaine AD DS est ajouté à une arborescence AD DS existant, de nouvelles relations d'approbation parents et enfants sont créées.
Racine d'arborescence	Transitive	Bidirectionnelle	Quand une nouvelle arborescence AD DS est créée dans une forêt AD DS existante, une nouvelle relation d'approbation arborescence-racine est créée.
Externe	Non transitive	À sens unique ou bidirectionnelle	Les relations d'approbation externes activent l'accès aux ressources à accorder dans un domaine Windows NT 4.0 ou un domaine AD DS dans une autre forêt. Celles-ci peuvent également être définies pour fournir une infrastructure pour une migration.
Domaine	Transitive ou non transitive	À sens unique ou bidirectionnelle	Les approbations de domaine établissent un chemin d'accès d'authentification entre un domaine de Windows Server AD DS et un domaine de Kerberos V5 implémentés avec un service d'annuaire autre qu'AD DS.
Forêt (totale ou sélective)	Transitive	À sens unique ou bidirectionnelle	Les relations d'approbation entre forêts AD DS permettent à deux forêts de partager leurs ressources.
Raccourci	Non transitive	À sens unique ou bidirectionnelle	Les approbations de raccourci améliorent les délais d'authentification entre domaines AD DS situés dans différentes parties d'une forêt AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment les approbations fonctionnent-elles à l'intérieur d'une forêt ?

Lorsque vous définissez des approbations entre domaines, que ce soit dans la même forêt, entre forêts, ou avec un domaine externe, les informations relatives à ces approbations sont enregistrées dans AD DS. Un objet domaine approuvé (Trusted Domain Object) stocke ces informations.



L'objet domaine approuvé (TDO) stocke des informations relatives à l'approbation, telles que sa transitivité ou son type. À chaque création d'une approbation, un nouvel objet domaine approuvé est créé et stocké dans le conteneur Système d'AD DS.

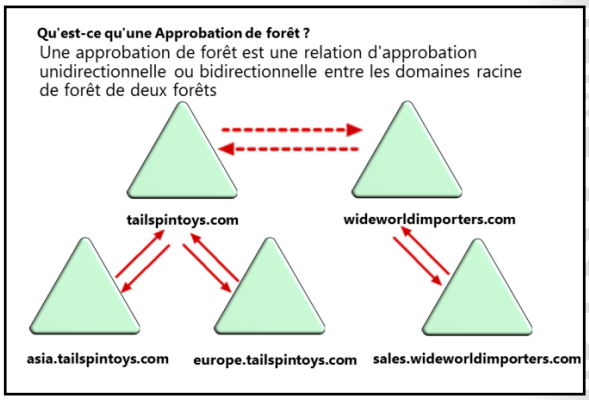
Comment les approbations permettent-elles aux utilisateurs d'accéder aux ressources d'une forêt ?

Lorsqu'un utilisateur du domaine tente d'accéder à une ressource partagée d'un autre domaine de la forêt, son ordinateur contacte d'abord un contrôleur de domaine de son propre domaine pour demander un ticket de session à la ressource. La ressource n'appartenant pas au domaine de l'utilisateur, le contrôleur de domaine doit déterminer si une approbation existe avec le domaine cible. Le contrôleur de domaine peut utiliser l'objet domaine approuvé pour vérifier l'existence de l'approbation. Cependant, pour accéder à la ressource, l'ordinateur client doit communiquer avec un contrôleur de domaine dans chaque domaine tout au long du chemin d'accès d'approbation. Le contrôleur de domaine dans le domaine de l'ordinateur client envoie l'ordinateur client à un contrôleur de domaine dans le domaine suivant le long du chemin d'accès d'approbation. S'il ne s'agit pas du domaine où la ressource se trouve, ce contrôleur de domaine envoie l'ordinateur client à un contrôleur de domaine dans le domaine suivant. Au bout du compte, l'ordinateur client est envoyé à un contrôleur de domaine dans le domaine où la ressource se trouve, et le client reçoit un ticket de session pour accéder à la ressource.

Le chemin d'approbation est le chemin d'accès le plus court dans la hiérarchie d'approbation. Dans une forêt ne comprenant que les approbations par défaut configurées, le chemin d'accès d'approbation remonte l'arborescence de domaine jusqu'au domaine racine de forêt, puis redescend l'arborescence de domaine jusqu'au domaine cible. Si des approbations de raccourci sont configurées, le chemin d'accès d'approbation peut être un tronçon unique du domaine d'ordinateur client au domaine contenant la ressource.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment les approbations entre forêts fonctionnent-elles ?



Si l'environnement AD DS contient plus d'une forêt, il est possible de définir des relations d'approbation entre les domaines racines de forêt AD DS. Ces approbations de forêt peuvent être les approbations à l'échelle de la forêt ou les approbations sélectives. Les approbations de forêt peuvent être uni- ou bidirectionnelles. Les approbations de forêt sont également transitives pour les domaines de chaque forêt.

Des relations d'approbation de forêt permettent aux utilisateurs authentifiés par un domaine d'une forêt d'accéder aux ressources qui sont dans un domaine d'une autre forêt, pour autant qu'ils disposent des droits d'accès. Si l'approbation de forêt est unidirectionnelle, les contrôleurs de domaine dans la forêt d'approbation peuvent fournir des tickets de session aux utilisateurs dans n'importe quel domaine de la forêt approuvée. Il est sensiblement plus facile d'établir, de maintenir, et d'administrer des approbations de forêt que des relations d'approbation distinctes entre chacun des domaines des forêts.

Les approbations de forêt sont particulièrement utiles dans les scénarios qui impliquent une collaboration inter organisations, ou des fusions et acquisitions, ou dans une même organisation qui a plusieurs forêts pour isoler les données et les services Active Directory. Les approbations de forêt sont également utiles pour les fournisseurs de services d'application, pour les extranets collaboratifs, et pour des sociétés recherchant une solution d'autonomie administrative.

Les approbations de forêt présentent les avantages suivants :

- Gestion simplifiée des ressources à travers deux forêts de Windows Server 2008 (ou des versions plus récentes) en réduisant le nombre d'approbations externes nécessaires pour le partage des ressources.
- Relations complètes d'approbation bidirectionnelle avec chaque domaine dans chaque forêt.
- Utilisation de l'authentification du nom de l'utilisateur principal (UPN) entre deux forêts.
- Utilisation du protocole Kerberos V5 pour améliorer la fiabilité des données d'autorisation transférées entre les forêts.
- Flexibilité d'administration. Les tâches d'administration peuvent être spécifiques à chaque forêt.

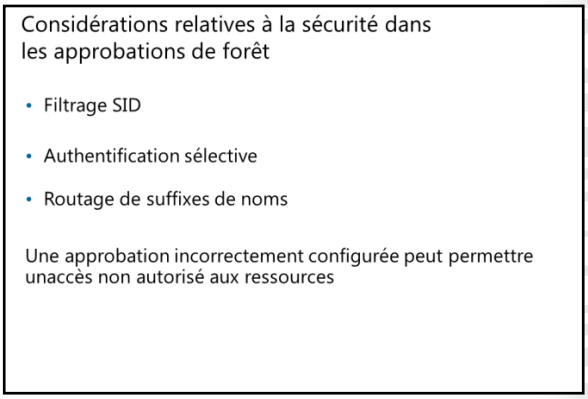
Il n'est possible de créer une approbation de forêt qu'entre deux forêts AD DS (pas plus). Cela signifie que, si vous créez une approbation de forêt entre la forêt 1 et la forêt 2, et que vous créez une approbation de forêt entre la forêt 2 et la forêt 3, la forêt 1 n'a pas une approbation implicite avec la forêt 3. Les relations de forêt ne sont pas transitives entre plusieurs forêts.

Vous devez répondre à plusieurs exigences de configuration avant de pouvoir implémenter une approbation de forêt, parmi lesquelles figurent le niveau fonctionnel de la forêt doit être Windows Server 2003 ou une version plus récente, et la condition que vous disposiez de la résolution de nom DNS entre les forêts.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des paramètres avancés d'approbation AD DS

Dans certains cas, les approbations peuvent comporter des problèmes de sécurité. En outre, si une approbation est mal configurée, les utilisateurs appartenant à un autre domaine peuvent avoir un accès indésirable à certaines ressources. Il existe plusieurs technologies pour vous aider à contrôler et gérer la sécurité d'une approbation.



Filtrage SID

Par défaut, quand vous établissez une approbation de forêt ou de domaine, vous activez une quarantaine de domaine, également appelée filtrage SID. Quand un utilisateur s'authentifie dans un domaine approuvé, il fournit les données d'autorisation dont les SID de tous les groupes auxquels il appartient. En outre, les données d'autorisation de l'utilisateur comprennent les SID d'autres attributs de l'utilisateur et des groupes de l'utilisateur.

AD DS définit le filtrage SID par défaut pour empêcher que les utilisateurs bénéficiant d'un accès au domaine ou au niveau administrateur de l'entreprise dans un domaine ou une forêt approuvés, puissent s'octroyer (ou d'octroyer à d'autres comptes d'utilisateur de leur forêt ou domaine) des droits d'utilisateur élevés à une forêt ou un domaine d'approbation. Le filtrage SID empêche l'abus des attributs contenant les SID sur des entités de sécurité dans la forêt ou le domaine approuvés.

Un exemple classique d'un attribut contenant un SID est l'attribut Historique SID (SIDHistory) sur un objet de compte d'utilisateur. Les administrateurs de domaine utilisent en général l'attribut historique SID pour migrer l'utilisateur et les comptes du groupe qui sont privés de la mobilité d'un domaine à un autre par une entité de sécurité.

Dans un scénario de domaine approuvé, il est possible qu'un administrateur utilise les informations d'identification d'administration dans le domaine approuvé pour charger les SID identiques aux SID des comptes privilégiés dans votre domaine dans l'attribut SIDHistory d'un utilisateur. Cet utilisateur aurait alors des niveaux inadéquats d'accès aux ressources dans votre domaine. Le filtrage SID empêche cela en activant le filtrage par le domaine d'approbation, des SID du domaine approuvé qui ne sont pas les SID principaux des entités de sécurité. Chaque SID comprend le SID du domaine d'origine. Ainsi, quand un utilisateur d'un domaine approuvé présente la liste des SID de l'utilisateur et des SID des groupes d'utilisateurs, le filtrage SID donne la consigne au domaine d'approbation d'ignorer tous les SID sans le SID de domaine du domaine approuvé. Le filtrage SID est activé par défaut pour toutes les approbations sortantes vers des domaines ou forêts externes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Authentification sélective

Quand vous créez une approbation externe ou une approbation de forêt, vous pouvez gérer l'étendue de l'authentification des entités de sécurité approuvées. Il existe deux modes d'authentification pour une approbation externe ou de forêt :

- Authentification pour l'ensemble du domaine (dans le cas d'une approbation externe) ou authentification pour l'ensemble de la forêt (dans le cas d'une approbation de forêt)
- Authentification sélective

Si vous choisissez l'authentification pour l'ensemble du domaine ou de la forêt, cela permet à tous les utilisateurs approuvés de s'authentifier pour des services et avoir des accès sur tous les ordinateurs dans le domaine d'approbation. Par conséquent, l'autorisation d'accéder aux ressources où que ce soit dans le domaine d'approbation peut être donnée aux utilisateurs approuvés. Si vous utilisez ce mode d'authentification, tous les utilisateurs d'un domaine ou d'une forêt approuvés sont considérés comme Utilisateurs authentifiés dans le domaine d'approbation. Donc, si vous choisissez l'authentification pour l'ensemble du domaine ou de la forêt, n'importe quelle ressource ayant des autorisations accordées aux utilisateurs authentifiés est accessible immédiatement par les utilisateurs approuvés de domaine.

Si, cependant, vous choisissez l'authentification sélective, tous les utilisateurs du domaine approuvé sont des identités approuvées. Cependant, ils ne sont autorisés à s'authentifier que pour les services sur les ordinateurs que vous spécifiez. Par exemple, imaginez que vous avez une approbation externe avec le domaine d'une organisation partenaire. Vous souhaitez vérifier que seuls les utilisateurs du groupe marketing de l'organisation partenaire peuvent accéder à des dossiers partagés sur un seul de vos nombreux serveurs de fichiers. Vous pouvez configurer l'authentification sélective pour la relation d'approbation, puis donner aux utilisateurs approuvés le droit de s'authentifier pour ce serveur de fichiers uniquement.

Routage de suffixes de noms

Le routage de suffixes de noms est un mécanisme de gestion du routage des requêtes d'authentification à travers les forêts qui s'exécutent sous Windows Server 2003 ou des forêts plus récentes qui sont liées entre elles par des approbations de forêt. Pour simplifier l'administration des requêtes d'authentification, quand vous créez une approbation de forêt, AD DS distribue tous les suffixes de noms uniques par défaut. Un *suffixe de nom unique* est un suffixe de nom dans une forêt - tel qu'un suffixe UPN, un suffixe SPN, une forêt DNS ou le nom d'une arborescence de domaine, qui n'est subordonné à aucun autre suffixe de nom. Par exemple, le nom de forêt DNS fabrikam.com est un suffixe de nom unique dans la forêt de fabrikam.com.

AD DS distribue tous les noms subordonnés aux suffixes de nom unique implicitement. Par exemple, si la forêt utilise fabrikam.com comme suffixe de nom unique, des demandes d'authentification pour tous les domaines enfants de fabrikam.com (childdomain.fabrikam.com) sont distribuées, parce que les domaines enfants font partie du suffixe de nom de fabrikam.com. Les noms enfants apparaissent dans le composant logiciel enfichable des domaines et approbations Active Directory. Si vous souhaitez exclure des membres d'un domaine enfant de l'authentification dans la forêt spécifiée, vous pouvez désactiver le routage de suffixe de nom pour ce nom. Vous pouvez également désactiver le routage pour le nom de forêt lui-même.

Démonstration : Configurer une approbation de forêt

Dans cette démonstration, vous allez apprendre à :

- configurer la résolution de nom DNS à l'aide d'un redirecteur conditionnel ;
- configurer une approbation de forêt sélective bidirectionnelle.

Procédure de démonstration

Configurez la résolution de nom DNS à l'aide d'un redirecteur conditionnel

- Configurez la résolution de nom DNS entre adatum.com et treyresearch.net en créant un redirecteur conditionnel de sorte que LON-DC1 renvoie à MUN-DC1 en tant que serveur DNS pour le domaine DNS treyresearch.net.

Configurez une approbation de forêt sélective bidirectionnelle

- Sur LON-DC1, dans les domaines et approbations Active Directory, créez une approbation de forêt sélective bidirectionnelle entre adatum.com et treyresearch.net, en fournissant les informations d'identification du compte **Administrateur** du domaine treyresearch.net.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation des déploiements AD DS distribués

Scénario

La société A. Datum Corporation a déployé un domaine unique AD DS dont tous les contrôleurs de domaine sont situés dans son centre de données à Londres. Comme la société a grossi et que des filiales se sont ajoutées (et avec elles un grand nombre d'utilisateurs), il devient de plus en plus évident que l'environnement actuel AD DS ne satisfait pas aux exigences de la société. L'équipe réseau est préoccupée par la densité du trafic sur le réseau liée à AD DS et qui passe par les liaisons WAN, dont le taux d'utilisation devient très élevé.

La société est également devenue de plus en plus intégrée avec des organisations partenaires, dont certaines ont besoin d'accéder aux ressources partagées et aux applications qui se trouvent sur le réseau interne d'A. Datum. Le service de sécurité d'A. Datum souhaite assurer un accès aussi sécurisé que possible pour ces utilisateurs externes.

En tant qu'un des administrateurs réseau expérimentés chez A. Datum, vous êtes responsable de l'implémentation d'une infrastructure AD DS répondant aux besoins de la société. Vous êtes responsable de l'organisation du déploiement de domaine et de forêt AD DS qui fournira des services optimaux aux utilisateurs internes et externes, tout en satisfaisant aux exigences de sécurité d'A. Datum.

Objectifs

- Implémenter des domaines enfants dans AD DS
- Implémenter des approbations de forêt dans AD DS

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-TOR-DC1** **22412B-LON-SVR1** **22412B-MUN-DC1**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
    - Nom d'utilisateur : **ADATUM\Administrateur**
    - Mot de passe : **Pa$$w0rd**

5. Répétez les étapes 2 à 4 pour **22412B-LON-SVR1** et **22412B-TOR-DC1**.
6. Démarrez **22412B-MUN-DC1** et ouvrez une session en tant que **TREYRESEARCH\Administrateur** avec le mot de passe **Pa$$w0rd**.

Exercice 1 : Implémenter des domaines enfants dans AD DS

Scénario

A. Datum a décidé de déployer un nouveau domaine dans la forêt d'adatum.com pour la région nord-américaine. Le premier contrôleur de domaine sera déployé à Toronto, et le nom de domaine sera na.adatum.com. Vous devez configurer et installer le nouveau contrôleur de domaine.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le DNS (Domain Name System) pour la délégation de domaine
2. Installer un contrôleur de domaine dans un domaine enfant
3. Vérifier la configuration d'approbation par défaut

▶ Tâche 1 : Configurer le DNS (Domain Name System) pour la délégation de domaine

- Sur LON-DC1, ouvrez le **Gestionnaire DNS** et configurez un enregistrement de zone déléguée pour **na.adatum.com**. Spécifiez **TOR-DC1** en tant que serveur DNS faisant autorité.

▶ Tâche 2 : Installer un contrôleur de domaine dans un domaine enfant

1. Sur TOR-DC1, utilisez le Gestionnaire de serveurs pour installer AD DS.
2. Quand les binaires AD DS sont installés, utilisez l'Assistant de configuration des services de domaine Active Directory pour installer et configurer TOR-DC1 en tant que contrôleur de domaine AD DS pour un nouveau domaine enfant nommé **na.adatum.com**.
3. Lorsque vous y êtes invité, indiquez **Pa$$w0rd** comme **mot de passe pour le mode Restauration des services d'annuaire (DSRM)**.

▶ Tâche 3 : Vérifier la configuration d'approbation par défaut

1. Ouvrez une session TOR-DC1 en tant que **NA\Administrateur** à l'aide du mot de passe **Pa$$w0rd**.
2. Quand le Gestionnaire de serveurs s'ouvre, cliquez sur **Serveur local**. Vérifiez que le **Pare-feu Windows** indique **Domaine : Actif**. Si ce n'est pas le cas, à côté de **Connexion au réseau local**, cliquez sur **172.16.0.25, IPv6 activé**. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Désactiver**. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Activer**. La connexion au réseau local devrait à présent indiquer **Adatum.com**.
3. À partir du Gestionnaire de serveurs, lancez la console de gestion **Domaines et approbations Active Directory** et vérifiez les relations d'approbation parent-enfant.

 **Remarque :** Si vous recevez un message disant que l'approbation ne peut pas être validée, ou que la vérification de canal sécurisé (SC) a échoué, assurez-vous que vous avez terminé l'étape 2, et attendez au moins 10 à 15 minutes avant de réessayer. Vous pouvez continuer les travaux pratiques et revenir ultérieurement à cette étape.

Résultats : À la fin de cet exercice, vous aurez implémenté des domaines enfants dans AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Implémenter des approbations de forêt

Scénario

A. Datum travaille, en collaboration avec une organisation partenaire nommée Trey Research, sur plusieurs projets prioritaires. Pour simplifier le processus d'activation de l'accès aux ressources des deux organisations, ils ont déployé un WAN dédié à cela entre Londres et Munich, où Trey Research est localisé. Vous devez maintenant implémenter et valider une approbation de forêt entre les deux forêts, et configurer l'approbation pour permettre l'accès uniquement aux serveurs sélectionnés à Londres.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les zones de stub pour la résolution de nom DNS
2. Configurer une approbation de forêt avec authentification sélective
3. Configurer un serveur pour l'authentification sélective.

▶ Tâche 1 : Configurer les zones de stub pour la résolution de nom DNS

1. Ouvrez une session sur **LON-DC1** en tant qu' **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Avec la console de gestion DNS, configurez une zone de stub de DNS pour treyresearch.net.
3. Utilisez **172.16.10.10** en tant que serveur DNS maître.
4. Fermez le Gestionnaire DNS.
5. Ouvrez une session sur **MUN-DC1** en tant que **TREYRESEARCH\Administrateur** à l'aide du mot de passe **Pa$$w0rd**.
6. Avec la console de gestion DNS, configurez une zone de stub de DNS pour adatum.com.
7. Utilisez **172.16.0.10** en tant que serveur DNS maître.
8. Fermez le Gestionnaire DNS.

▶ Tâche 2 : Configurer une approbation de forêt avec authentification sélective

1. Sur LON-DC1, créez une approbation sortante unidirectionnelle entre la forêt AD DS de treyresearch.net et la forêt d'adatum.com. Configurez une approbation pour utiliser une **Authentification sélective**.
2. Sur LON-DC1, confirmez et validez l'approbation de treyresearch.net.
3. Fermez la fenêtre Domaines et approbations Active Directory.

▶ Tâche 3 : Configurer un serveur pour l'authentification sélective.

1. Sur LON-DC1, à partir du Gestionnaire de serveurs, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Sur LON-SVR1, configurez les membres du groupe **TreyResearch.net\it** avec l'autorisation **Autorisé à s'authentifier.** Si vous êtes invité à entrer les informations d'identification, saisissez **TREYRESEARCH\Administrateur** avec le mot de passe **Pa$$w0rd**.

3. Sur LON-SVR1, créez un dossier partagé nommé **Données IT**, et accordez l'accès en **Lecture et écriture** aux membres du groupe **TreyResearch.net\it.** Si vous êtes invité à entrer les informations d'identification, saisissez **TREYRESEARCH\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Déconnectez-vous de MUN-DC1.
5. Connectez-vous à **MUN-DC1** en tant que **TREYRESEARCH\Alice** avec le mot de passe **Pa$$w0rd**, et vérifiez que vous pouvez accéder au dossier partagé sur LON-SVR1.

Résultats : À la fin de cet exercice, vous aurez implémenté des approbations de forêt.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-TOR-DC1**, **22412B-MUN-DC1**, et **22412B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Vous recevez des messages d'erreur comme : Échec de recherche DNS, serveur RPC non disponible, le domaine n'existe pas, le contrôleur de domaine n'a pas été trouvé.	
L'utilisateur ne peut pas être authentifié pour accéder à des ressources sur un autre domaine AD DS ou Kerberos.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5

Implémentation des sites et de la réplication Active Directory Domain Services (AD DS)

Table des matières :

Vue d'ensemble du module **5-1**

Leçon 1 : Vue d'ensemble de la réplication AD DS **5-2**

Leçon 2 : Configuration des sites AD DS **5-12**

Leçon 3 : Configuration et contrôle de la réplication AD DS **5-21**

Atelier pratique : Implémentation des sites et de la réplication AD DS **5-29**

Contrôle des acquis et éléments à retenir **5-34**

Vue d'ensemble du module

Quand vous déployez Active Directory® Domain Services (AD DS), il est important que vous fournissiez une infrastructure d'ouverture de session efficace et un service d'annuaire très disponible. Vous atteindrez ces deux objectifs en mettant en œuvre plusieurs contrôleurs de domaine dans toute infrastructure. Cependant, vous devez vérifier qu'Active Directory DS réplique les informations d'Active Directory entre chaque contrôleur de domaine dans la forêt. Dans ce module, vous apprendrez comment AD DS réplique les informations entre les contrôleurs de domaine dans un site unique et dans plusieurs sites. Vous également apprendrez comment créer de plusieurs sites et surveiller la réplication pour aider à optimiser la réplication des services de domaine Active Directory et le trafic d'authentification.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- Décrire le fonctionnement de la réplication AD DS.
- Configurez les sites d'Active Directory DS pour aider à optimiser l'authentification et la réplication.
- Configurez et surveillez la réplication des services de domaine Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble de la réplication AD DS

Dans une infrastructure AD DS, les contrôleurs de domaine standards répliquent les informations de Active Directory en utilisant un modèle de réplication multiples maîtres. Ceci signifie que si un contrôleur de domaine est modifié, cette modification est répliquée à tous les autres contrôleurs de domaine dans le domaine, et potentiellement à tous les contrôleurs de domaine dans toute la forêt. Cette leçon fournit une vue d'ensemble de la façon dont Active Directory DS réplique les informations entre les contrôleurs de domaine standards et en lecture seule (RODC).

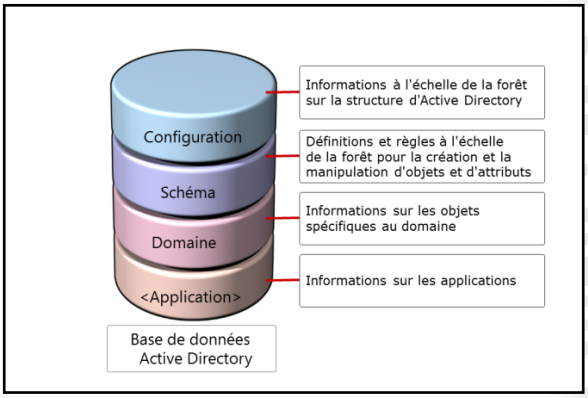
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les partitions AD DS.
- Décrire les caractéristiques de la réplication AD DS.
- Décrire le processus de réplication dans un site unique.
- Décrire comment AD DS résout des conflits de réplication.
- Décrire comment vous générez la topologie de réplication.
- Décrire comment la réplication des contrôleurs de domaine en lecture seule fonctionne.
- Décrire la réplication SYSVOL.

Qu'est-ce que les partitions AD DS ?

Le magasin de données d'Active Directory contient des informations qu'AD DS distribue à tous les contrôleurs de domaine dans toute l'infrastructure de forêt. Une grande partie des informations que le magasin de données contient est distribuée dans un domaine unique. Cependant, certaines informations peuvent être en lien et être répliquées dans toute la forêt indépendamment des limites de domaine.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

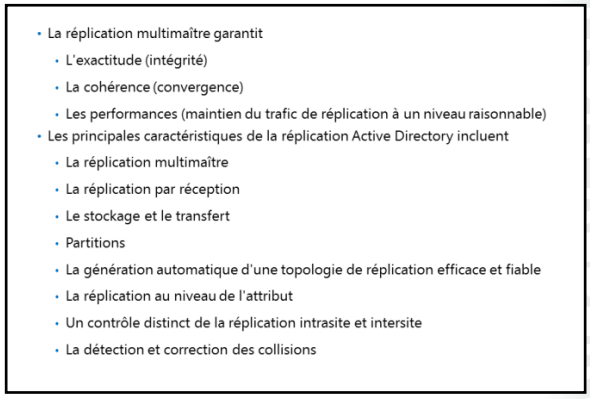
Pour contribuer à garantir l'efficacité et l'extensibilité de la réplication entre les contrôleurs de domaine, les données d'Active Directory sont divisées de façon logique en plusieurs partitions. Chaque partition est une unité de réplication et possède sa propre topologie de réplication. Les partitions par défaut comprennent :

- La partition de configuration. La partition de configuration est créée automatiquement quand vous créez le premier domaine d'une forêt. La partition de la configuration contient des informations sur la structure AD DS dans toute la forêt, notamment quels domaines et quels sites existent et quels contrôleurs de domaine existent dans chaque domaine. La partition de configuration stocke également des informations sur des services dans l'ensemble de la forêt, tels que l'autorisation et les modèles de certificats de protocole DHCP. Cette partition est répliquée sur tous les contrôleurs de domaine de la forêt.
- Partition de schéma. Elle contient les définitions de tous les objets et attributs créés dans la base de données, ainsi que les règles qui permettent de les créer et de les manipuler. Les données du schéma sont répliquées dans tous les contrôleurs de domaine de la forêt. C'est pourquoi tous les objets doivent être conformes à l'objet de schéma et attribuer des règles de définitions d'objet et d'attribut du schéma. AD DS contient un ensemble de classes et d'attributs par défaut que vous ne pouvez pas modifier. Cependant, si vous avez les informations d'identification d'Administrateurs du schéma, vous pouvez étendre le schéma en ajoutant de nouveaux attributs et de nouvelles classes pour représenter les classes spécifiques à l'application. Beaucoup d'applications telles que Microsoft Exchange Server® et Microsoft System Center Configuration Manager peuvent étendre le schéma pour fournir des améliorations spécifiques à l'application de configuration. Ces modifications ont pour cible le contrôleur de domaine qui contient le rôle de l'Administrateur de schéma de la forêt. Seul l'Administrateur de schéma est autorisé à faire des ajouts aux classes et aux attributs.
- Partition de domaine. Quand vous créez un nouveau domaine, AD DS crée et réplique automatiquement une instance de la partition de domaine pour tous les contrôleurs de domaine de tous les domaines. La partition de domaine contient des données sur tous les objets propres au domaine et créés dans ce domaine, dont les utilisateurs, les groupes, les ordinateurs, les unités d'organisation (UO) et les paramètres système liés au domaine. Tous les objets de chaque partition de domaine d'une forêt sont stockés dans le catalogue global, avec un seul sous-ensemble de leurs valeurs d'attribut.
- Partition d'application La partition d'application enregistre les informations qui ne sont pas liées au domaine mais qui sont liées à l'application et qui peuvent avoir une tendance à être mis à jour fréquemment ou ont une durée de vie spécifiée. Une application est en général programmée pour déterminer comment elle stocke, catégorise, et utilise les informations spécifiques à l'application qui sont enregistrées dans la base de données Active Directory. Pour éviter toute réplication inutile d'une partition d'applications, vous pouvez désigner les contrôleurs de domaine dans une forêt qui hébergeront la partition d'applications spécifique. À la différence d'une partition de domaine, une partition d'applications ne peut pas stocker les principaux objets de sécurité, tels que les comptes d'utilisateurs. En outre, le catalogue global n'enregistre pas les données qui sont contenues dans des partitions d'application.

Remarque : Vous pouvez utiliser l'éditeur d'interfaces ADSI (ADSI Edit) pour vous connecter aux partitions et les afficher.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Caractéristiques de réplication de AD DS



Une conception efficace de réplication AD DS garantit que chaque partition sur un contrôleur de domaine est compatible avec les réplicas de cette partition qui sont hébergés sur d'autres contrôleurs de domaine. En général, tous les contrôleurs de domaine n'ont pas exactement les mêmes informations dans leurs réplicas à un moment donné parce que des modifications ont constamment lieu dans la direction. Cependant, la réplication Active Directory permet de garantir que toutes les modifications effectuées sur une partition sont transférées à tous les réplicas de la partition. La réplication Active Directory crée un équilibre entre précision (ou intégrité) et la cohérence appelée *convergence*) avec la performance (en conservant le trafic de réplication à un niveau raisonnable).

Les caractéristiques principales de la réplication Active Directory sont :

- La réplication multi maître. Tout contrôleur de domaine, excepté les RODC, peut initialiser et valider une modification à Active Directory DS. Ceci fournit la tolérance de panne et élimine la dépendance sur un contrôleur de domaine unique pour maintenir les opérations du magasin d'annuaire.
- Réplication par réception. Un contrôleur de domaine demande, ou *extrait*, les modifications d'autres contrôleurs de domaine. Même si un contrôleur de domaine peut informer ses partenaires de réplication qu'il a des modifications pour l'annuaire, ou sonder ses partenaires pour voir s'ils ont des modifications pour le répertoire, le contrôleur de domaine cible demande et extrait lui-même les modifications.
- Réplication de stockage et transfert. Un contrôleur de domaine peut extraire des modifications d'un partenaire, puis apporte ces modifications disponibles à un autre partenaire. Par exemple, le contrôleur de domaine B peut extraire des modifications initialisées par le contrôleur de domaine A. Puis, le contrôleur de domaine C peut extraire les modifications du contrôleur de domaine B. Ceci aide à équilibrer la charge de réplication pour les domaines qui contiennent plusieurs contrôleurs de domaine.
- Partitionnement du magasin de données. Les contrôleurs de domaine d'un domaine hébergent le contexte domaine-appellation pour leurs domaines, ce qui permet de minimiser la réplication, en particulier dans les forêts multi domaines. Les contrôleurs de domaine hébergent aussi les copies des partitions de schéma et de configuration, qui sont répliquées dans toute la forêt. Cependant, les modifications de la configuration et des partitions de schéma sont beaucoup moins fréquents que dans la partition de domaine. Par défaut, d'autres données, notamment les partitions de l'annuaire d'applications et le jeu partiel d'attributs (catalogue global), ne sont pas répliqués à chaque contrôleur de domaine dans la forêt.
- La génération automatique d'une topologie de réplication efficace et fiable. Par défaut, Active Directory DS configure une topologie de réplication efficace et bidirectionnelle de sorte que la perte d'un contrôleur de domaine n'empêche pas la réplication. Active Directory DS met automatiquement cette topologie à jour pendant que des contrôleurs de domaine sont ajoutés, supprimés, ou déplacés entre les sites.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

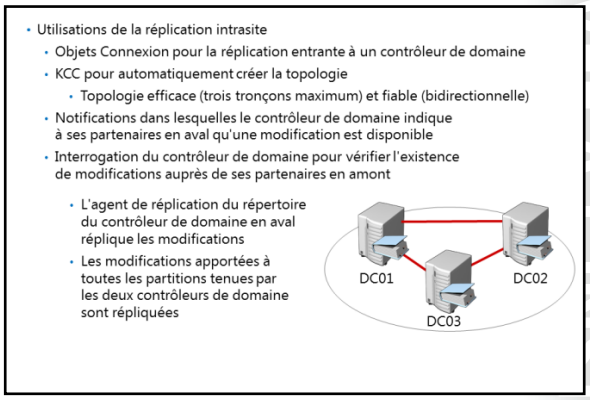
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Réplication au niveau de l'attribut. Quand un attribut d'un objet change, seul cet attribut et des métadonnées minimales décrivant cet attribut sont répliqués. L'objet entier n'est pas répliqué, sauf suite à sa création initiale.
- Un contrôle distinct de la réplication intrasite et de la réplication intersite. Vous pouvez contrôler la réplication dans un site unique *et* entre les sites.
- Détection et gestion de collision. En de rares occasions, vous pouvez modifier un attribut sur deux contrôleurs de domaine différents au cours d'une seule fenêtre de réplication. Si ceci se produit, vous devez réconcilier les deux modifications. Active Directory DS a des algorithmes de résolution qui satisfont presque tous les scénarios.

Fonctionnement de la réplication AD DS dans un site

La réplication AD DS dans un site unique, qui a lieu automatiquement, est appelé *réplication d'intrasite*. Cependant, vous pouvez également la configurer en mode manuel, selon les besoins. Les concepts suivants sont liés à la réplication d'intrasite :

- Objets de connexion
- Vérificateur de cohérence des connaissances
- Notification
- Interrogation



Objets de connexion

Un contrôleur de domaine qui réplique des modifications d'un autre contrôleur de domaine est appelé un partenaire de réplication. Les partenaires de réplication sont liés par des objets de connexion. Un objet de connexion représente un chemin d'accès de réplication d'un contrôleur de domaine à un autre. Les objets de connexion sont unidirectionnels et représentent la réplication par réception entrante uniquement.

Pour afficher et configurer des objets de connexion, ouvrez les sites et les services AD, puis sélectionnez le conteneur de paramètres NTDS d'un objet serveur d'un contrôleur de domaine. Vous pouvez forcer la réplication entre deux contrôleurs de domaine en cliquant avec le bouton droit sur l'objet de connexion, puis en le sélectionnant **Répliquer maintenant**. Notez que la réplication est entrante uniquement, donc si vous souhaitez répliquer les deux contrôleurs de domaine, vous devez répliquer l'objet de connexion entrant de chaque contrôleur de domaine.

Vérificateur de cohérence des connaissances

Les chemins d'accès de réplication qui sont générés entre les contrôleurs de domaine par des objets de connexion créent la topologie de réplication de la forêt. Vous ne devez pas créer la topologie de réplication manuellement. Par défaut, Active Directory DS crée une topologie qui vérifie que la réplication est efficace. La topologie est bidirectionnelle, ce qui signifie que si n'importe quel contrôleur de domaine échoue, la réplication continue de façon ininterrompue. La topologie vérifie également qu'il n'y a pas plus de trois tronçons entre deux contrôleurs de domaine quelconques.

Sur chaque contrôleur de domaine, un composant Active Directory DS, appelé le vérificateur de cohérence des données (KCC), aide automatiquement à générer et à optimiser la réplication entre les contrôleurs de domaine dans un site. Le vérificateur KCC évalue les contrôleurs de domaine dans un site, puis crée des objets Connexion pour établir le bidirectionnel, topologie de trois-tronçon décrite plus tôt.

Si vous ajoutez ou supprimez un contrôleur de domaine, ou si un contrôleur de domaine ne répond pas, le vérificateur KCC réorganise la topologie de façon dynamique, en ajoutant ou en supprimant des objets de connexion pour reconstruire une topologie de réplication efficace. Le vérificateur KCC s'exécute à intervalles spécifiés (par défaut toutes les 15 minutes) et désigne les itinéraires de réplication entre contrôleurs de domaine les plus judicieux disponibles à ce moment-là.

Vous pouvez manuellement créer des objets Connexion pour spécifier les chemins d'accès de réplication qui devraient persister. Cependant, créant un objet de connexion manuellement n'est pas en général requis ou n'est pas recommandé parce que le vérificateur KCC ne vérifie pas ou n'utilise pas l'objet de connexion manuel pour le basculement. Le vérificateur KCC n'enlèvera également pas les objets Connexion manuels, ce qui signifie que vous devez vous souvenir de supprimer les objets Connexion que vous créez manuellement.

Notification

Lors de la modification d'une partition Active Directory sur un contrôleur de domaine, le contrôleur de domaine créée une file d'attente de modifications destinées à être répliquées à ses partenaires. Par défaut, le serveur source attend 15 secondes pour informer son premier partenaire de réplication de la modification. La notification est le processus par lequel un partenaire en amont informe à ses partenaires en aval qu'une modification est disponible. Par défaut, le contrôleur de domaine source attend alors trois secondes entre les notifications aux partenaires supplémentaires. Ces délais, appelé *délai initial de notification* et *délai suivant de notification*, sont conçus pour ralentir le trafic réseau qui peut être provoqué par la réplication intrasite.

En recevant la notification, le partenaire en aval demande les modifications du contrôleur de domaine source, et l'agent de réplication d'annuaire extrait les modifications du contrôleur de domaine source. Par exemple, supposez que le contrôleur de domaine DC01 initialise une modification à Active Directory DS. Quand DC02 reçoit la modification de DC01, il apporte la modification à son annuaire. DC02 met alors la modification en file d'attente pour la répliquer à ses propres partenaires situés en aval.

Ensuite, supposez que DC03 est un partenaire de réplication situé en aval de DC02. Après 15 secondes, DC02 informe DC03 qu'il a une modification. DC03 apporte la modification répliquée à son annuaire, puis informe ses partenaires en aval. La modification a fait deux tronçons, de DC01 à DC02, puis de DC02 à DC03. La topologie de réplication vérifie que pas plus de trois tronçons se produisent avant que tous les contrôleurs de domaine dans le site reçoivent la modification. Avec approximativement 15 secondes par tronçon, la modification est totalement répliquée dans le site en moins d'une minute.

Interrogation

Parfois, un contrôleur de domaine n'apporte aucune modifications à ses réplicas pendant une longue période, en particulier pendant les heures d'absence d'activités. Supposez que c'est le cas avec DC01. Ceci signifie que DC02, son partenaire de réplication en aval, ne recevra pas de notifications de DC01. DC01 pourrait également être hors connexion, ce qui l'empêcherait d'envoyer des notifications à DC02.

Il est important que DC02 sache que son partenaire en amont est en ligne, et qu'il n'a aucune modification. Ceci ce fait par le biais d'un processus appelé interrogation. Au cours de l'interrogation, le partenaire de réplication en aval contacte le partenaire de réplication en amont avec des requêtes pour savoir si une ou plusieurs modifications sont mises en file d'attente pour la réplication. Par défaut, la fréquence d'interrogation pour la réplication intrasite a lieu une fois par heure. Vous pouvez configurer la fréquence d'interrogation dans les propriétés d'un objet de connexion en cliquant sur **Modifier la planification**, bien que nous ne le recommandions pas. Si un partenaire en amont ne répond pas aux requêtes répétées d'interrogation, le partenaire en aval lance le vérificateur KCC pour activer la topologie de réplication. Si le serveur en amont est en effet hors connexion, le vérificateur KCC réorganise la topologie de réplication du site pour adapter la modification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Résolution des conflits de réplication

Puisqu'Active Directory DS prend en charge un modèle de réplication multimaître, des conflits de réplication peuvent se produire. En général, il y a trois types de conflits de réplication qui peuvent se produire dans Active Directory DS :

- Dans les modèles de réplication à multiples maîtres, des conflits de réplication surgissent quand
  - Le même attribut est modifié simultanément sur deux contrôleurs de domaine
  - Un objet est déplacé ou ajouté dans un conteneur supprimé sur un autre contrôleur de domaine
  - Deux objets avec le même nom unique relatif sont ajoutés dans le même conteneur sur deux contrôleurs de domaine différents
- Pour résoudre vos conflits de réplication, AD DS utilise
  - Le numéro de version
  - L'horodateur
  - Le GUID du serveur

- En modifiant simultanément la même valeur d'attribut du même objet sur deux contrôleurs de domaine.
- En ajoutant ou en modifiant le même objet sur un contrôleur de domaine pendant que l'objet conteneur pour l'objet est supprimé sur un autre contrôleur de domaine.
- En ajoutant des objets avec le même nom distinctif relatif dans le même conteneur.

Pour aider à réduire des conflits, tous les contrôleurs de domaine dans l'enregistrement de forêt et répliquent des modifications d'objet au niveau d'attribut plutôt qu'au niveau d'objet. Par conséquent, les modifications à deux attributs différents d'un objet, tels que le mot de passe d'utilisateur et le code postal, ne provoquent pas un conflit même si vous les modifiez en même temps dans différents emplacements.

Quand une mise à jour d'origine est appliquée à un contrôleur de domaine, un tampon est créé et transmis avec la mise à jour pendant qu'il est répliqué à d'autres contrôleurs de domaine. Le tampon contient les composants suivants :

- Numéro de version. Les numéros de version commencent à zéro pour chaque attribut d'objet, et augmente de un à chaque mise à jour. En effectuant une mise à jour d'origine, la version de l'attribut mis à jour est un numéro plus haut que la version de l'attribut qui est remplacé.
- Horodateur. L'horodateur indique la date et heure d'origine de la mise à jour selon l'horloge système du contrôleur de domaine où la modification est apportée.
- Serveur Identificateur unique global (GUID). Le serveur GUID identifie le contrôleur de domaine qui a effectué la mise à jour d'origine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

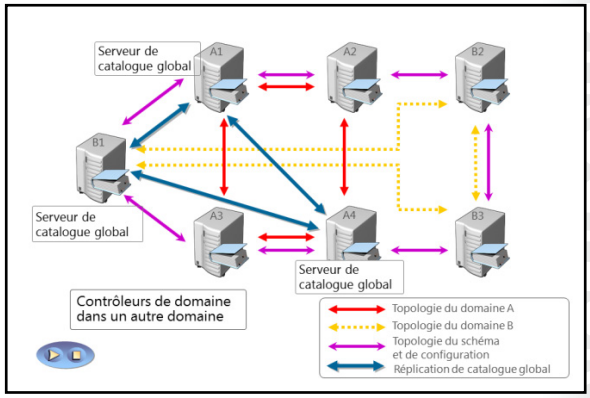
Conflits de réplication communs

Le tableau suivant reprend plusieurs conflits, et décrit comment Active Directory DS résout le problème.

Conflit	Résolution
Valeur d'attribut	Si la valeur du numéro de version est identique, mais la valeur d'attribut diffère, alors l'horodateur est évalué. L'opération de mise à jour qui a la valeur la plus élevée de tampon remplace la valeur d'attribut de l'opération de mise à jour avec la valeur de tampon inférieure.
Ajouter ou déplacer sous un objet conteneur supprimé, ou supprimer un objet conteneur	Après que la résolution se reproduise à tous les réplicas, Active Directory DS supprime l'objet conteneur, et l'objet de feuille devient un enfant du conteneur du dossier spécial LostAndFound. Les tampons ne sont pas impliqués dans cette résolution.
Ajoutez des objets avec le même nom distinctif relatif	L'objet avec le tampon plus grand conserve le nom distinctif relatif. Active Directory DS attribue à l'objet frère un nom distinctif relatif unique par le contrôleur de domaine. L'attribution du nom est le nom distinctif relatif + CNF : + un caractère réservé (l'astérisque) + GUID de l'objet. Cette attribution de nom vérifie que le nom généré n'est en conflit avec aucun autre nom d'objet.

Comment la topologie de réplication est générée

La topologie de réplication est l'itinéraire suivi par les données de la réplication à travers un réseau. Pour créer une topologie de réplication, Active Directory DS doit déterminer quels contrôleurs de domaine répliquent les données avec les autres contrôleurs de domaine. Active Directory DS crée une topologie de réplication selon les informations qu'Active Directory DS contient. Puisque chaque partition d'Active Directory DS peut être répliquée à différents contrôleurs de domaine dans un site, la topologie de réplication peut différer pour le schéma, la configuration, le domaine, et les partitions d'application.



Comme tous les contrôleurs de domaine d'une même forêt partagent les partitions de schéma et de configuration, Active Directory réplique ces partitions de schéma et de configuration sur tous les contrôleurs de domaine. Les contrôleurs de domaine du même domaine répliquent également la partition du domaine. De plus, les contrôleurs de domaine qui hébergent une partition d'applications répliquent également la partition d'applications. Pour optimiser le trafic de la réplication, un contrôleur de domaine peut avoir plusieurs partenaires de réplication pour différentes partitions. Dans un site unique, la topologie de réplication sera à tolérance de panne et redondante. Ceci signifie que si le site contient plus de deux contrôleurs de domaine, chaque contrôleur de domaine aura au moins deux partenaires de réplication pour chaque partition d'Active Directory DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment le schéma et les partitions de configuration sont répliqués

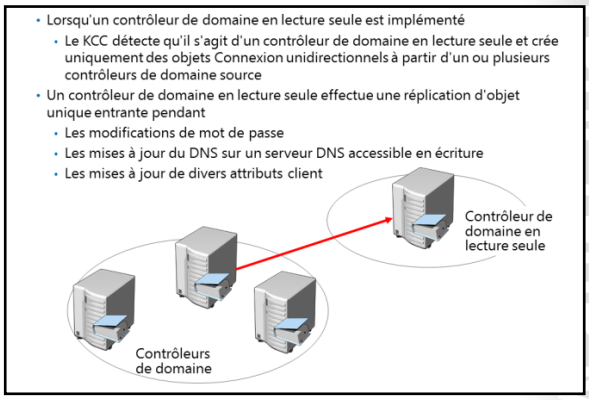
La réplication du schéma et des partitions de configuration suit le même processus que toutes autres partitions d'annuaire. Cependant, parce que ces partitions se font au niveau de l'ensemble de la forêt et non au niveau d'un domaine, les objets de connexion pour ces partitions peuvent exister entre deux contrôleurs de domaine quelconques indépendamment du domaine du contrôleur de domaine. En outre, la topologie de réplication pour ces partitions comprend tous les contrôleurs de domaine dans la forêt.

Comment le catalogue global affecte la réplication

La partition de configuration contient des informations sur la topologie du site et d'autres données globales pour tous les domaines membres de la forêt. Active Directory DS réplique la partition de configuration à tous les contrôleurs de domaine au moyen d'une réplication normale dans l'ensemble de la forêt. Chaque serveur de catalogue global devient un réplica partiel du nouveau domaine en contactant un contrôleur de domaine pour ce domaine et en obtenant les données du réplica partiel. La partition de configuration fournit également aux contrôleurs de domaine la liste de tous les serveurs de catalogue global de la forêt.

Les serveurs de catalogue global inscrivent les enregistrements de service DNS dans la zone DNS qui correspond au domaine racine de forêt. Ces enregistrements, réalisés uniquement dans la zone DNS racine de la forêt, aident les clients et les serveurs à localiser les serveurs de catalogue global à travers la forêt.

Fonctionnement de la réplication RODC



Comme précédemment indiqué, les contrôleurs de domaine répliquent des données en extrayant des modifications d'autres contrôleurs de domaine d'origine. Un contrôleur de domaine en lecture seule (RODC) interdit d'écrire dans sa base de donnée des modifications non-répliquées, et il ne réplique jamais une information à d'autres contrôleurs de domaine. Puisque les modifications ne sont jamais directement enregistrées dans un contrôleur de domaine en lecture seule, d'autres contrôleurs de domaine ne doivent pas extraire des modifications d'annuaire d'un contrôleur de domaine en lecture seule. Empêcher les contrôleurs de domaine en lecture seule de lancer des modifications permet d'éviter la survenance de modification ou d'altération indésirable qu'un utilisateur ou une application malveillants pourraient apporter suite à une réplication au reste de la forêt.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Quand un utilisateur ou une application tentent d'effectuer une requête d'écriture à un contrôleur de domaine en lecture seule, une des actions suivantes se produit en général :

- Le contrôleur de domaine en lecture seule fait suivre la requête d'enregistrement à un contrôleur de domaine accessible en écriture, qui réplique alors de nouveau au contrôleur de domaine en lecture seule. Les exemples de ce type de requête comprennent des modifications de mot de passe, des mises à jour du nom principal du service (SPN), et des modifications des attributs de membre de l'ordinateur et du domaine.
- Le contrôleur de domaine en lecture seule répond au client et fournit une référence à un contrôleur de domaine accessible en écriture. L'application peut alors communiquer directement avec un contrôleur de domaine accessible en écriture. Les mises à jour de Lightweight Directory Access Protocol (LDAP) et des enregistrements DNS sont des exemples de références acceptables de contrôleur de domaine en lecture seule.
- L'opération d'écriture échoue parce qu'elle n'est pas consultée ou n'est pas transférée à un contrôleur de domaine accessible en écriture. Les écritures d'appels de procédure distants (RPC) sont un exemple de communication dont il est interdit de laisser des références ou de transférer à autre contrôleur de domaine.

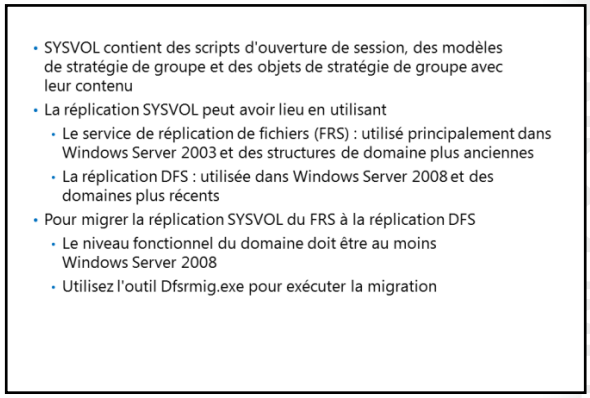
Quand vous mettez en œuvre un contrôleur de domaine en lecture seule, le vérificateur KCC détecte que le contrôleur de domaine est configuré avec un réplica en lecture seule de toutes les partitions applicables de domaine. Pour cette raison, le vérificateur KCC crée uniquement des objets de connexion unidirectionnels depuis une ou plusieurs sources Windows Server® 2008 ou un système d'exploitation plus récent vers le contrôleur de domaine en lecture seule.

Pour quelques tâches précises, un contrôleur de domaine en lecture seule effectue la réplication entrante en utilisant une opération de réplication d'un objet unique (RSO). C'est une demande qui n'entre pas dans la planification standard de réplication. Ces tâches sont les suivantes :

- Modifier le mot de passe.
- Mettre à jour le DNS quand un client est référé à un serveur DNS accessible en écriture par le contrôleur de domaine en lecture seule. Le contrôleur de domaine en lecture seule essaie ensuite d'extraire à nouveau les modifications en utilisant une opération de RSO. Ceci se produit seulement pour les zones DNS intégrées dans l'AD.
- Mises à jour pour différents attributs clients comprenant le nom du client, le DnsHostName, l'OsName, l'OsVersionInfo, les types de chiffrement pris en charge, et l'attribut de LastLogontimeStamp.

Fonctionnement de la réplication SYSVOL

SYSVOL est une collection de fichiers et dossiers sur chaque contrôleur de domaine qui est lié à l'emplacement %SystemRoot%\SYSVOL. SYSVOL contient des scripts d'ouverture de session et des objets mis en relation à la stratégie de groupe telle que des modèles de stratégie de groupe. Le contenu du dossier SYSVOL est répliqué à chaque contrôleur de domaine dans le domaine utilisant la topologie et la planification d'objet de connexion que le vérificateur KCC crée.



Selon la version du système d'exploitation de contrôleur de domaine, le niveau fonctionnel du domaine, et le statut de migration de réplication de (DFS) de SYSVOL, le service de réplication de fichiers (FRS) ou la réplication de système de fichiers distribués (DFS) réplique les modifications de SYSVOL entre les contrôleurs de domaine. Le FRS a été utilisé principalement dans Windows Server 2003 R2 et des structures de domaine plus anciennes. Le service de réplication de fichiers est limité dans sa capacité et ses performances, ce qui a mené à l'adoption de la réplication DFS.

Dans Windows Server 2008 et des domaines plus récents, vous pouvez utiliser la réplication DFS pour répliquer le contenu de SYSVOL. La réplication DFS prend en charge la planification et la limitation de bande passante de réplication, et elle utilise un algorithme de compression appelé la compression différentielle à distance (RDC). Utilisant RDC, Réplication DFS répliques seulement les différences (ou modifications dans des fichiers) entre les deux serveurs, ayant pour résultat l'utilisation de bande passante inférieure pendant la réplication.

 **Remarque :** Vous pouvez utiliser l'outildfsrmig.exepour migrer la réplication SYSVOL du FRS à la réplication DFS. Pour que la migration réussisse, le niveau fonctionnel du domaine doit être au moins Windows Server 2008.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration des sites AD DS

Dans un site unique, le réplication des services de domaine Active Directory se produit automatiquement sans avoir à se soucier de l'utilisation du réseau. Cependant, certains organisations ont plusieurs emplacements qui sont connectés par des connexions de réseau étendu (WAN). Si c'est le cas, vous devez vérifier que le réplication des services de domaine Active Directory n'a pas de conséquence néfaste sur l'utilisation du réseau entre les emplacements. Vous pouvez également avoir besoin de localiser des services réseau à un emplacement spécifique. Par exemple, vous souhaiterez peut-être que des utilisateurs à une filiale s'authentifient à un contrôleur de domaine situé dans leur bureau local, plutôt qu'au-dessus de la connexion WAN à un contrôleur de domaine situé dans le bureau principal. Vous pouvez mettre en place des sites d'Active Directory DS pour aider à gérer la bande passante au-dessus des connexions réseau lentes ou peu fiables, et aider à la localisation de service pour l'authentification et beaucoup d'autres services en lien avec les sites sur le réseau.

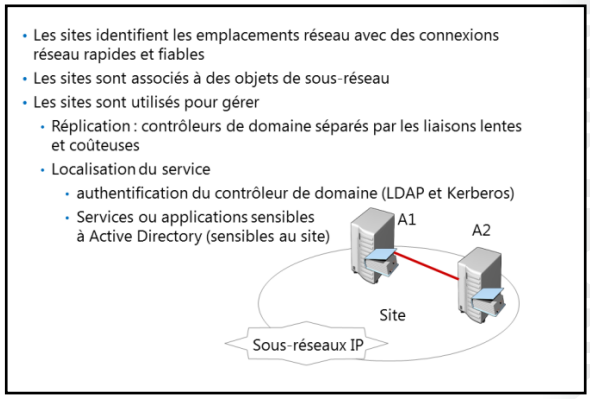
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les sites AD DS.
- Expliquez pourquoi les organisations pourraient mettre en place des sites supplémentaires.
- Configurez des sites supplémentaires d'Active Directory DS.
- Décrire le fonctionnement de la réplication AD DS entre les sites.
- Décrire le générateur de topologie intersite.
- Décrire comment des enregistrements de ressource du service (SRV) sont utilisés pour localiser des contrôleurs de domaine.
- Décrire comment les ordinateurs client localisent des contrôleurs de domaine.

Que sont les sites AD DS ?

Pour la plupart des administrateurs, un site est un emplacement physique, un bureau, ou une ville en général séparée par une connexion WAN. Ces sites sont physiquement connectés par des liens réseau qui pourraient être aussi basiques que des connexions par ligne ou aussi sophistiqués que des liaisons par fibres. Ensemble, les emplacements physiques et les liens composent l'infrastructure réseau physique.



Active Directory DS représente l'infrastructure réseau physique avec des objets appelés *sites*. Les objets de site d'Active Directory DS sont enregistrés dans le conteneur de configuration (CN=Sites, CN=Configuration, DC=and*domaine racine de forêt*) et sont utilisés pour accomplir deux principales tâches de gestion de service :

- Gérer le trafic de réplication. En général, il y a deux types de connexions par réseau local dans l'environnement physique d'une entreprise : Signal de connexion très élevé, et signal moins élevé. Conceptuellement, une modification apportée à Active Directory DS devrait être répliquée immédiatement à d'autres contrôleurs de domaine au sein du réseau à fort signal dans lequel la modification a été apportée. Cependant, il n'est pas toujours souhaitable que la modification soit répliquée à un autre site immédiatement si vous avez un signal plus lent, plus cher et moins fiable. Vous devriez plutôt optimiser les performances, réduire les coûts, et gérer la bande passante en faisant en sorte que la réplication ait lieu sur les segments moins bien connectées de votre entreprise. Un site Active Directory représente une portion avec forte connexion dans votre entreprise. Quand vous définissez un site, les contrôleurs de domaine dans le domaine répliquent les modifications presque instantanément. Cependant, vous pouvez gérer et planifier la réplication entre les sites en fonction des besoins.
- Fournir la localisation de service. Les sites Active Directory vous aident à localiser des services, y compris ceux fournis par des contrôleurs de domaine. Pendant l'ouverture de session, les clients Windows sont dirigés automatiquement vers des contrôleurs de domaine dans leurs sites. Si les contrôleurs de domaine ne sont pas disponibles dans leurs sites, alors ils sont dirigés vers des contrôleurs de domaine dans le site le plus proche susceptible d'authentifier efficacement le client. Beaucoup d'autres services tels que les ressources DFS répliquées sont également en lien avec les sites pour garantir que des utilisateurs sont dirigés vers une copie locale de la ressource.

Qu'est-ce que des objets sous-réseau ?

Les objets sous-réseau identifient les adresses réseau utilisées par mapper les ordinateurs avec les sites AD DS. Un sous-réseau est un segment d'un réseau TCP/IP auquel un jeu d'adresses IP logiques est attribué. Les objets sous-réseau se mappant au réseau physique, les sites font de même. Un site peut comporter un ou plusieurs sous-réseaux. Par exemple, si votre réseau a trois sous-réseaux à New York et deux à London, vous pouvez créer un site à New York et un à London, puis ajoutez les sous-réseaux aux sites respectifs.

 **Remarque :** En concevant votre configuration de site d'Active Directory DS, il est important que vous mappiez correctement des sous-réseaux IP aux sites. De même, si la configuration réseau sous-jacente change, vous devez vérifier que ces modifications sont mises à jour pour refléter le mappage actuel du sous-réseau IP au site. Les contrôleurs de domaine utilisent les informations de sous-réseau IP dans Active Directory DS pour mapper les ordinateurs client et les serveurs au site Active Directory DS correct. Si ce mappage n'est pas exact, les opérations d'Active Directory DS telles que le trafic d'ouverture de session et l'application des stratégies de groupe sont susceptibles de se produire à travers des liaisons WAN, et peuvent être interrompues.

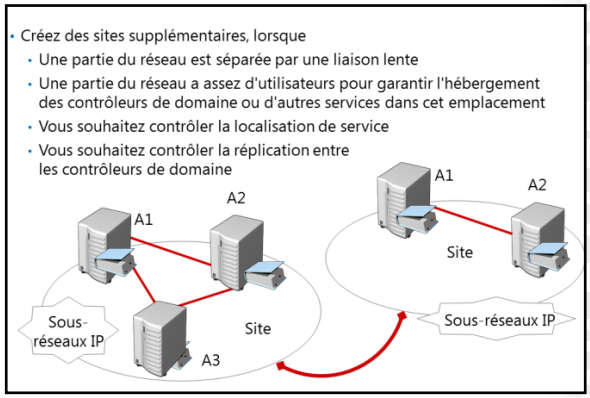
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Premier site par défaut

Lorsque vous installez le premier contrôleur de domaine d'une forêt, Active Directory crée un site par défaut. Par défaut, ce site est appelé *Default-First-Site-Name*. Vous pouvez le renommer de manière plus descriptive. Quand vous installez le premier contrôleur de domaine de la forêt, Active Directory DS le place automatiquement dans le site par défaut. Si vous avez un site unique, il n'est pas nécessaire de configurer des sous-réseaux ou des sites supplémentaires, parce que toutes les machines seront couvertes par le site par défaut Default-First-Site-Name. Cependant, plusieurs sites doivent avoir des sous-réseaux associés à eux en fonction des besoins.

Pourquoi mettre en place des sites supplémentaires ?

Chaque forêt Active Directory comprend au moins un site. Vous devriez créer des sites supplémentaires lorsque:



- Une liaison lente sépare une partie du réseau. Comme précédemment indiqué, un site est caractérisé par un emplacement avec la connectivité rapide, fiable, peu coûteuse. Si deux emplacements sont connectés par une liaison lente, vous devriez configurer chaque emplacement comme un site distinct Active Directory DS. Une liaison lente est en général une liaison qui a une connexion inférieure à 512 kilobits par seconde (Kbits/s).
- Une partie du réseau a assez d'utilisateurs pour garantir l'hébergement des contrôleurs de domaine ou d'autres services dans cet emplacement. Les concentrations d'utilisateurs peuvent également influencer votre création de site. Si un emplacement réseau a un numéro suffisant d'utilisateurs, qu'il serait problématique de ne pas pouvoir s'authentifier, placez un contrôleur de domaine dans l'emplacement pour prendre en charge l'authentification dans l'emplacement. Après avoir placé un contrôleur de domaine ou tout autre service distribué dans un emplacement qui prendra en charge ces utilisateurs, vous pouvez gérer la réplication Active Directory à l'emplacement, ou localiser l'utilisation de service en configurant un site Active Directory pour représenter l'emplacement.
- Vous souhaitez contrôler la localisation de service. En établissant des sites Active Directory DS, vous pouvez vous assurer que les clients utilisent les contrôleurs de domaine qui sont les plus proches d'eux pour l'authentification, ce qui réduit la latence et le trafic d'authentification sur des connexions WAN. Dans la plupart des scénarios, chaque site contiendra un contrôleur de domaine. Cependant, vous pourriez configurer des sites pour localiser des services autres que l'authentification, telle que des services DFS, Windows BranchCache®, et Exchange Server. Dans ce cas, certains sites pourraient être configurés sans la présence d'un contrôleur de domaine dans le site.
- Vous souhaitez contrôler la réplication entre les contrôleurs de domaine. Il peut y avoir des scénarios dans lesquels deux contrôleurs de domaine bien connectés sont autorisés à communiquer seulement à certains moments précis de la journée. Créer des sites vous permet de contrôler comment et quand la réplication a lieu entre les contrôleurs de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration des sites AD DS

Dans cette démonstration, vous allez apprendre à configurer des sites AD DS.

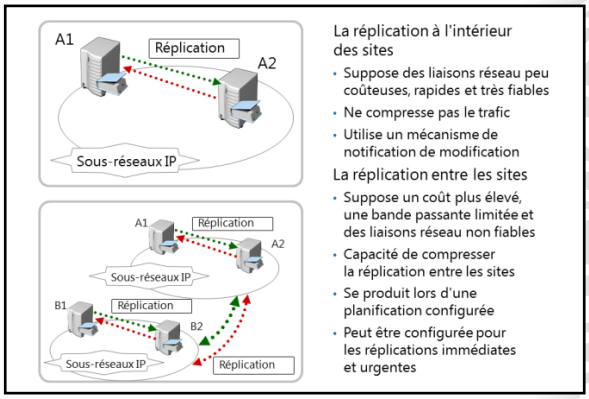
Procédure de démonstration

1. À partir du Gestionnaire de serveur, ouvrez les **sites et services Active Directory**.
2. Renommez le **Default-First-Site-Name LondonHQ** si nécessaire.
3. Cliquez avec le bouton droit sur le nœud **Sites**, puis cliquez sur **Nouveau site**. Spécifiez le nom **Toronto**, puis associez le nouveau site avec le lien du site par défaut.
4. Créez les sites supplémentaires, selon les besoins.
5. Dans le volet de navigation, cliquez avec le bouton droit de **Subnets**, puis cliquez sur **Nouveau sous-réseau**.
6. Fournissez le préfixe **172.16.0.0/24**, puis associez le préfixe IP à un objet du site disponible.
7. Si besoin, déplacez un contrôleur de domaine vers un nouveau site.

Comment fonctionne la réplication entre les sites

Les principales caractéristiques de la réplication à l'intérieur des sites sont les suivantes:

- Les connexions réseau d'un site sont fiables, peu chères et ont suffisamment de bande passante disponible.
- Le trafic de réplications à l'intérieur d'un site n'est pas compressé, car un site suppose la présence de connexions réseau rapides et très fiables. Le fait de ne pas compresser le trafic de réplications réduit la charge de traitement des contrôleurs de domaine. Cependant, le trafic non compressé peut augmenter la bande passante réseau.



- Un processus de notification de modification lance la réplication à l'intérieur d'un site.

Les principales caractéristiques de la réplication entre des sites sont les suivantes:

- La bande passante réservée aux liaisons réseau entre les sites est limitée, peut être plus chère, et risque de ne pas être fiable.
- Le trafic de réplications entre les sites peut être conçu pour optimiser la bande passante en compressant tout le trafic de réplications entre les sites. Avant d'être transmis, ce trafic est compressé de 10 à 15 pour cent par rapport à sa taille d'origine. Bien que la compression optimise la bande passante du réseau, elle entraîne une charge de traitement supplémentaire des contrôleurs de domaine — lors de la compression et de la décompression des données de la réplication.
- La réplication entre les sites se produit automatiquement dès que vous avez défini les valeurs configurables, telles que la planification et l'intervalle de réplication. Vous pouvez planifier la réplication aux heures creuses ou économiques. Par défaut, les modifications sont répliquées entre les sites selon une planification que vous définissez manuellement — et non pas en fonction du moment auquel se produisent les modifications. La planification détermine le moment de la réplication. L'intervalle spécifie la manière dont les contrôleurs de domaine vont vérifier la présence de modifications pendant la période de réplication planifiée.

Notifications de modification entre les sites Active Directory DS

Par conception, les modifications dans Active Directory DS sont répliqués entre les contrôleurs de domaine dans différents sites selon une planification définie par l'utilisateur de réplication, et non en fonction du moment où les modifications ont lieu, comme dans le cas de la réplication intrasite. Pour cette raison, la latence de réplication dans la forêt peut être égale à la somme des plus grandes latences de réplication ayant pris le plus long chemin d'accès de réplication depuis n'importe quelle partition d'annuaire. Dans certains cas, cela peut être inefficace.

Pour éviter la latence dans la réplication, vous pouvez configurer des notifications de modification sur des connexions entre les sites. En modifiant l'objet de lien de sites, vous pouvez activer la notification de modification entre les sites pour toutes les connexions qui se produisent sur ce lien. Puisque le partenaire de réplication dans tout le site est informé des modifications, l'intervalle de réplication intersite est efficacement ignoré. Le contrôleur de domaine d'origine informe le contrôleur de domaine de l'autre site qu'il a une modification, comme il le fait dans un site unique.

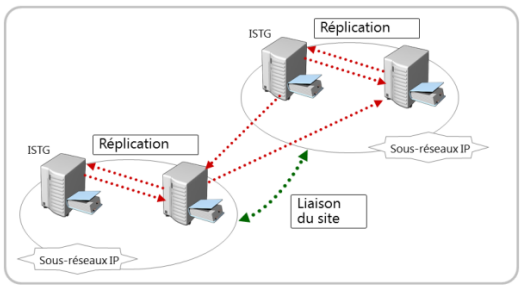
Pour des modifications telles que des verrouillages de compte ou des modifications similaires relatives à la sécurité, il est essentiel que la réplication soit immédiate. Dans ces cas de figure, la réplication urgente est utilisée. La réplication urgente ignore le délai de notification et traite les notifications de modification immédiatement. Ceci affecte uniquement les notifications de modification. Si vous n'avez pas de notifications de modification activées entre les sites, la réplication respecte toujours l'intervalle de réplication sur le lien du site.

 **Remarque :** Quand le mot de passe d'utilisateur est modifié, la réplication immédiate est initialisée vers le maître d'opérations émulation du contrôleur de domaine principal. Ceci diffère de la réplication urgente parce qu'il se produit immédiatement sans se soucier de l'intervalle de réplication intersite.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Définition du générateur de topologie intersite

Le générateur de topologie intersite (ISTG) définit la réplication entre les sites AD DS d'un réseau



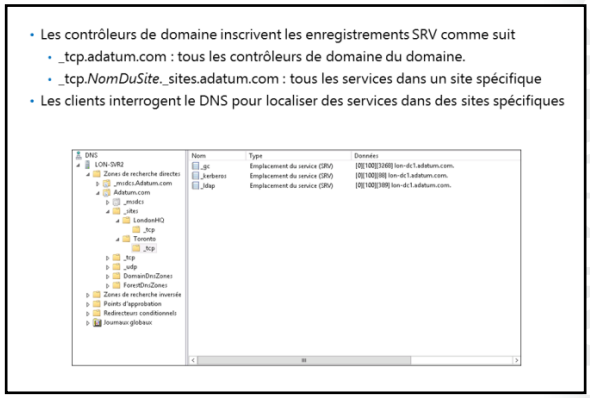
Quand vous configurez plusieurs sites, le vérificateur KCC sur un contrôleur de domaine dans chaque site est indiqué comme générateur de topologie intersite du site (ISTG). Il y a seulement un ISTG par site, indépendamment du nombre de domaines ou autres partitions d'annuaire que le site détient. ISTG est chargé de calculer la topologie de réplication idéale du site.

Quand vous ajoutez un nouveau site à la forêt, l'ISTG de chaque site détermine quelles partitions d'annuaire sont présentes dans le nouveau site. L'ISTG calcule alors combien de nouveaux objets de connexion sont nécessaires pour répliquer l'information requise du nouveau site. Dans certains réseaux vous pouvez spécifier que seuls certains contrôleurs de domaine sont responsables de la réplication intersite. Vous pouvez le faire en spécifiant des serveurs tête de pont. Les serveurs tête de pont sont responsables de toute la réplication dans le site et en dehors. ISTG crée l'accord requis de connexion dans son répertoire, et ces informations sont alors répliquées au serveur tête de pont. Le serveur tête de pont crée alors une connexion de réplication avec le serveur tête de pont dans le site distant, et la réplication commence. Si un partenaire de réplication devient non disponible, l'ITSG sélectionne un autre contrôleur de domaine automatiquement, dans la mesure du possible. Si des serveurs tête de pont ont été attribués manuellement, et s'ils deviennent non disponibles, ISTG ne sélectionnera pas automatiquement d'autres serveurs.

L'ISTG sélectionne des serveurs tête de pont automatiquement, et crée la topologie de réplication intersite pour vérifier que les modifications sont répliquées efficacement entre les serveurs qui partagent un lien de sites. Des serveurs tête de pont sont sélectionnés par partition. Par conséquent, il est possible qu'un contrôleur de domaine dans un site puisse être le serveur tête de pont pour le schéma, tandis qu'un autre sert pour la configuration. Cependant, vous constaterez en général qu'un contrôleur de domaine est le serveur tête de pont pour toutes les partitions dans un site, à moins qu'il y ait des contrôleurs de domaine d'autres domaines ou d'autres partitions de l'annuaire d'applications. Dans ce cas, des serveurs tête de pont seront choisis pour ces partitions.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des enregistrements de ressource SRV pour des contrôleurs de domaine



Quand vous ajoutez un contrôleur de domaine à un domaine, le contrôleur de domaine informe de l'existence de ses services en créant des enregistrements de ressource du service (SRV) (également appelé *enregistrements de localisateur*) dans le DNS. À la différence des enregistrements de ressource de l'hôte (A), qui mappent des noms d'hôte aux adresses IP, la carte d'enregistrements SRV enregistre les services de mappage associés aux noms d'hôte. Par exemple, pour informer de sa capacité à fournir l'authentification et l'accès au répertoire, un contrôleur de domaine enregistre le protocole Kerberos v5 et les enregistrements LDAP SRV. Ces enregistrements SRV sont ajoutés à plusieurs dossiers dans les zones DNS de la forêt.

Dans la zone de domaine, un dossier appelé *nom*_tcp contient les enregistrements SRV pour tous les contrôleurs de domaine dans le domaine. En outre, dans la zone de domaine se trouve un dossier appelé *nom*des _sites, qui contient des sous-dossiers pour chaque site configuré dans le domaine. Chaque dossier spécifique à un site contient les enregistrements SRV qui représentent des services disponibles dans le site. Par exemple, si un contrôleur de domaine est situé dans un site, un enregistrement SRV sera situé dans sous le chemin d'accès _sites\sitename_tcp, où *sitename* est le nom du site.

Un enregistrement SRV typique contient les informations suivantes:

- Le nom du service et le port. Cette partie de l'enregistrement SRV indique un service avec un port fixe. Ce ne doit pas être un port connu. Les enregistrements SRV dans Windows Server 2012 comprennent LDAP (port 389), Kerberos (port 88) et le protocole de mot de passe de Kerberos (KPASSWD, port 464), ainsi que les services de catalogue global (port 3268).
- Protocole. Le protocole TCP ou protocole UDP est indiqué en tant que un protocole de transport pour le service. Le même service peut utiliser les deux protocoles dans des enregistrements SRV distincts. Des enregistrements Kerberos, par exemple, sont enregistrés pour TCP et pour UDP. Les clients de Microsoft utilisent seulement le TCP, mais les clients d'UNIX peuvent utiliser à la fois UDP et TCP.
- Nom de l'hôte. Le nom de l'hôte correspond à l'enregistrement de l'hôte A pour le serveur hébergeant le service. Quand un client envoie une requête pour un service, le serveur DNS renvoie l'enregistrement SRV et les enregistrements associés de l'hôte A, ainsi le client n'a pas besoin d'envoyer une requête distincte pour résoudre l'adresse IP d'un service.

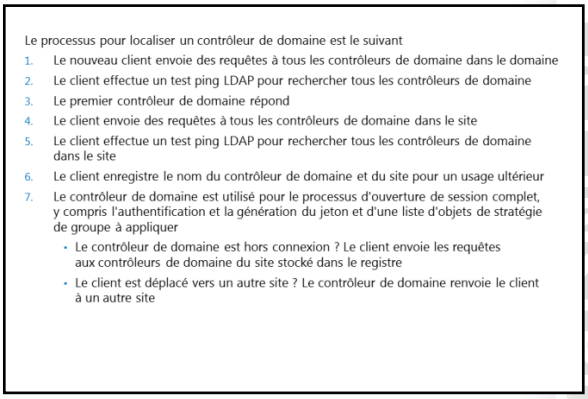
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le nom du service dans un enregistrement SRV suit la hiérarchie DNS standard avec des composants séparés par des points. Par exemple, le service Kerberos d'un contrôleur de domaine est enregistré sous la forme : kerberos._tcp.*sitename*._sites.*domainn*om, où :

- *domainName* est le domaine ou la zone, par exemple contoso.com.
- _sites correspond à tous les sites inscrits avec DNS.
- *nom de site* est le site du contrôleur de domaineenregistrant le service.
- _tcp correspond à tous les services basés sur TCP dans le site.
- kerberos est un centre de distribution de clés (KDC) de Kerberos qui utilise le TCP en tant que protocole de transport propre.

Comment les ordinateurs client localisent des contrôleurs de domaine dans les sites

Quand vous joignez un système d'exploitation Windows client à un domaine, puis que vous le redémarrez, le client complète un emplacement de contrôleur de domaine et le processus d'enregistrement. L'objectif de ce processus d'enregistrement est de localiser le contrôleur de domaine avec l'emplacement le plus efficace et le plus proche de l'emplacement du client selon les informations du sous-réseau IP.



Le processus pour localiser un contrôleur de domaine est le suivant :

1. Le nouveau client envoie des requêtes à tous les contrôleurs de domaine dans le domaine. Comme le nouveau domaine client redémarre, il reçoit une adresse IP d'un serveur DHCP, et est prêt à s'authentifier au domaine. Cependant, le client ne sait pas où rechercher un contrôleur de domaine. Par conséquent, le client envoie une requête à un contrôleur de domaine en demandant le dossier _tcp, qui contient les enregistrements SRV pour tous les contrôleurs de domaine dans le domaine.
2. Le client tente un ping LDAP à tous les contrôleurs de domaine dans une séquence. Le DNS renvoie une liste de tous les contrôleurs de domaine correspondants, et le client essaie d'entrer en contact avec tous dès son premier démarrage.
3. Le premier contrôleur de domaine répond. Le premier contrôleur de domaine qui répond au client examine l'adresse IP du client, les renvois liés à des objets de sous-réseau, et informe le client du site auquel le client appartient. Le client enregistre le nom de site dans son Registre, puis envoie une requête pour des contrôleurs de domaine dans le dossier _tcp spécifique au site.
4. Le nouveau client envoie des requêtes à tous les contrôleurs de domaine dans le site. Le DNS renvoie une liste de tous les contrôleurs de domaine dans le site.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Le client tente un ping LDAP de façon séquentielle à tous les contrôleurs de domaine dans le site. Le contrôleur de domaine qui répond d'abord authentifie le client.
6. Le client forme une affinité. Le client forme une affinité avec le contrôleur de domaine qui a répondu d'abord, puis, à l'avenir, tente de s'authentifier avec le même contrôleur de domaine. Si le contrôleur de domaine est non disponible, le client interroge de nouveau le dossier _tcp du site, et puis retente de se lier avec le premier contrôleur de domaine qui répond dans le site.

Si le client se déplace dans un autre site, comme avec un ordinateur portable, le client tente de s'authentifier à son contrôleur de domaine favoris. Le contrôleur de domaine remarque que l'adresse IP du client est associée à un site différent, puis renvoie le client au nouveau site. Le nouveau client envoie ensuite des requêtes DNS pour les contrôleurs de domaine dans le site local.

Couverture automatique de site

Comme indiqué précédemment, vous pouvez configurer des sites pour diriger des utilisateurs vers les copies locales des ressources répliquées, telles que des dossiers partagés répliqués dans un espace de noms DFS. Dans certains cas, vous aurez besoin uniquement de la localisation de service et vous n'aurez pas besoin qu'un contrôleur de domaine soit situé dans le site. Dans ce cas, un contrôleur de domaine voisin inscrira ses enregistrements SRV dans le site à l'aide d'un processus appelé couverture de site.

Un site sans contrôleur de domaine est en général couvert par un contrôleur de domaine dans un site qui a les liaisons sites les moins coûteuses avec le site qui requiert la couverture. Vous pouvez également configurer la couverture de site et la priorité d'enregistrement SRV manuellement si vous souhaitez contrôler l'authentification dans les sites sans contrôleurs de domaine.

Documentation supplémentaire : Pour plus d'informations sur la façon dont la couverture de site est évaluée, consultez http://go.microsoft.com/fwlink/?LinkId=168550.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration et contrôle de la réplication AD DS

Après avoir configuré les sites qui représentent votre infrastructure réseau, l'étape suivante est de déterminer si des liens de sites supplémentaires sont nécessaires pour aider à gérer le réplication AD DS. Active Directory DS fournit plusieurs options que vous pouvez configurer pour contrôler comment la réplication se produit sur des liens de sites. Vous devez également comprendre les outils que vous pouvez utiliser pour surveiller et gérer la réplication dans un environnement réseau d'Active Directory DS.

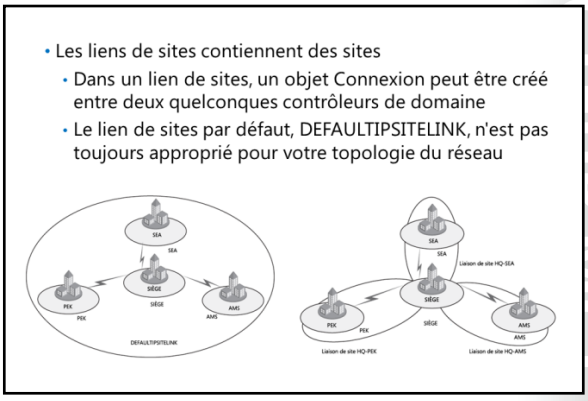
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les liens de site AD DS.
- Expliquer le concept de la transition de lien de sites.
- Décrire la mise en cache de l'appartenance au groupe universel.
- Décrire comment contrôler la réplication intersite.
- Configurer la réplication intersite Active Directory DS.
- Décrire les options pour configurer des stratégies de réplication de mot de passe pour des contrôleurs de domaine en lecture seule.
- Configurer les stratégies de réplication du mot de passe.
- Décrire les outils utilisés pour surveiller et gérer la réplication.

Qu'est-ce que les liens de sites AD DS ?

Pour que deux sites échangent des données de réplication, un lien de sites doit les connecter. Un lien de sites est un chemin d'accès logique que le KCC\ISTG utilise pour établir la réplication entre les sites. Quand vous créez des sites supplémentaires, vous devez sélectionner au moins un lien de sites qui connectera le nouveau site à un site existant. Sauf dans le cas où un lien de sites est en place, la vérification KCC ne peut pas faire des connexions entre les ordinateurs de différents sites, et la réplication entre sites ne peut pas avoir lieu non plus.



La chose importante à se souvenir au sujet d'un lien de sites est qu'il représente un chemin d'accès disponible pour la réplication. Un lien de sites unique ne contrôle pas les itinéraires réseau qui sont utilisées. Quand vous créez un lien de sites et que vous lui ajoutez des sites, vous indiquez à Active Directory DS qu'il peut répliquer entre l'un quelconque sites associés avec le lien de sites. L'ISTG crée des objets de connexion, et ces objets détermineront le chemin d'accès réel de réplication. Bien que la topologie de réplication que l'ISTG établit réplique efficacement Active Directory DS, elle pourrait ne pas être efficace à cause de votre topologie de réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour mieux comprendre ce concept, prenez l'exemple suivant. Quand vous créez une forêt, un objet de lien de sites est créé : DEFAULTIPSITELINK. Par défaut, chaque nouveau site que vous ajoutez est associé avec le DEFAULTIPSITELINK. Imaginez une organisation avec un centre de données au siège et trois filiales. Chacune des trois filiales est connectée au centre de données avec une liaison spécialisée. Vous créez des sites pour chaque filiale : Seattle (MER), Amsterdam (AMS), et Pékin (PEK). Chacun des sites, y compris le siège, est associé avec l'objet de lien de sites de DEFAULTIPSITELINK.

Puisque chacun des quatre sites se trouve sur le même lien de sites, vous indiquez à Active Directory DS que chacun des quatre sites peut se répliquer les uns avec les autres. Cela signifie qui Seattle peut répliquer des modifications d'Amsterdam ; Amsterdam peut répliquer des modifications de Pékin ; et Pékin peut répliquer des modifications du siège, qui à son tour réplique les modifications de Seattle. Dans plusieurs de ces chemins de réplication, le trafic de réplication sur le réseau se déplace d'un branchement qui passe par le siège et qui rejoint un autre branchement. Avec un lien de sites unique, vous ne créez pas une topologie de réplication en étoile même lorsque votre topologie du réseau est en étoile.

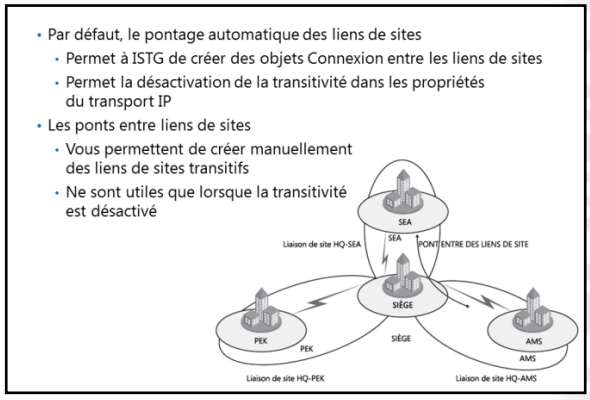
Pour aligner votre topologie du réseau avec la réplication Active Directory, vous devez créer les liens de sites spécifiques. C'est-à-dire que vous pouvez manuellement créer les liens de sites qui reflètent votre topologie de réplication désirée. Pour continuer avec l'exemple précédent, vous créeriez trois liens de sites comme suit :

- HQ-AMS comprend le site du siège et le site d'Amsterdam.
- HQ-SEA comprend le site du siège et le site de Seattle.
- HQ-PEK comprend le site du siège et le site de Pékin.

Après que vous créiez des liens de sites, l'ISTG utilisera la topologie pour établir une topologie de réplication intersite qui connecte chaque site, puis crée des objets de connexion automatiquement pour configurer les chemins d'accès de réplication. Il est recommandé d'installer votre topologie du site correctement et d'éviter de créer des objets de connexion manuellement.

Qu'est-ce que le pont de lien de sites ?

Une fois les liens de sites créés et que l'ISTG génère des objets de connexion aux partitions répliquées entre les contrôleurs de domaine qui partagent un lien de sites, votre travail pourrait bien être terminé. Dans beaucoup d'environnements, en particulier ceux avec des topologies du réseau simples, les liens de sites pourraient être suffisants pour gérer la réplication intersite. Dans des réseaux plus complexes, cependant, vous pouvez configurer des composants additionnels et des propriétés de réplication.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le pont de lien de sites automatique

Par défaut, tous les liens de sites sont reliés par des ponts. Par exemple, si les sites d'Amsterdam et du siège sont liés, et les sites du siège et de Seattle sont liés, alors Amsterdam et Seattle sont reliés à un coût plus élevé. Cela signifie, théoriquement, que l'ISTG pourrait créer un objet de connexion directement entre un contrôleur de domaine à Seattle et un contrôleur de domaine à Amsterdam, si un contrôleur de domaine était non disponible au siège pour la réplication. Ceci est accompli en travaillant autour de la topologie du réseau en étoile.

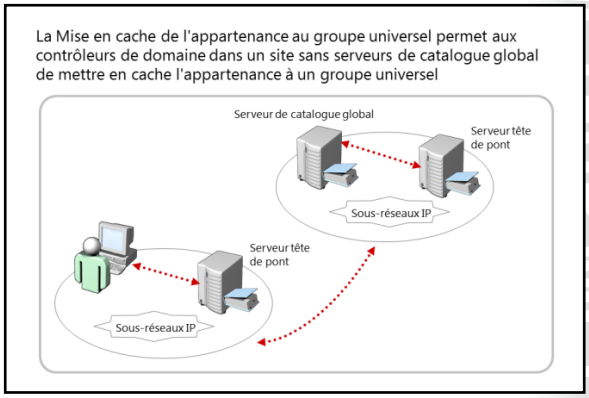
Vous pouvez désactiver le pont automatique reliant les liens de sites en ouvrant les propriétés du transport IP dans le conteneur de transports intersite, puis en désactivant la case à cocher **Relier tous les liens de sites**. Avant d'effectuer cette action dans un environnement de production, lisez les ressources techniques au sujet de la réplication dans les bibliothèques techniques de Windows Server sur le site Web de Microsoft TechNet.

Ponts entre des liens de site

Un pont entre les liens de sites connecte deux liens de sites ou plus en créant un lien transitif. Les ponts entre lien de sites sont nécessaires seulement quand vous avez désactivé la case à cocher **Relier tous les liens de sites** pour le protocole de transport. Souvenez-vous que la transition automatique de lien de sites est activée par défaut, dans ce cas les ponts entre lien de sites ne sont pas requis.

L'illustration sur la diapositive montre l'utilisation d'un pont lien de sites dans une forêt dans laquelle la transition automatique de lien de sites a été désactivée. En créant le pont entre lien de sites AMS-HQ-SEA, qui comprend les liens de sites de HQ-AMS et de HQ-SEA, ces deux liens de sites deviennent transitifs. Par conséquent une connexion de réplication peut être établie entre un contrôleur de domaine à Amsterdam et un contrôleur de domaine à Seattle.

Définition de la mise en cache de l'appartenance au groupe universel



Un des problèmes pouvant être soulevés lorsque l'on configure la réplication AD DS, consiste à savoir s'il faut déployer des serveurs de catalogue global dans chaque site. Puisque des serveurs de catalogue global sont requis quand les utilisateurs se connectent au domaine, déployer un serveur de catalogue global dans chaque site optimise l'expérience de l'utilisateur. Cependant, le déploiement d'un serveur de catalogue global dans un site pourrait avoir pour conséquence un trafic de réplication supplémentaire, ce qui peut être un problème si la connexion réseau entre les sites Active Directory DS a une bande passante limitée. Dans de tels cas de figure, vous pouvez déployer des contrôleurs de domaine exécutant Windows Server 2008 ou plus récent, puis activer la mise en cache de l'appartenance au groupe universel pour le site.

Comment fonctionne la mise en cache de l'appartenance au groupe universel

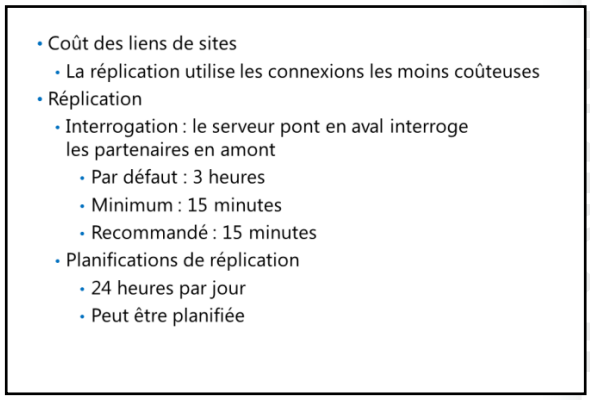
Un contrôleur de domaine dans un site qui a permis la mise en cache de l'appartenance au groupe universel stocke localement les informations du système dès la toute première tentative d'un utilisateur d'ouvrir une session. Le contrôleur de domaine récupère les informations de l'appartenance au groupe universel de l'utilisateur à partir d'un serveur de catalogues global dans un autre site. Il met ensuite ces informations de manière permanente en mémoire cache et les actualise régulièrement. Lors de la prochaine tentative d'ouverture de session de l'utilisateur, le contrôleur de domaine récupère les informations de l'appartenance au groupe universel à partir de sa mémoire cache locale sans contacter un serveur de catalogues global.

Par défaut, les informations de l'appartenance au groupe universel contenues dans la mémoire cache de chaque contrôleur de domaine sont actualisées toutes les huit heures. Pour actualiser le cache, les contrôleurs de domaine envoient une requête de confirmation d'appartenance au groupe universel à un serveur catalogue global désigné.

Vous pouvez configurer la mise en cache de l'appartenance au groupe universel à partir des propriétés du nœud de paramètres du site NTDS.

Gestion de la réplication intersite

Quand vous créez un lien de sites, vous avez un certain nombre d'options de configuration que vous pouvez utiliser pour mieux gérer la réplication intersite. Ces options sont les suivantes :



- Coût des liens de sites. Les coûts des liaisons entre sites gèrent le flux du trafic de réplication quand il y a plus d'un itinéraire pour le trafic de réplication. Vous pouvez configurer des coûts de liaisons entre sites pour indiquer qu'un lien est plus rapide, plus fiable, ou est le lien préféré. Des coûts plus élevés sont utilisés pour des liaisons lentes, et des coûts plus faibles sont utilisés pour les liens rapides. Active Directory DS est répliqué avec la connexion avec la moins coûteuse. Par défaut, tous les liens de sites sont configurés avec un coût de 100.
- Fréquence de réplication. La réplication intersite est basée uniquement sur l'interrogation. Par défaut, toutes les trois heures un partenaire de réplication interroge ses partenaires de réplication en amont pour déterminer si des modifications sont disponibles. Cet intervalle de réplication peut être trop long pour les organisations qui souhaitent que les modifications au répertoire soient répliquées plus rapidement. Vous pouvez modifier la fréquence d'interrogation en accédant aux propriétés de l'objet de lien de sites. La fréquence d'interrogation minimale est de 15 minutes.
- Planifications de réplication. Par défaut, la réplication se produit 24 heures sur 24. Cependant, vous pouvez restreindre la réplication intersite à des heures précises en modifiant les attributs de planification d'un lien de sites.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

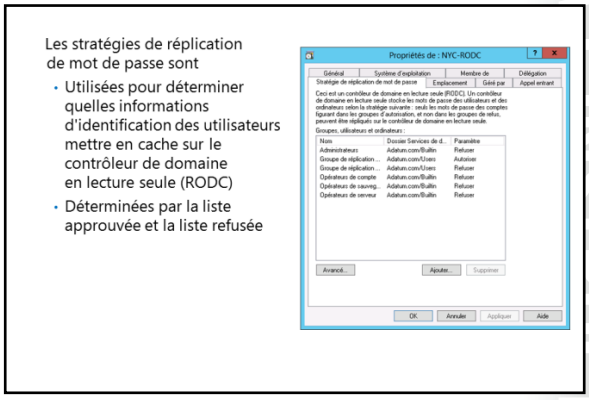
Démonstration : Configurer la réplication Active Directory DS intersite

Dans cette démonstration, vous allez apprendre à configurer la réplication AD DS intersite.

Procédure de démonstration

1. À partir du Gestionnaire de serveur, ouvrez les **sites et services Active Directory**.
2. Renommez DEFAULTIPSITELINK par **LON-TOR**.
3. Cliquez avec le bouton droit sur le lien de sites, puis cliquez sur **Propriétés**.
4. Modifiez le coût, l'intervalle de réplication, et la planification en fonction des besoins.
5. S'il y a lieu, ouvrez les propriétés du nœud IP, puis modifiez l'option **Relier tous les liens de sites**.

Options pour configurer les stratégies de réplication du mot de passe pour les contrôleurs de domaine en lecture seule



Les contrôleurs de domaine en lecture seule ont des exigences particulières concernant la réplication AD DS, liées aux informations d'identification de l'utilisateur mis en cache. Ils utilisent les stratégies de réplication de mot de passe pour déterminer quelles informations d'identification d'utilisateurs pourraient être mises en cache sur le serveur. Si une stratégie de réplication de mot de passe permet à un contrôleur de domaine en lecture seule de mettre les informations d'identification de l'utilisateur en cache, le contrôleur de domaine en lecture seule peut traiter les activités d'authentification et de ticket de service de l'utilisateur. Si les informations d'identification de l'utilisateur ne sont pas autorisées à être mises en cache sur le contrôleur de domaine en lecture seule, alors le contrôleur de domaine en lecture seule envoie les activités d'authentification et de ticket de service à un contrôleur de domaine accessible en écriture.

Pour accéder à la stratégie de réplication de mot de passe, ouvrez les propriétés du contrôleur de domaine en lecture seule dans l'unité d'organisation des contrôleurs de domaine, puis cliquez sur l'onglet **Stratégie de réplication du mot de passe**. La stratégie de réplication du mot de passe d'un contrôleur de domaine en lecture seule est déterminée par deux attributs à valeurs multiples du compte d'ordinateur du contrôleur de domaine en lecture seule. Ces attributs sont généralement connus en tant que liste des approuvés et liste des refusés. Si un compte utilisateur est sur la liste autorisée, les informations d'identification de l'utilisateur sont mises en cache. Si vous incluez des groupes sur la liste autorisée, les informations d'identification de tous les utilisateurs qui appartiennent au groupe pourront être mises en cache sur le contrôleur de domaine en lecture seule. Si l'utilisateur est sur la liste des approuvés *et* la liste des refusés, le contrôleur de domaine en lecture seule ne met pas les informations d'identification de l'utilisateur en cache. La liste des refusés a la priorité.

Pour faciliter la gestion de la stratégie de réplication du mot de passe, deux groupes de sécurité locaux du domaine sont créés dans le conteneur Utilisateurs Active Directory DS. Le premier groupe de sécurité, le groupe autorisé de réplication du mot de passe du contrôleur de domaine en lecture seule, est ajouté à la liste approuvée pour chaque nouveau contrôleur de domaine en lecture seule. Par défaut, ce groupe ne comprend pas de membres. Par conséquent, par défaut, un nouveau contrôleur de domaine en lecture seule ne mettra aucune informations d'identification de l'utilisateur en cache. S'il y a des utilisateurs pour qui vous souhaiteriez que les informations d'identification soient mises en cache par tous les contrôleurs de domaine en lecture seule, vous devez ajouter ces utilisateurs au groupe autorisé de réplication du mot de passe du contrôleur de domaine en lecture seule. Il est conseillé de créer une liste approuvée par site, et de configurer uniquement les utilisateurs assignés à ce site dans la liste approuvée.

Le second groupe, le groupe non autorisé de réplication du mot de passe du contrôleur de domaine en lecture seule, est ajouté à la liste des refusés pour chaque nouveau contrôleur de domaine en lecture seule. Si vous voulez vous assurer que les contrôleurs de domaine en lecture seule ne mettent jamais en cache les informations d'identification des utilisateurs, vous pouvez ajouter ces utilisateurs au groupe refusé de réplication du mot de passe du contrôleur de domaine en lecture seule. Par défaut, ce groupe contient les comptes de sécurité sensibles qui sont des membres des groupes, notamment les groupes administrateurs du domaine, administrateurs entreprise, administrateurs schéma, éditeurs de certification, et des propriétaires de création de stratégie de groupe (Group Policy Creator Owners).

Démonstration : Configurer les stratégies de réplication du mot de passe

Dans cette démonstration, vous allez apprendre à configurer les stratégies de réplication du mot de passe.

Procédure de démonstration

1. Démarrez **Utilisateurs et ordinateurs Active Directory**.
2. Créez au préalable un objet ordinateur de contrôleur de domaine en lecture seule nommé **LON-RODC1**.
3. Dans l'unité d'organisation **Domain Controllers**, ouvrez les propriétés de **LON-RODC1**.
4. Cliquez sur l'onglet **Stratégie de réplication de mot de passe**, et affichez la stratégie par défaut.
5. Fermez la boîte de dialogue **Propriétés de LON-RODC1**.
6. Dans la console **Utilisateurs et ordinateurs Active Directory** cliquez sur le conteneur **Utilisateurs**.
7. Double-cliquez sur **Groupe de réplication dont le mot de passe RODC est autorisé**, puis cliquez sur l'onglet **Membres** et étudiez les membres par défaut de **Groupe de réplication dont le mot de passe RODC est autorisé**. Il ne devrait y avoir aucun membre par défaut.
8. Cliquez sur **OK**.
9. Double-cliquez sur **Groupe de réplication dont le mot de passe RODC est refusé**, puis cliquez sur l'onglet **Membres**.
10. Cliquez sur **Annuler** pour fermer la boîte de dialogue **Propriétés de : Groupe de réplication dont le mot de passe...**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Outils pour gérer et surveiller la réplication

Après avoir mise en place votre configuration de réplication, vous devez pouvoir surveiller la réplication pour la prise en charge, l'optimisation, et le dépannage en continu. Deux outils sont particulièrement utiles pour créer des rapports sur la réplication et l'analyser : l'outil Diagnostics de réplication (Repadmin.exe), et l'outil Diagnostics de serveur de répertoires (Dcdiag.exe).



L'outil Diagnostics de réplication

L'outil de diagnostic de réplication, Repadmin.exe, est un outil de ligne de commande qui permet d'indiquer le statut de réplication sur chaque contrôleur de domaine. Les informations que Repadmin.exe produit peuvent vous aider à déceler un problème potentiel avec réplication dans la forêt. Vous pouvez afficher des niveaux de précision jusqu'aux métadonnées de réplication pour les objets spécifiques et les attributs, vous permettant d'identifier le lieu et le moment où une modification problématique a été apportée à Active Directory DS. Vous pouvez même utiliser Repadmin.exe pour créer la topologie de réplication et forcer la réplication entre les contrôleurs de domaine.

Repadmin.exe prend en charge un certain nombre de commandes qui effectuent des tâches spécifiques. Vous pouvez vous renseigner sur chaque commande en saisissant **repadmin/? : commande** dans une ligne de commande. La plupart des commandes requièrent des arguments. Beaucoup de commandes utilisent un paramètre *DC_LIST*, qui est simplement une étiquette de réseau (DNS, nom NetBIOS, ou adresse IP) d'un contrôleur de domaine. Voici certaines des tâches de surveillance de réplication que vous pouvez effectuer à l'aide de Repadmin :

- Afficher les partenaires de réplication pour un contrôleur de domaine. Pour afficher les connexions de réplication d'un contrôleur de domaine, saisissez **repadmin /showrepl *DC_LIST***. Par défaut, Repadmin.exe montre seulement des connexions intersite. Ajoutez l'argument de **/repsto** pour voir des connexions intersite, aussi bien.
- Afficher les objets de connexion pour un contrôleur de domaine. Saisissez **repadmin /showconn *DC_LIST*** pour afficher les objets de connexion pour un contrôleur de domaine.
- Afficher les métadonnées au sujet d'un objet, de ses attributs, et de la réplication. Vous pouvez en apprendre beaucoup sur la réplication en examinant un objet sur deux contrôleurs de domaine différents pour découvrir si les attributs ont été répliqués ou non. Saisissez **repadmin /showobjmeta *Objet de DC_LIST***, où *DC_LIST* indique le contrôleur de domaine à interroger. (Vous pouvez utiliser un astérisque [*] pour indiquer tous les contrôleurs de domaine.) *Objet* est un identificateur unique pour l'objet, son nom unique ou GUID, par exemple.

Vous pouvez également apporter des modifications à votre infrastructure de réplication à l'aide de l'outil Repadmin. Certaines des tâches de gestion que vous pouvez effectuer sont :

- Le lancement du vérificateur KCC. Saisissez **repadmin /kcc** pour forcer le vérificateur KCC pour recalculer la topologie de réplication entrante pour le serveur.
- Forcer la réplication entre deux partenaires. Vous pouvez utiliser Repadmin pour forcer la réplication d'une partition entre un contrôleur de domaine source et un contrôleur de domaine cible. Saisissez **repadmin /replicate *Destination_DC_LIST Source_DC_Name Naming_Context***.
- Synchroniser un contrôleur de domaine avec tous les partenaires de réplication. Saisissez **repadmin /syncall *Contrôleur de domaine*//e** pour synchroniser un contrôleur de domaine avec tous ses partenaires, y compris ceux situés dans d'autres sites.

L'outil de diagnostic du serveur d'annuaire

L'outil de diagnostic du service d'annuaire, Dcdiag.exe, effectue un certain nombre de tests et de rapports sur la santé et la sécurité globale de la réplication pour Active Directory DS. S'exécutant tout seul, dcdiag.exe réalise les tests récapitulatifs puis enregistre les résultats dans un rapport. À l'autre extrémité, **dcdiag.exe /c** réalise presque tous les tests. Le résultat des tests peut être redirigé vers les fichiers de divers types, notamment XML. Inscrivez **dcdiag/?** pour des informations complètes d'utilisation.

Vous pouvez également spécifier un ou plusieurs tests à effectuer en utilisant le paramètre***Nom de test*** de **/test :**. Les tests qui sont directement mis en relation à la réplication comprennent :

- FrsEvent. Enregistre toutes les erreurs d'opération dans un rapport, dans le système de réplication de fichiers.
- DFSREvent. Enregistre toutes les erreurs d'opération dans un rapport, dans le système de réplication DFS.
- Intersite. Vérifie les défaillances qui empêcheraient ou retarderaient la réplication intersite.
- KccEvent. Identifie des erreurs dans le vérificateur KCC.
- Réplications. Vérifie que la réplication entre les contrôleurs de domaine est ponctuelle.
- Topologie. Vérifie que la topologie de réplication est connectée entièrement pour tous les contrôleurs de domaine.
- VerifyReplicas. Vérifie que toutes les partitions de l'annuaire d'applications sont entièrement instanciées sur tous les contrôleurs de domaine qui hébergent des réplicas.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation des sites et de la réplication AD DS

Scénario

La société A. Datum Corporation a déployé un domaine unique AD DS dont tous les contrôleurs de domaine sont situés dans le centre de données à Londres. Comme la société a grossi et que des filiales se sont ajoutées, et avec elles un grand nombre d'utilisateurs, il est devenu de plus en plus évident que l'environnement actuel AD DS ne satisfait pas aux exigences de la société. Les utilisateurs dans certaines des filiales signalent que le temps d'attente pour se connecter sur leurs ordinateurs est long. L'accès aux ressources réseau telles que les serveurs Microsoft Exchange 2010 de la société et Microsoft SharePoint® peuvent être lents, et ils échouent sporadiquement.

En tant qu'un des administrateurs réseau principaux, vous êtes responsable de la planification et de la mise en œuvre d'une infrastructure AD DS qui aidera à répondre aux exigences stratégiques de l'organisation. Vous êtes responsable de configurer les sites et la réplication AD DS pour optimiser l'expérience de l'utilisateur et l'utilisation du réseau dans l'organisation.

Objectifs

- Configurez le site par défaut créé dans Active Directory DS.
- Créez et configurez les sites supplémentaires dans Active Directory DS.
- Configurez et surveillez la réplication entre les sites AD DS.

Configuration de l'atelier pratique

Durée approximative : 30 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-TOR-DC1**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   a. Nom d'utilisateur : **Adatum\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22412B-TOR-DC1**.

Exercice 1 : Modification du site par défaut

Scénario

Datum Corporation a décidé de mettre en œuvre des sites AD DS supplémentaires pour optimiser l'utilisation du réseau pour le trafic réseau AD DS. La première étape en mettant en œuvre le nouvel environnement est d'installer un nouveau contrôleur de domaine pour le site de Toronto. Vous allez ensuite reconfigurer le site par défaut et attribuer au site des sous-réseaux aux adresses IP appropriées.

Enfin, il vous a été demandé de modifier le nom du site par défaut par LondonHQ et de l'associer au sous-réseau IP 172.16.0.0/24, qui est la plage sous-réseau utilisée pour le siège à London.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le contrôleur de domaine de Toronto.
2. Renommer le site par défaut
3. Configurez les sous-réseaux IP associés au site par défaut.

▶ Tâche 1 : Installer le contrôleur de domaine de Toronto

1. Sur TOR-DC1, utiliser le gestionnaire de serveur pour installer **Active Directory Domain Services**.
2. Quand les binaires AD DS sont installés, utilisez l'**Assistant de configuration des services de domaine Active Directory** pour installer et configurer **TOR-DC1** en tant que contrôleur de domaine supplémentaire pour Adatum.com.
3. Après le redémarrage du serveur, ouvrez une session en tant qu' **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.

▶ Tâche 2 : Renommer le site par défaut

1. Si nécessaire, sur LON-DC1, ouvrez la console du gestionnaire de serveur.
2. Ouvrez les sites Active Directory et les services, puis renommez le site **Default-First-Site-Name** par **LondonHQ**.
3. Vérifiez que **LON-DC1** et **TOR-DC1** sont des membres du site **LondonHQ**.

▶ Tâche 3 : Configurez les sous-réseaux IP associés au site par défaut

1. S'il y a lieu, sur LON-DC1, ouvrez la console du **Gestionnaire de serveur**, puis ouvrez les **sites et les services Active Directory**.
2. Créez un nouveau sous-réseau avec la configuration suivante :
   - Préfixe : **172.16.0.0/24**
   - Objet de site : **LondonHQ**

Résultats : Après avoir complété cet exercice, vous aurez reconfiguré le site par défaut et assigné les sous-réseaux IP au site.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Création de sites et de sous-réseaux supplémentaires

Scénario

L'étape suivante dans la mise en œuvre de la conception du site AD DS est de configurer le nouveau site AD DS. Le premier site que vous devez mettre en œuvre est le site de Toronto pour le centre de données nord-américain. L'équipe réseau à Toronto voudrait également avoir un site consacré appelé TestSite au centre de données de Toronto. Il vous a été indiqué que l'adresse de sous-réseau IP de Toronto est 172.16.1.0/24, et l'adresse de sous-réseau IP de test est 172.16.100.0/24.

Les tâches principales de cet exercice sont les suivantes :

1. Créez les sites AS DS pour Toronto
2. Créez les sous-réseaux IP associés avec les sites de Toronto

▶ Tâche 1 : Créez les sites AS DS pour Toronto

1. S'il y a lieu, sur LON-DC1, ouvrez la console du **Gestionnaire de serveur**, puis ouvrez les **sites et les services Active Directory**.
2. Créez un nouveau site avec la configuration suivante :
   - Nom : **Toronto**
   - Objet de lien de sites : **DEFAULTIPSITELINK**
3. Créez un autre nouveau site avec la configuration suivante :
   - Nom : **TestSite**
   - Objet de lien de sites : **DEFAULTIPSITELINK**

▶ Tâche 2 : Créez les sous-réseaux IP associés avec les sites de Toronto

1. Si nécessaire, sur LON-DC1, ouvrez **Sites et services Active Directory**.
2. Créez un nouveau sous-réseau avec la configuration suivante :
   - Préfixe : **172.16.1.0/24**
   - Objet de site : **Toronto**
3. Créez un autre nouveau sous-réseau avec la configuration suivante :
   - Préfixe : **172.16.100.0/24**
   - Objet de site : **TestSite**
4. Dans le volet de navigation, cliquez sur le dossier **Sous-réseau**. Vérifiez dans le volet d'informations que les trois sous-réseaux sont créés et associés avec leur site approprié.

Résultats : À la fin de cet exercice, vous aurez créé deux sites supplémentaires représentant les adresses IP de sous-réseau situées à Toronto.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Configuration de la réplication AD DS

Scénario

Maintenant que les sites Active Directory DS ont été configurés pour Toronto, l'étape suivante est de configurer les liens de sites pour gérer la réplication entre les sites, puis de déplacer le contrôleur de domaine TOR-DC1 vers le site de Toronto. Actuellement tous les sites appartiennent à DEFAULTIPSITELINK.

Vous devez modifier la liaison de site de telle sorte que LondonHQ et Toronto appartiennent à un lien de sites commun appelé LON-TOR. Vous devriez configurer ce lien pour répliquer chaque heure. En outre, vous devriez lier le site de TestSite uniquement au site de Toronto utilisant un lien de sites nommé TOR-TEST. La réplication ne devrait pas être disponible depuis le site de Toronto vers le TestSite pendant les heures de travail, c'est-à-dire de 9 h à 15h.

Vous utiliserez maintenant des outils pour surveiller la réplication entre les sites.

Les tâches principales de cet exercice sont les suivantes :

1. Configurez les liens de sites entre les sites Active Directory DS
2. Déplacez TOR-DC1 au site de Toronto
3. Surveillez la réplication de site AD DS

▶ Tâche 1 : Configurez les liens de sites entre les sites Active Directory DS

1. Si nécessaire, sur LON-DC1, ouvrez **Sites et services Active Directory**.
2. Créez un site de lien basé sur une adresse IP avec la configuration suivante :
   - Nom : **TOR-TEST**
   - Sites : **Toronto, TestSite**
   - Modifiez la planification pour permettre seulement la réplication entre **lundi 9h et vendredi 15h.**
3. Renommez DEFAULTIPSITELINK et configurez-le avec les paramètres suivants :
   - Nom : **LON-TOR**
   - Sites : **LondonHQ, Toronto**
   - Réplication : Toutes les **60** minutes.

▶ Tâche 2 : Déplacez TOR-DC1 au site de Toronto

1. Si nécessaire, sur LON-DC1, ouvrez **Sites et services Active Directory**.
2. Déplacez **TOR-DC1** depuis le site de **LondonHQ** vers le site de **Toronto**.
3. Vérifiez que TOR-DC1 est situé sous le nœud de serveurs dans le site de Toronto.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Surveillez la réplication de site AD DS

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell®**.
2. Utilisez les commandes suivantes pour surveiller la réplication de site :

```
Repadmin /kcc
```

La commande recalcule la topologie de réplication entrante pour le serveur.

```
Repadmin /showrepl
```

Vérifie que la dernière réplication avec TOR-DC1 a été réussie.

```
Repadmin /bridgeheads
```

Cette commande affiche les serveurs tête de pont pour la topologie du site.

```
Repadmin /replsummary
```

Cette commande affiche un résumé des tâches de réplication. Vérifiez qu'aucune erreur n'apparaît.

```
DCDiag /test:replications
```

Vérifie que tous les tests de connectivité et de réplication ont eu lieu avec succès.

3. Basculez vers **TOR-DC1**, puis répétez les commandes pour afficher les informations depuis le point de vue de TOR-DC1.

Résultats : À la fin de cet exercice, vous aurez configuré les liens de sites et surveillé la réplication.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-TOR-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée :

Mettez en œuvre les recommandations suivantes quand vous gérez les sites et la réplication Active Directory dans votre environnement :

- Fournissez toujours au moins un ou plusieurs serveurs de catalogue global par site.
- Assurez-vous que tous les sites ont des sous-réseaux associés appropriés.
- Ne paramétrez pas de longs intervalles sans réplication quand vous configurez des planifications de réplication pour la réplication intersite.
- Évitez d'utiliser SMTP comme protocole pour la réplication.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Le client ne peut pas localiser le contrôleur de domaine dans son site.	
La réplication entre les sites ne fonctionne pas.	
La réplication entre deux contrôleurs de domaine dans le même site ne fonctionne pas.	

Questions de contrôle des acquis

Question : Pourquoi est-il important que tous les sous-réseaux soient identifiés et associés à un site dans une entreprise multi sites ?

Question : Quels sont les avantages et les inconvénients de réduire l'intervalle de réplication intersite?

Question : Quelle est la fonction d'un serveur tête de pont ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6

Implémentation des services de certificats Active Directory

Table des matières :

Vue d'ensemble du module **6-1**

Leçon 1 : Présentation de l'infrastructure à clé publique (PKI) **6-2**

Leçon 2 : Déploiement d'autorités de certification **6-13**

Atelier pratique A : Déploiement et configuration de la hiérarchie d'autorités de certification **6-21**

Leçon 3 : Déploiement et gestion des modèles de certificats **6-25**

Leçon 4 : Implémentation de la distribution et de la révocation de certificats **6-31**

Leçon 5 : Gestion de la récupération de certificats **6-42**

Atelier pratique B : Déploiement et gestion de certificats **6-47**

Contrôle des acquis et éléments à retenir **6-54**

Vue d'ensemble du module

L'infrastructure à clé publique (PKI) se compose de plusieurs composants qui vous aident à sécuriser des communications et des transactions de l'entreprise. Un tel composant est l'autorité de certification (AC). Vous pouvez utiliser des autorités de certification pour gérer, distribuer et valider les certificats numériques qui sont utilisés pour sécuriser les informations. Vous pouvez installer des Services de certificats Active Directory® (AD CS) comme autorité de certification racine ou autorité de certification secondaire dans votre organisation. Dans ce module, vous apprendrez comment implémenter le rôle serveur et les certificats d'AD CS.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire la PKI ;
- déployer les autorités de certification ;
- déployer et configurer une hiérarchie d'autorité de certification ;
- déployer et gérer des modèles de certificats.
- implémenter la distribution et la révocation de certificats ;
- gérer la récupération de certificats.

Leçon 1
Présentation de l'infrastructure à clé publique (PKI)

La PKI vous permet de vérifier et d'authentifier l'identité de chaque partie impliquée dans une transaction électronique. Elle vous aide également à établir une confiance entre les ordinateurs et les applications correspondantes qui sont hébergées sur des serveurs d'applications. Un exemple classique est l'utilisation de la technologie de PKI pour sécuriser des sites Web. Les certificats numériques sont des composants principaux de la PKI qui contiennent les informations d'identification électroniques, utilisées pour authentifier des utilisateurs ou des ordinateurs. D'ailleurs, des certificats peuvent être validés à l'aide des processus de détection de certificats, de validation de chemin d'accès et du contrôle de la révocation. Windows Server® 2012 prend en charge la création d'une infrastructure de services de certificats dans votre organisation à l'aide des composants d'AD CS.

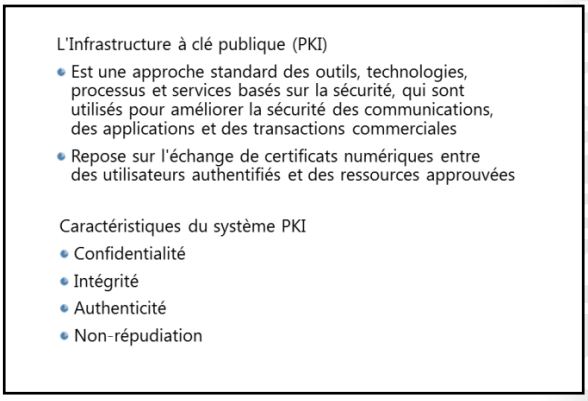
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire la PKI ;
- décrire les composants d'une solution de PKI ;
- décrire les AC ;
- décrire le rôle serveur d'AD CS dans Windows Server 2012 ;
- décrire de nouvelles fonctionnalités dans AD CS dans Windows Server 2012 ;
- expliquer la différence entre les AC privées et publiques ;
- décrire une hiérarchie de certifications croisées.

Qu'est-ce que PKI ?

Une infrastructure à clé publique est une combinaison de logiciels, de technologies de chiffrement, de processus et de services qui permettent à une organisation de sécuriser ses communications et transactions commerciales. C'est un système de certificats numériques, d'autorités de certification et d'autres autorités d'enregistrement. En cas de transaction électronique, la PKI vérifie et authentifie la validité de chaque partie impliquée. Les normes de la PKI évoluent toujours, mais sont largement implémentés comme élément essentiel du commerce électronique.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Concepts généraux de la PKI

Généralement une solution de PKI se fonde sur plusieurs technologies et composants. Lorsque vous envisagez d'implémenter une PKI, vous devez tenir compte de et comprendre ce qui suit :

- Infrastructure. La signification dans ce contexte est la même que dans n'importe quel autre contexte, comme l'électricité, le transport ou l'approvisionnement en eau. Chacun de ces éléments réalise un travail spécifique, et ses exigences doivent être respectées pour qu'il fonctionne correctement. La somme de ces éléments tient compte de l'utilisation efficace et sûre de la PKI. Les éléments qui composent une PKI sont les suivants :
    - une autorité de certification ;
    - un référentiel de certificat ;
    - une autorité d'inscription ;
    - une capacité à révoquer des certificats ;
    - une capacité à sauvegarder, récupérer et mettre à jour des clés ;
    - une capacité à réguler et suivre le temps.
    - Traitement côté client

      La plupart de ces composants seront présentés dans des rubriques et des cours postérieurs de ce module.
- Clés publiques/privées. Généralement, il existe deux méthodes pour chiffrer et déchiffrer des données :
    - Chiffrement symétrique : Les méthodes pour le chiffrement et le déchiffrement des données sont identiques ou se ressemblent. Les données sont chiffrées à l'aide d'une méthode ou d'une clé particulière. Pour déchiffrer les données, vous devez avoir la même méthode ou clé identique. Par conséquent, tout utilisateur possédant la clé peut déchiffrer les données. La clé doit demeurer privée pour assurer l'intégrité du chiffrement.
    - Chiffrement asymétrique : Dans ce cas, les méthodes pour le chiffrement et le déchiffrement des données ne sont pas identiques ou ne se ressemblent pas. Les données sont chiffrées à l'aide d'une méthode ou d'une clé particulière. Cependant, une clé différente est utilisée pour déchiffrer les données. Pour ce faire, utilisez une paire de clés. Chaque personne obtient une paire de clés, qui se compose d'une clé publique et d'une clé privée. Ces clés sont uniques, et les données que la clé publique chiffre peuvent être déchiffrées à l'aide de la clé privée, et inversement. Dans ce cas, les clés sont suffisamment différentes et connaître ou posséder une clé ne vous permet pas de déterminer l'autre. Par conséquent, une des clés (publiques) peut être rendue publiquement disponible sans restreindre la sécurité des données, tant que l'autre clé (privée) reste privée, d'où le nom Infrastructure à clé publique.

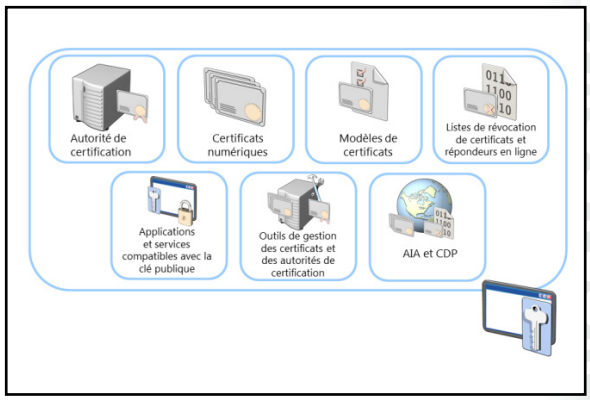
Les algorithmes qui utilisent le chiffrement symétrique sont rapides et efficaces pour un grand volume de données. Cependant, parce qu'ils utilisent une clé symétrique, ils ne sont pas considérés comme assez sécurisés, parce que vous devez toujours transporter la clé à l'autre partie. Sinon, les algorithmes qui utilisent le chiffrement asymétrique sont sécurisés, mais très lents. C'est pour cette raison que nous utilisons généralement une approche hybride, c'est-à-dire que les données sont chiffrées à l'aide du chiffrement symétrique, alors que la clé de chiffrement symétrique est protégée avec le chiffrement asymétrique.

Quand vous implémentez une solution de PKI, tout votre système, et particulièrement l'aspect sécurité, peut en bénéficier. Les avantages de l'utilisation de la PKI sont notamment les suivants :

- Confidentialité. Une solution d'infrastructure à clé publique vous permet de chiffrer aussi bien les données stockées que les données transmises.
- Intégrité. Vous pouvez utiliser une infrastructure à clé publique pour signer numériquement les données. Une signature numérique permet de déterminer si des données ont été modifiées pendant la communication d'informations.
- Authenticité et non-répudiation. Les données d'authentification passent par des algorithmes de hachage tels que l'algorithme de hachage sécurisé 1 (SHA-1) pour produire un résumé de message. Le résumé de message est ensuite signé numériquement à l'aide d'une clé privée de l'expéditeur pour montrer que le résumé du message a été produit par l'expéditeur. La non-répudiation, ce sont des données signées numériquement, ce qui prouve à la fois l'intégrité des données signées et l'origine des données.
- Approche basée sur des normes. La PKI est basée sur des normes, ce qui signifie que plusieurs fournisseurs de technologie sont obligés de prendre en charge les infrastructures de sécurité basées sur la PKI. Elle est basée sur des normes de l'industrie définies dans RFC 2527, « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework » (Stratégie de certificat d'infrastructure à clé publique Internet X.509 et infrastructure des pratiques de certification).

Composants d'une solution de PKI

Beaucoup de composants doivent être utilisés ensemble pour fournir une solution complète de PKI. Les composants de la PKI de Windows Server 2012 sont les suivants :



- AC. L'autorité de certification émet et gère des certificats numériques pour les utilisateurs, les ordinateurs et les services. En déployant l'autorité de certification, vous établissez l'infrastructure à clé publique dans votre organisation.
- Certificats numériques. Les certificats numériques s'apparentent à un passeport électronique. Un certificat numérique est utilisé pour justifier l'identité de l'utilisateur (ou de toute autre entité). Il contient des informations d'identification électroniques associées à une clé publique et à une clé privée, utilisées pour authentifier des utilisateurs et d'autres périphériques tels que des serveurs Web et des serveurs de messagerie. Les certificats numériques garantissent également qu'un logiciel ou du code est exécuté à partir d'une source approuvée. Ils contiennent différents champs, tels que **Objet**, **Émetteur** et **Nom commun**. Ces champs sont utilisés pour déterminer l'utilisation spécifique du certificat. Par exemple, un certificat de serveur Web peut comporter le champ **Nom commun** de **web01.contoso.com**, ce qui rendrait ce certificat valide uniquement pour ce serveur Web. Si une tentative venait à être effectuée pour utiliser ce certificat sur un serveur Web nommé **web02.contoso.com**, l'utilisateur de ce serveur recevrait alors un avertissement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

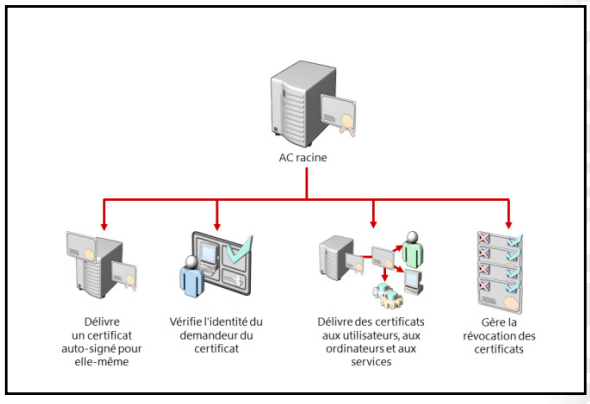
- Modèles de certificats. Ce composant décrit le contenu ainsi que l'objectif d'un certificat numérique. Lors de la demande d'un certificat auprès d'une autorité de certification d'entreprise AD CS, le demandeur de certificat peut, en fonction de ses droits d'accès, faire un choix parmi plusieurs types de certificats basés sur des modèles de certificats, tels que les modèles Utilisateur et Signature du code. Le modèle de certificat enregistre les utilisateurs de bas niveau et les décisions techniques relatives au type de certificat dont ils ont besoin. En outre, il permet aux administrateurs d'identifier le demandeur et le type de certificat demandé.
- Listes de révocation de certificats et répondeurs en ligne.
    - Les listes de révocation de certificats consistent en des listes complètes numériquement signées de certificats révoqués. Ces listes sont publiées périodiquement et peuvent être récupérées et mises en cache par les clients (selon la durée de vie configurée de la liste de révocation de certificats). Elles sont utilisées pour vérifier l'état de la révocation d'un certificat.
    - Les répondeurs en ligne font partie du service de rôle OCSP (Online Certificate Status Protocol) de Windows Server 2008 et Windows Server 2012. Un répondeur en ligne peut recevoir une demande de vérification de la révocation d'un certificat sans que le client ait besoin de télécharger la liste de révocation de certificats complète. Cette opération accélère le processus de vérification de la révocation de certificats et réduit la bande passante réseau. Elle améliore également l'évolutivité et la tolérance de panne en permettant la configuration de groupe des répondeurs en ligne.
- Applications et services basés sur une clé publique. Il s'agit des applications ou des services qui prennent en charge le chiffrement par clé publique. En d'autres termes, l'application ou les services doivent pouvoir prendre en charge les implémentations de clé publique pour en tirer profit.
- Outils de gestion des certificats et des autorités de certification. Les outils de gestion fournissent les outils basés sur l'interface graphique utilisateur et sur la ligne de commande pour :
    - configurer les autorités de certification ;
    - récupérer les clés privées archivées ;
    - importer et exporter les certificats et les clés ;
    - publier les certificats des autorités de certification et les listes de révocation de certificats ;
    - gérer les certificats émis.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Accès aux informations de l'autorité (AIA) et points de distribution de la liste de révocation de certificats (CDP). Les points d'accès aux informations de l'autorité déterminent l'emplacement de recherche et de validation des certificats des autorités de certification, et les emplacements de points de distribution de la liste de révocation de certificats déterminent les points de recherche des listes de révocation de certificats pendant le processus de validation du certificat. Dans la mesure où les listes de révocation de certificats peuvent devenir volumineuses (en fonction du nombre de certificats émis et révoqués par une autorité de certification), vous pouvez également publier des listes de révocation de certificats temporaires plus limitées appelées *listes de révocation de certificats delta*. Les listes de révocation de certificats delta contiennent uniquement les certificats révoqués depuis la publication de la dernière liste CRL standard. Cela permet aux clients de récupérer les listes de révocation de certificats delta plus petites et d'établir plus rapidement la liste complète des certificats révoqués. Les listes de révocation de certificats delta permettent également de publier plus fréquemment les données de révocation, dans la mesure où leur transfert s'effectue plus rapidement que celui des listes CRL complètes.
- Module de sécurité matériel (HSM). Un module de sécurité matériel est un périphérique matériel de chiffrement sécurisé facultatif qui accélère le traitement du chiffrement en vue de gérer les codes numériques. Ce matériel de stockage spécialisé hautement sécurisé est connecté à l'autorité de certification afin de gérer les certificats. En règle générale, le module de sécurité matériel est physiquement raccordé à un ordinateur. Il consiste en un module complémentaire facultatif de l'infrastructure à clé publique, et est plus fréquemment utilisé dans les environnements de haute sécurité dans lesquels les répercussions seraient importantes si une clé venait à être compromise.

Remarque : Le composant le plus important de n'importe quelle infrastructure de sécurité est la sécurité physique. Une infrastructure de sécurité n'est pas simplement l'implémentation de la PKI. D'autres éléments, comme les stratégies de sécurité physique et de sécurité adéquate, sont également des composants importants d'une infrastructure holistique de sécurité.

Que sont les autorités de certification ?



Une autorité de certification est un service bien conçu et très fiable dans une entreprise, qui fournit des certificats à des utilisateurs et des ordinateurs, conserve les listes de révocation de certificats et répond éventuellement aux demandes d'OCSP. Vous pouvez installer une autorité de certification dans votre environnement en déployant le rôle AD CS sur Windows Server 2012. Quand vous installez la première autorité de certification, elle établit la PKI dans le réseau et elle fournit le point le plus élevé dans la structure entière. Vous pouvez avoir une ou plusieurs autorités de certification dans un réseau, mais seulement une autorité de certification peut être au point le plus élevé de la hiérarchie d'autorité de certification (cette autorité de certification est appelée *autorité de certification racine*, qui sera présentée plus tard dans ce module).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les principaux objectifs de l'autorité de certification sont l'émission de certificats, la révocation de certificats et la publications d'informations de l'AIA et de la liste de révocation de certificats. Ce faisant, l'autorité de certification vérifie que les utilisateurs, les services et les ordinateurs sont des certificats émis qui peuvent être validés.

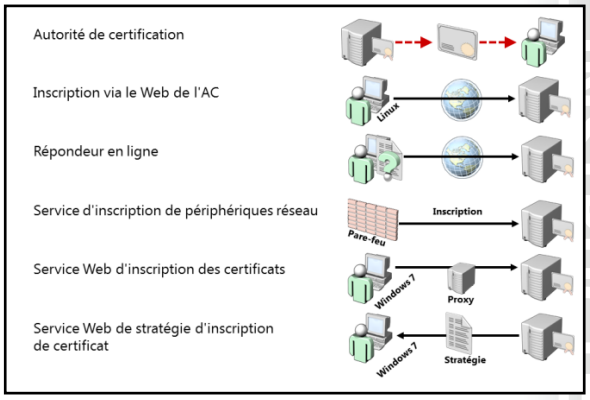
Une autorité de certification a plusieurs fonctions ou rôles dans une PKI. Dans une grande PKI, la séparation des rôles de l'autorité de certification entre plusieurs serveurs est commune. Une autorité de certification fournit plusieurs des tâches de gestion, notamment :

- la vérification de l'identité du demandeur du certificat ;.
- l'émission de certificats aux utilisateurs, ordinateurs et services qui en font la demande ;.
- la gestion de la révocation des certificats.

Quand vous déployez une première autorité de certification (autorité de certification racine) dans votre réseau, elle délivre un certificat pour elle-même. Ensuite, d'autres autorités de certification reçoivent des certificats de la première autorité de certification. Vous pouvez également choisir d'émettre un certificat pour votre autorité de certification à l'aide de l'une des autorités de certification publiques.

Vue d'ensemble du rôle serveur AD CS dans Windows Server 2012

Tous les composants liés à la PKI sont déployés comme services de rôle du rôle serveur AD CS. Le rôle serveur AC CS se compose de plusieurs composants appelés *services de rôle*. Chaque service de rôle est responsable d'une partie spécifique de l'infrastructure de certificat, tout en travaillant ensemble pour former une solution complète.



Les services du rôle AD CS sont :

- AC. Ce composant émet des certificats pour les utilisateurs, les ordinateurs et les services. Elle gère également la validité de certificat. Plusieurs autorités de certification peuvent être reliées pour former une hiérarchie de PKI.
- Inscription via le Web de l'AC. Ce composant fournit une méthode pour émettre et remplacer des certificats pour des utilisateurs, ordinateurs et périphériques qui ne sont pas joints au domaine, qui ne sont pas connectés directement au réseau ou qui sont destinés aux utilisateurs de systèmes d'exploitation non-Windows®.
- Répondeur en ligne. Vous pouvez utiliser ce composant pour configurer et gérer la validation d'OCSP et le contrôle de la révocation. Le répondeur en ligne décode des demandes d'état de révocation de certificats spécifiques, évalue l'état de ces certificats et renvoie une réponse signée contenant les informations d'état de certificat demandées. À la différence de Windows Server 2008 R2, vous pouvez installer le répondeur en ligne sur n'importe quelle version de Windows Server 2012. Les données de révocation des certificats peuvent provenir d'une autorité de certification sur un ordinateur sous Windows Server 2003, Windows Server 2008 ou d'une autorité de certification non-Microsoft.
- Service d'inscription de périphériques réseau. Avec ce composant, les routeurs, les commutateurs et d'autres périphériques réseau peuvent obtenir des certificats d'AD CS. Sous Windows Server 2008 R2, ce composant est seulement disponible dans les éditions Entreprise et Datacenter, mais avec Windows Server 2012, vous pouvez installer ce service de rôle sur n'importe quelle version.

- Service Web d'inscription des certificats. Ce composant fonctionne comme proxy entre les ordinateurs clients Windows 7 et Windows 8 et l'autorité de certification. Ce composant est nouveau dans Windows Server 2008 R2 et Windows Server 2012, et nécessite que la forêt Active Directory soit au moins au niveau de Windows Server 2008 R2. Il permet à des utilisateurs de se connecter à une autorité de certification au moyen d'un navigateur Web pour effectuer ce qui suit :
  - demander, remplacer et installer des certificats émis ;
  - récupérer des listes de révocation de certificats ;
  - télécharger un certificat racine ;
  - s'inscrire sur Internet ou via des forêts (nouveautés dans Windows Server 2008 R2).
- Service Web de stratégie d'inscription de certificats. Ce composant est nouveau dans Windows Server 2008 R2 et Windows Server 2012. Il permet à des utilisateurs d'obtenir des informations sur la stratégie d'inscription de certificat. Combiné au service Web d'inscription de certificat, il permet l'inscription de certificat basée sur la stratégie quand l'ordinateur client n'est pas un membre d'un domaine, ou quand aucun membre du domaine n'est connecté au domaine.

Nouveautés d'AD CS dans Windows Server 2012

Comme beaucoup d'autres rôles de Windows Server, AD CS est amélioré et optimisé dans Windows Server 2012. Le rôle AD CS dans Windows Server 2012 a toujours les six mêmes services de rôle, comme décrit dans la rubrique précédente. En outre, il fournit maintenant plusieurs nouvelles fonctionnalités et fonctions en comparaison avec des versions précédentes.

- Tous les services de rôle AD CS sont exécutables sur toutes les versions de Windows Server
- Intégration complète avec le Gestionnaire de serveur
- Gestion avec Windows PowerShell
- Nouvelle version des modèles de certificats (v4)
- Prise en charge du renouvellement automatique des certificats pour les ordinateurs non associés à un domaine
- Application du renouvellement des certificats avec la même clé
- Sécurité accrue pour les demandes de certificat
- Prise en charge des cartes à puces virtuelles

Dans Windows Server 2008 R2, certains services de rôle AD CS ont besoin d'une version spécifique de Windows Server. Par exemple, le service d'inscription de périphériques réseau ne fonctionne pas sous Windows Server 2008 Standard Edition, mais seulement sous Windows Server 2008 Enterprise Edition. Sous Windows Server 2012, tous les services de rôle sont disponibles sur toutes les versions de Windows Server.

Le rôle de serveur AD CS, en plus de tous les services de rôle associés, peut fonctionner sous Windows Server 2012 avec une interface graphique utilisateur complète, une interface serveur minimale ou sur un serveur exécutant l'installation minimale. Vous pouvez déployer des services de rôle AD CS dans Windows Server 2012 à l'aide du Gestionnaire de serveur ou des applets de commande Windows PowerShell®. En outre, vous pouvez déployer les services de rôle tout en travaillant localement sur l'ordinateur ou à distance sur le réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

D'un point de vue de la gestion, AD CS et ses événements, et l'outil de Best Practices Analyzer sont maintenant entièrement intégrés à la console Gestionnaire de serveur, ce qui signifie que vous pouvez accéder à toutes ses options directement depuis le Gestionnaire de serveur. AD CS peut également être entièrement géré à l'aide de l'interface de ligne de commande Windows PowerShell.

La version d'AD CS pour Windows Server 2012 présente également une nouvelle version de modèle de certificat, la version 4 (v4), qui propose quelques nouvelles fonctions. Ce point sera présenté séparément dans le cours 3.

Des services Web d'inscription de certificat sont également améliorés dans Windows Server 2012. Cette fonctionnalité, présentée dans Windows 7 et Windows Server 2008 R2, permet des demandes de certificat en ligne provenant de domaines Active Directory Domain Services (AD DS), voire d'ordinateurs ou de périphériques qui ne sont pas joints à un domaine. AD CS dans Windows Server 2012 permet également de remplacer des certificats automatiquement pour les ordinateurs qui font partie de domaines AD DS ou qui ne sont pas joints à un domaine.

Du point de vue de la sécurité, AD CS dans Windows Server 2012 permet de demander le renouvellement d'un certificat avec la même clé. Windows Server 2012 prend également en charge la génération de clés protégées par TPM à l'aide de fournisseurs de stockage de clé basé sur TPM. L'avantage d'utiliser un fournisseur de stockage de clé basé sur TPM est l'absence d'exportabilité réelle des clés qui sont sauvegardées par le mécanisme TPM qui bloque les utilisateurs s'ils entrent un code PIN erroné trop souvent. Pour encore améliorer la sécurité, vous pouvez maintenant forcer le chiffrement de toutes les demandes de certificat qui proviennent d'AD CS dans Windows Server 2012.

Cartes à puce virtuelles

En option pour l'authentification à facteurs multiples, des cartes à puce ont été utilisées depuis Microsoft® Windows 2000 Server. Les cartes à puce améliorent la sécurité via des mots de passe, car il est beaucoup plus difficile pour un utilisateur non autorisé d'accéder à un système et d'y rester connecté. En outre, l'accès à un système protégé par carte nécessite qu'un utilisateur ait une carte valide et connaisse le code PIN qui permet d'accéder à cette carte. Par défaut, une seule copie de la carte à puce existe. Par conséquent, une seule personne peut utiliser les informations d'identification d'ouverture de session. En outre, un utilisateur remarquera rapidement si sa carte a été perdue ou volée, particulièrement quand sa carte est combinée à l'accès physique aux portes ou autres fonctions. Ceci réduit considérablement le risque du vol d'informations d'identification par rapport aux mots de passe.

Cependant, l'implémentation de l'infrastructure de carte à puce s'est parfois avérée trop chère. Pour implémenter des cartes à puce, les sociétés devaient acheter le matériel, y compris des lecteurs de cartes à puce et des cartes à puce. Dans certains cas, ce coût a empêché le déploiement de l'authentification à facteurs multiples.

Pour aborder ces problèmes, Windows Server 2012 AD CS présente une technologie qui fournit la sécurité des cartes à puce tout en réduisant les coûts de matériel et du support technique. Pour ce faire, des cartes à puce virtuelles sont fournies. Les cartes à puce virtuelles émulent la fonctionnalité des cartes à puce traditionnelles, mais au lieu de nécessiter l'achat du matériel supplémentaire, elles utilisent la technologie que les utilisateurs possèdent déjà et sont susceptibles d'avoir sur eux à tout moment.

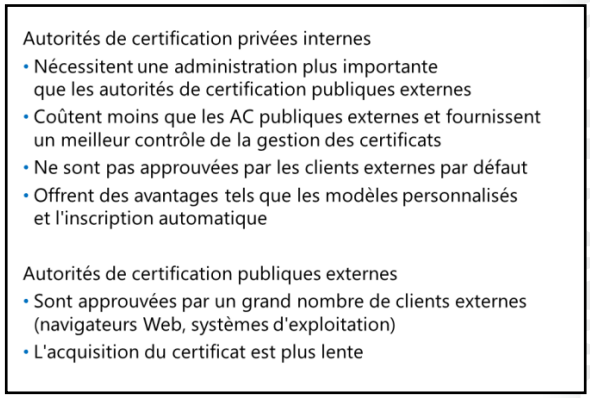
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les cartes à puce virtuelles dans Windows Server 2012 tirent profit des fonctions de la puce TPM qui est présente sur la plupart des cartes mères de l'ordinateur produites ces deux dernières années. Puisque la puce se trouve déjà dans l'ordinateur, il n'y a aucun coût lié à l'achat des cartes à puce et des lecteurs de cartes à puce. Cependant, à la différence des cartes à puce traditionnelles, où l'utilisateur possédait physiquement la carte, dans le scénario de la carte à puce virtuelle, un ordinateur (ou pour être plus spécifique, la puce TPM sur sa carte mère) agit comme une carte à puce. À l'aide de cette approche, l'authentification à deux facteurs semblable aux cartes à puce traditionnelles est accomplie. Un utilisateur doit avoir son ordinateur (qui a été configuré avec la carte à puce virtuelle) et connaître également le code PIN nécessaire pour utiliser sa carte à puce virtuelle.

Il est important de comprendre comment les cartes à puce virtuelles protègent des clés privées. Les cartes à puce traditionnelles ont leurs propres stockage et mécanisme de chiffrement pour protéger les clés privées. Dans le scénario de la carte à puce virtuelle, des clés privées sont protégées non pas par l'isolement de la mémoire physique, mais plutôt par les fonctions de chiffrement du TPM : toutes les informations confidentielles qui sont enregistrées sur une carte à puce sont chiffrées à l'aide du TPM, puis stockées sur le disque dur de manière chiffrée. Bien que des clés privées soient stockées sur un disque dur (de manière chiffrée), toutes les opérations de chiffrement se produisent dans l'environnement sécurisé et isolé du TPM. Les clés privées ne laissent jamais cet environnement non chiffré. Si le disque dur de la machine est compromis de quelque façon que ce soit, il est impossible d'accéder à des clés privées car elles sont protégées et chiffrées par TPM. Pour plus de sécurité, vous pouvez également chiffrer le lecteur avec le chiffrement de lecteur Windows BitLocker®. Pour déployer des cartes à puce virtuelles, vous avez besoin de Windows Server 2012 AD CS et d'un ordinateur client Windows 8 avec une puce TPM sur la carte mère.

AC publiques et AC privées

Quand vous prévoyez l'implémentation de la PKI pour votre organisation, un des premiers choix que vous devriez faire est de savoir si vous voulez utiliser des autorités de certification privées ou publiques. Il est possible que vous établissiez la PKI à l'aide de l'une de ces deux approches. Si vous décidez d'utiliser une autorité de certification privée, déployez le rôle de serveur AD CS, puis établissez une PKI interne. Si vous décidez d'utiliser une PKI externe, vous ne devez déployer aucun service en interne.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les deux approches ont des avantages et des inconvénients, comme spécifié dans le tableau suivant.

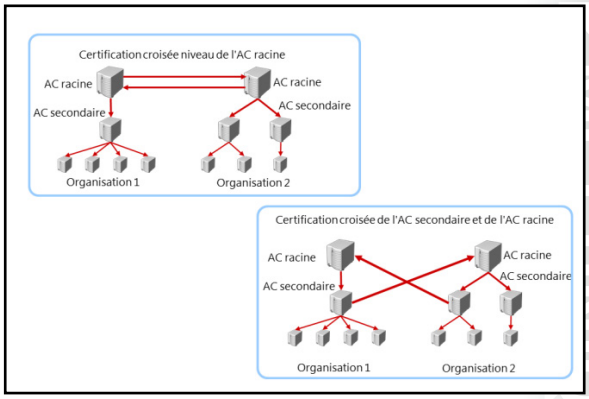
Type d'AC	Avantages	Inconvénients
Autorité de certification publique externe	• À laquelle beaucoup de clients externes font confiance (navigateurs Web, systèmes d'exploitation) • Nécessite une administration minimale	• Un coût plus élevé par rapport à une autorité de certification interne • Le coût est basé sur le certificat • L'acquisition du certificat est plus lente
Autorité de certification privée interne	• Assure un contrôle supérieur de la gestion de certificat • Moins onéreux par rapport à une autorité de certification publique • Modèles personnalisés • Inscription automatique	• Par défaut, à laquelle les clients externes ne font pas confiance (navigateurs Web, systèmes d'exploitation) • Nécessite une administration supérieure

Quelques organisations ont commencé à l'aide d'une approche hybride de leur architecture de PKI. Une approche hybride utilise une autorité de certification publique externe pour l'autorité de certification racine, et une hiérarchie d'autorité de certification interne pour la distribution des certificats. Les organisations ont l'avantage que les clients externes ont confiance en leurs certificats émis en interne, avec les avantages d'une autorité de certification interne. Le seul inconvénient à cette méthode est le coût. Une approche hybride est en général l'approche la plus chère, parce que les certificats publics pour des autorités de certification sont très chers.

Vous pouvez également choisir de déployer une PKI interne à des fins internes, comme le système de fichiers EFS et les signatures numériques. Pour les fins externes, comme la protection des serveurs Web ou de messagerie avec SSL, vous devez acheter un certificat public. Cette approche n'est pas très coûteuse et est probablement la solution la plus rentable.

Qu'est-ce qu'une hiérarchie de certification croisée ?

Pendant la certification croisée, dans la hiérarchie de certification croisée, l'AC racine de chaque hiérarchie d'AC fournit un certificat de certification croisée à l'AC racine de l'autre hiérarchie d'AC. L'autre AC racine de hiérarchie installe alors le certificat fourni. Ce faisant, l'approbation passe à toutes les AC secondaires sous le niveau d'installation du certificat de certification croisée.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avantages de la certification croisée

Une hiérarchie de certification croisée propose les avantages suivants :

- Permet l'interopérabilité entre entreprises et entre les produits de PKI
- Joint des PKI disparates
- Assume l'approbation complète d'une hiérarchie d'AC étrangère

Les sociétés déploient habituellement des certifications croisées pour établir une approbation mutuelle au niveau de la PKI, et pour implémenter également d'autres applications qui se basent sur la PKI, comme les services AD RMS (AD RMS).

Question : Votre société acquiert une autre société. Les deux sociétés exécutent leur propre PKI. Que pourriez-vous faire pour réduire le temps d'arrêt et continuer à fournir des services de PKI de manière transparente ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Déploiement d'autorités de certification

La première autorité de certification que vous installez sera une autorité de certification racine. Après l'installation de l'autorité de certification racine, vous pouvez éventuellement installer une autorité de certification secondaire pour appliquer des restrictions de stratégie et distribuer des certificats. Vous pouvez également utiliser un fichier CAPolicy.inf pour automatiser les installations supplémentaires d'autorité de certification et pour fournir les paramètres de configuration supplémentaires qui ne sont pas disponibles avec l'installation standard sur la base de l'interface utilisateur graphique. Dans ce cours, vous découvrirez le déploiement des AC dans l'environnement de Windows Server 2012.

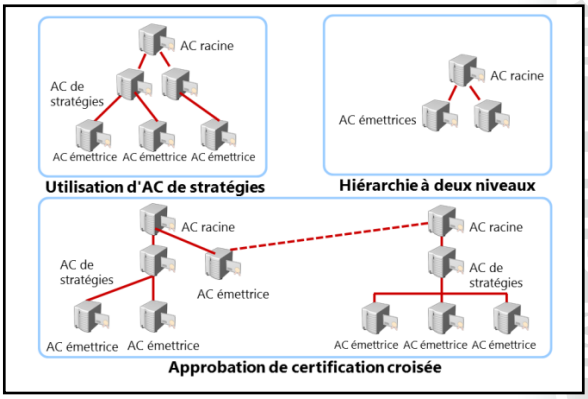
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options d'implémentation des hiérarchies d'AC ;
- expliquer les différences entre les autorités de certification autonomes et d'entreprise ;
- présenter les considérations relatives au déploiement d'une AC racine ;
- déployer une AC racine ;
- présenter les considérations relatives au déploiement d'une AC secondaire ;
- décrire l'utilisation du fichier CAPolicy.inf pour installer l'autorité de certification.

Options pour l'implémentation des hiérarchies d'AC

Quand vous décidez d'implémenter la PKI dans votre organisation, une des premières décisions que vous devez prendre est la procédure de conception de votre hiérarchie d'autorité de certification. La hiérarchie d'autorité de certification détermine la conception de base de votre PKI interne, ainsi que l'objectif de chaque autorité de certification dans la hiérarchie. Chaque hiérarchie d'autorité de certification comprend deux autorités de certification ou plus. Généralement, la deuxième autorité de certification (et toutes celles qui suivent) est déployée dans un objectif spécifique, parce que seule l'autorité de certification racine est obligatoire.

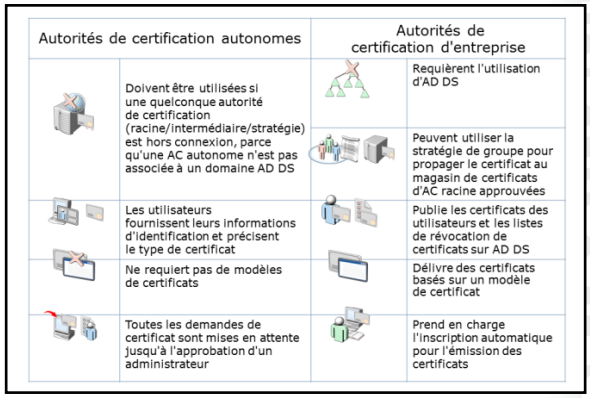


Les points suivants décrivent quelques scénarios d'implémentation d'une hiérarchie d'autorité de certification.

- Autorités de certification de stratégies. Les autorités de certification de stratégies sont un type d'autorité de certification secondaire directement en dessous de l'autorité de certification racine dans une hiérarchie d'autorité de certification. Vous utilisez des autorités de certification de stratégies pour émettre des certificats d'autorité de certification aux autorités de certification secondaires directement en dessous de l'autorité de certification de stratégies dans la hiérarchie. Utilisez les autorités de certification de stratégies quand les différents divisions, secteurs ou sites de votre organisation requièrent différentes stratégies et procédures d'émission.
- Approbation de certification croisée. Dans ce cas, deux hiérarchies d'autorité de certification indépendantes interagissent quand une autorité de certification dans une hiérarchie émet un certificat d'autorité de certification à une autorité de certification dans l'autre hiérarchie. Des approbations de certification croisée sont détaillées plus loin dans ce module.
- Hiérarchie à deux niveaux. Dans une hiérarchie à deux étages, il existe une autorité de certification racine et au moins une autorité de certification secondaire. Dans ce cas, l'autorité de certification secondaire est responsable des stratégies et de l'émission des certificats aux demandeurs.

CA autonomes et d'entreprise

Sous Windows Server 2012, vous pouvez déployer deux types d'autorités de certification : AC autonome et AC d'entreprise. Ces types ne concernent pas la hiérarchie, mais les fonctionnalités et le stockage de configuration. La différence la plus importante entre ces deux types d'AC est l'intégration et la dépendance d'Active Directory. Une autorité de certification autonome peut fonctionner sans AD DS, et n'en dépend pas. Une AC d'entreprise requiert AD DS, mais présente également plusieurs avantages, comme l'inscription automatique.



Le tableau suivant répertorie les différences principales entre une autorité de certification autonome et une autorité de certification d'entreprise.

Caractéristique	Autorité de certification autonome	Autorité de certification d'entreprise
Utilisation normale	Une autorité de certification autonome est en général utilisée pour des autorités de certification hors connexion, mais elle peut être utilisée pour une autorité de certification qui est uniformément disponible sur le réseau.	Une AC d'entreprise est en général utilisée pour émettre des certificats aux utilisateurs, aux ordinateurs et aux services, et n'est en général pas utilisée comme autorité de certification hors connexion.
Dépendances d'Active Directory	Une autorité de certification autonome ne dépend pas d'AD DS et peut être déployée dans des environnements non-Active Directory.	Une AC d'entreprise requiert AD DS, qui peut être utilisé comme base de données de configuration et d'inscription. Une AC d'entreprise constitue également un point de publication pour des certificats émis aux utilisateurs et aux ordinateurs.

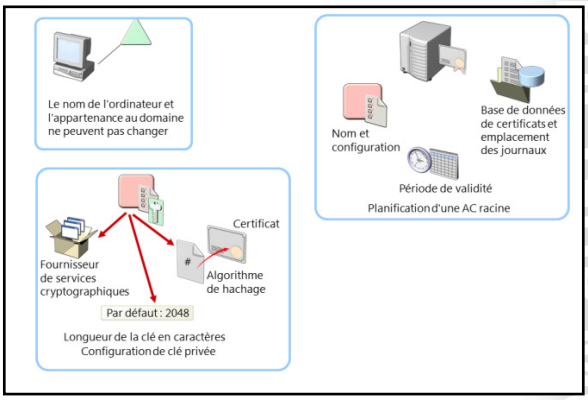
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Caractéristique	Autorité de certification autonome	Autorité de certification d'entreprise
Méthodes de demande de certificat	Les utilisateurs peuvent demander des certificats à une autorité de certification autonome uniquement à l'aide d'une inscription manuelle ou sur le Web.	• Les utilisateurs peuvent demander des certificats à une AC d'entreprise comme suit : • Inscription manuelle • Inscription via le Web • Inscription automatique • Agent d'inscription
Méthodes d'émission de certificat	Toutes les demandes doivent être approuvées manuellement par un administrateur de certificat.	Des demandes peuvent être automatiquement émises ou refusées, selon la liste de contrôle d'accès discrétionnaire (DACL) du modèle.

Généralement, l'autorité de certification racine (qui est la première autorité de certification déployée) est déployée en tant qu'autorité de certification autonome, et elle est mise hors connexion après l'émission d'un certificat pour elle-même et pour une autorité de certification secondaire. De plus, une autorité de certification secondaire est habituellement déployée comme une AC d'entreprise, et est configurée dans un des scénarios décrits dans la rubrique précédente.

Considérations relatives au déploiement d'une AC racine



Avant que vous ne déployiez une autorité de certification racine, plusieurs décisions doivent être prises. D'abord, vous devriez décider si vous déploierez une AC racine hors connexion. Sur la base de cette décision, vous déciderez également si vous déploierez une autorité de certification racine autonome ou une autorité de certification racine d'entreprise.

Habituellement, si vous déployez une hiérarchie d'autorité de certification à une seule couche, ce qui signifie que vous déployez seulement une autorité de certification, il n'est pas rare de choisir une AC racine d'entreprise. Toutefois, si vous déployez une hiérarchie à deux couches, le scénario le plus commun est le déploiement d'une autorité de certification racine autonome et d'une autorité de certification secondaire d'entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le facteur suivant à prendre en considération est le type d'installation du système d'exploitation. AD CS est pris en charge dans les scénarios d'installation complète et d'installation minimale. L'installation minimale offre une plus petite exposition aux attaques et moins de traitement administratif, et il faudrait donc en tenir compte pour AD CS dans un environnement d'entreprise. Sous Windows Server 2012, vous pouvez également utiliser Windows PowerShell pour déployer et gérer le rôle AD CS.

Vous devriez également être conscient du fait que vous ne pouvez pas modifier des noms d'ordinateur ou des appartenances au domaine d'ordinateur après le déploiement d'une autorité de certification de n'importe quel type sur cet ordinateur, et que vous ne pouvez pas modifier le nom de domaine. Par conséquent, il est important de déterminer ces attributs avant d'installer une autorité de certification.

Le tableau suivant détaille des considérations supplémentaires.

Considération	Description
Un fournisseur de services de chiffrement qui est utilisé pour générer une nouvelle clé	• Le fournisseur de services de chiffrement par défaut est le fournisseur de services cryptographiques renforcés Microsoft. • N'importe quel fournisseur dont le nom commence par un signe de numéro (#) est un fournisseur CNG.
Longueur de caractère de clé	La longueur de clé par défaut pour le fournisseur de services cryptographiques renforcés Microsoft est de 2 048 caractères. C'est la valeur minimale recommandée pour une autorité de certification racine.
L'algorithme de hachage est utilisé pour signer des certificats émis par une autorité de certification	La valeur par défaut de l'algorithme de hachage est SHA-1.
Période de validité des certificats émis par une autorité de certification	La valeur par défaut pour des certificats est de cinq ans.
L'état du serveur racine (en ligne ou hors connexion)	Le serveur racine devrait être déployé comme une autorité de certification hors connexion. Ceci améliore la sécurité et protège le certificat racine (parce qu'il n'est pas disponible pour attaquer sur le réseau).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Spécifiquement, si vous décidez de déployer une autorité de certification racine autonome hors connexion, il y a quelques considérations spécifiques à ne pas oublier :

- Avant que vous n'émettiez un certificat secondaire d'autorité de certification racine, assurez-vous que vous fournissiez au moins un emplacement de CDP et d'AIA qui sera à la disposition de tous les clients. En effet, par défaut, le CDP et l'AIA d'une autorité de certification racine autonome se trouve sur au même endroit. Par conséquent, quand vous mettez l'autorité de certification racine hors réseau, le test de vérification de révocation échoue car les emplacements de CDP et d'AIA sont inaccessibles. Quand vous définissez ces emplacements, vous devriez copier manuellement les informations de liste de révocation de certificats et d'AIA à cet emplacement.
- Définissez une période de validité pour les listes de révocation de certificats que l'autorité de certification racine publie pour une longue période (par exemple, un an). Ceci signifie que vous devrez activer l'autorité de certification racine une fois par an pour publier une nouvelle liste de révocation de certificats, puis la copier à un emplacement qui est à la disposition des clients. Sinon, après l'expiration de la liste de révocation de certificats de l'AC racine, le test de vérification de révocation pour tous les certificats échoue également.
- Utilisez la stratégie de groupe pour publier le certificat d'AC racine dans un magasin Autorité de certification racine de confiance sur tous les serveurs et les ordinateurs clients. Vous devez le faire manuellement, parce qu'une autorité de certification autonome ne peut pas le faire automatiquement, à la différence d'une AC d'entreprise. Vous pouvez également publier le certificat d'AC racine sur Active Directory DS à l'aide de l'outil de ligne de commande **Certutil**.

Démonstration : Déploiement d'une AC racine

Au cours de cette démonstration, vous allez apprendre à déployer une AC racine d'entreprise.

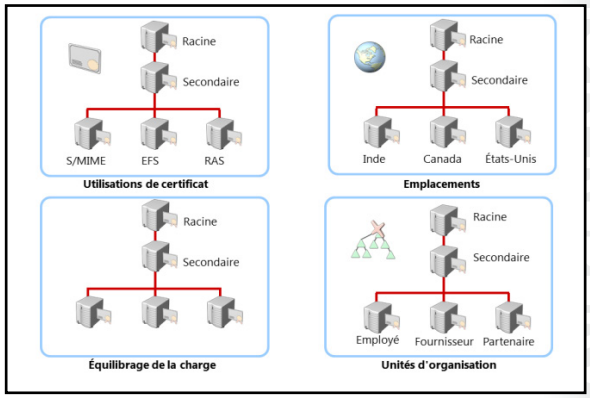
Procédure de démonstration

Déploiement d'une AC racine

1. Dans le Gestionnaire de serveur, ajoutez le rôle **Active Directory Certificate Services**.
2. Sélectionnez le service de rôle **Autorité de certification**.
3. Après la réussite de l'installation, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
4. Sélectionnez pour installer **AC racine d'entreprise**.
5. Définissez la longueur de clé sur **4 096**.
6. Donnez à l'AC le nom **AdatumRootCA**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Considérations relatives au déploiement d'une AC secondaire



Vous pouvez utiliser une autorité de certification secondaire pour implémenter des restrictions de stratégie pour la PKI, et pour distribuer des certificats aux clients. Après l'installation d'une autorité de certification racine pour l'organisation, vous pouvez installer une ou plusieurs autorités de certification secondaires.

Quand vous utilisez une autorité de certification secondaire pour distribuer des certificats aux utilisateurs ou aux ordinateurs qui ont un compte dans un environnement AD DS, vous pouvez installer l'autorité de certification secondaire comme AC d'entreprise. Puis, vous pouvez utiliser les données des comptes clients dans AD DS pour distribuer et gérer des certificats et pour publier des certificats dans AD DS. Toutefois, pour terminer cette procédure, vous devez être membre du groupe local Administrateurs ou avoir des autorisations équivalentes. Si l'autorité de certification secondaire sera une AC d'entreprise, vous devez également être membre du groupe Admins du domaine ou avoir des autorisations équivalentes. Du point de vue de la sécurité, un scénario recommandé serait d'avoir une autorité de certification racine autonome hors connexion et une autorité de certification secondaire d'entreprise.

Une autorité de certification secondaire est habituellement déployée pour accomplir certaines des fonctionnalités suivantes :

- Utilisation. Vous pouvez émettre des certificats pour un certain nombre d'objets, tels que S/MIME (Secure Multipurpose Internet Mail Extensions), le système de fichiers EFS ou le service d'accès à distance (RAS). Les stratégies d'émission quant à ces utilisations peuvent être distinctes et la séparation constitue une base pour administrer ces stratégies.
- Divisions d'organisation. Il peut y avoir différentes stratégies d'émission de certificats, selon le rôle d'une entité dans l'organisation. Vous pouvez créer des autorités de certification secondaires pour séparer et administrer ces stratégies.
- Divisions géographiques. Les organisations ont souvent des entités sur plusieurs sites physiques. La connectivité réseau limitée entre ces sites peut nécessiter des autorités de certification secondaires individuelles pour beaucoup de ces sites ou pour tous.
- Équilibrage de la charge. Si vous allez utiliser votre PKI pour émettre et gérer un grand nombre de certificats, avoir une seule autorité de certification peut avoir comme conséquence la charge du réseau considérable pour cette autorité de certification unique. L'utilisation de plusieurs autorités de certification secondaires pour émettre le même genre de certificats divise la charge du réseau entre les autorités de certification.
- Sauvegarde et tolérance de panne. Le fait de disposer de plusieurs autorités de certification augmente la possibilité pour votre réseau de disposer en permanence d'autorités de certification opérationnelles pour répondre aux demandes des utilisateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure d'utilisation du fichier CAPolicy.inf pour l'installation

Le fichier CAPolicy.inf est enregistré dans le dossier %Windir% de l'AC racine ou secondaire. Ce fichier définit ce qui suit

- CPS
- Identificateur d'objet
- Intervalles de publication de la liste CRL
- Paramètres de renouvellement de l'autorité de certification
- Taille de clé
- Période de validité des certificats
- Chemins d'accès CDP et AIA

Si vous souhaitez déployer une AC racine ou secondaire, et si vous souhaitez prédéfinir quelques valeurs à utiliser pendant l'installation et définir des paramètres supplémentaires, vous pouvez utiliser le fichier CAPolicy.inf pour effectuer cette procédure. Le fichier CAPolicy.inf est un fichier de texte en clair qui contient les différents paramètres qui sont utilisés lors de l'installation du rôle AD CS ou du renouvellement du certificat d'AC. Le fichier CAPolicy.inf n'est pas obligatoire pour installer AD CS, mais sans lui, les paramètres par défaut seront appliqués, et dans de nombreux cas, les paramètres par défaut sont insuffisants. Vous pouvez utiliser le fichier CAPolicy.inf pour configurer des autorités de certification dans des déploiements plus compliqués.

Chaque fichier CAPolicy.inf est divisé en sections et a une structure simple, qui peut être décrite comme suit :

- Une *section* est une zone dans le fichier .inf qui contient un groupe logique de clés. Une section s'affiche toujours entre parenthèses dans le fichier .inf.
- Une *clé* est le paramètre qui est à la gauche du signe égal (=).
- Une *valeur* est le paramètre qui est à la droite du signe égal (=).

Par exemple, si vous souhaitez spécifier un point d'accès de l'information d'autorité dans le fichier CAPolicy.inf, vous utiliserez la syntaxe suivante :

```
 [AuthorityInformationAccess]
URL=http://pki.adatum.com/CertData/adatumCA.crt
```

Dans cet exemple, AuthorityInformationAccess est une section, l'URL est la clé et **http://pki.adatum.com/CertData/adatumCA.crt** est la valeur.

Vous pouvez également spécifier quelques paramètres de serveur d'autorité de certification dans le fichier CAPolicy.inf. Un exemple de la section qui spécifie ces paramètres est :

```
 [certsrv_server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=Days
CRLPeriodUnits=2
CRLDeltaPeriod=Hours
CRLDeltaPeriodUnits=4
ClockSkewMinutes=20
LoadDefaultTemplates=True
AlternateSignatureAlgorithm=0
ForceUTF8=0
EnableKeyCounting=0
```

Remarque : Tous les paramètres des exemples précédents sont facultatifs.

Vous pouvez également utiliser le fichier CAPolicy.inf lors de l'installation d'AD CS pour définir ce qui suit :

- Déclaration CPS (Certification Practice Statement) : Décrit les méthodes utilisées par l'autorité de certification pour émettre des certificats. Ceci comprend les types des certificats émis, des informations sur l'émission, le remplacement et la récupération des certificats, et d'autres détails sur la configuration de l'autorité de certification.
- Identificateur d'objet (OID) : Identifie un objet ou un attribut spécifique.
- Intervalles de publication de la liste CRL : Définit l'intervalle entre les publications pour la liste de révocation de certificats de base.
- Paramètres de renouvellement de l'autorité de certification : Définit des paramètres de renouvellement comme suit :
    - Taille de clé : Définit la longueur de la paire de clés utilisée pendant le renouvellement de l'autorité de certification racine.
    - Période de validité des certificats : Définit la période de validité d'un certificat d'une AC racine.
    - Chemins d'accès CDP et AIA : Fournit le chemin d'accès utilisé pour des installations et des renouvellements d'autorité de certification racine.

Une fois que vous avez créé votre fichier CAPolicy.inf, vous devez le copier dans le dossier %systemroot% de votre serveur (par exemple C:\Windows) avant d'installer le rôle AD CS ou avant de remplacer le certificat d'AC.

 **Remarque :** Le fichier CAPolicy.inf est traité pour les installations et les renouvellements d'AC racine et secondaire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique A : Déploiement et configuration de la hiérarchie d'autorités de certification

Scénario

Alors que la société A. Datum Corporation s'est développée, ses besoins de sécurité ont également augmenté. Le département sécurité est particulièrement intéressé par l'activation d'un accès sécurisé aux sites Web critiques et par la fourniture d'une sécurité supplémentaire pour des fonctionnalités. Pour faire face à ces exigences de sécurité, A. Datum a décidé d'implémenter une PKI à l'aide du rôle AD CS sous Windows Server 2012.

En tant que l'un des principaux administrateurs réseau chez A. Datum, vous êtes chargé de l'implémentation du déploiement d'AD CS.

Objectifs

- Déployer une AC racine autonome
- Déployer une AC secondaire d'entreprise

Configuration de l'atelier pratique

Durée approximative : 50 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-SVR2** **22412B-LON-CA1** **22412B-LON-CL1**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-SVR2**, **22412B**-**LON-CA1** et **22412B**-**LON-CL1**. Ne vous connectez pas avant d'être invité à le faire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Déploiement d'une AC racine autonome

Scénario

A. Datum souhaite commencer à utiliser des certificats à différentes fins. Vous devez installer l'infrastructure d'AC appropriée. Étant donné qu'ils utilisent Windows Server 2012 AD DS, vous avez décidé d'implémenter le rôle AD CS. Quand vous passiez en revue les conceptions possibles, vous avez décidé d'implémenter une AC racine autonome. Cette AC sera mise hors connexion après la publication d'un certificat pour une AC secondaire.

Les tâches principales de cet exercice sont les suivantes :

1. Installez le rôle serveur Active Directory® Certificate Services (AD CS) sur un serveur non joint au domaine
2. Configuration d'un nouvel emplacement de révocation de certificat
3. Création d'un enregistrement d'hôte DNS pour LON-CA1 et configuration du partage

▶ Tâche 1 : Installez le rôle serveur Active Directory® Certificate Services (AD CS) sur un serveur non joint au domaine

1. Connectez-vous à **LON-CA1** comme **Administrateur** à l'aide du mot de passe **Pa$$w0rd**.
2. L'Assistant Ajouter des rôles et des fonctionnalités permet d'installer le rôle **Services de certificats Active Directory**.
3. Après la réussite de l'installation, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination.**
4. Configurez le rôle AD CS comme une AC racine autonome. Appelez-la **AdatumRootCA**.
5. Définissez la longueur de clé sur **4 096**, acceptez toutes autres valeurs en tant que valeurs par défaut.

▶ Tâche 2 : Configuration d'un nouvel emplacement de révocation de certificat

1. Dans LON-CA1, ouvrez la console **Autorité de certification**.
2. Ouvrez la boîte de dialogue **Propriétés** pour **AdatumRootCA**.
3. Configurez de nouveaux emplacements pour CDP : **http://lon-svr1.adatum.com/CertData/<NomAutoritéCertification><CRLNameSuffix><ListeRévocationCertificatsDeltaAutorisée>.crl**.
4. Sélectionnez les options suivantes
   - **Inclure dans l'extension CDP des certificats émis**
   - **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta**
5. Configurez les nouveaux emplacements pour AIA sur **http://lon-svr1.adatum.com/CertData/*<Nom du Serveur DNS>*_*<NomAutoritéCertification>*<*NomCertificat*>.crt**

 **Remarque :** Assurez-vous que des emplacements pour le CDP et l'AIA sont entrés exactement comme écrit ici.

6. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**.
7. Publiez la liste de révocation de certificats sur LON-CA1.
8. Exportez le certificat d'AC racine et copiez le fichier .cer dans **\\lon-svr1\C$**.
9. Copiez le contenu du dossier **C:\Windows\System32\CertSrv\CertEnroll** sur **\\lon-svr1\C$**.

▶ Tâche 3 : Création d'un enregistrement d'hôte DNS pour LON-CA1 et configuration du partage

1. Sur LON-DC1, ouvrez la console du **Gestionnaire DNS**.
2. Créez l'enregistrement d'hôte pour la machine LON-CA1 dans la zone de recherche directe d'Adatum.com.
3. Utilisez l'adresse IP **172.16.0.40** pour l'enregistrement d'hôte LON-CA1.
4. Dans la machine LON-CA1, activez le partage de fichiers et d'imprimantes sur les réseaux d'invité et publics.

Résultats : À la fin de cet exercice, vous aurez déployé une AC autonome racine.

Exercice 2 : Déploiement d'une AC secondaire d'entreprise

Scénario

Après le déploiement de l'autorité de certification racine autonome, l'étape suivante est le déploiement d'une AC secondaire d'entreprise. A. Datum souhaite utiliser une autorité de certification secondaire d'entreprise pour utiliser l'intégration d'AD DS. En outre, étant donné que l'autorité de certification racine est autonome, vous souhaitez publier son certificat pour tous les clients.

Les tâches principales de cet exercice sont les suivantes :

1. Installation et configuration d'AD CS sur LON-SVR1
2. Installation d'un certificat d'autorité de certification secondaire
3. Publication du certificat d'AC racine via la stratégie de groupe

▶ Tâche 1 : Installation et configuration d'AD CS sur LON-SVR1

1. Ouvrez une session sur **LON-SVR1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Installez le rôle **Services de certificats Active Directory** sur **LON-SVR1**. Incluez les services de rôle **Autorité de certification** et **Inscription de l'autorité de certification via le Web**.
3. Après l'installation, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
4. Sélectionnez les services de rôle **Autorité de certification** et **Inscription de l'autorité de certification via le Web**.
5. Configurez **LON-SVR1** comme une **AC d'entreprise**.
6. Configurez le type d'autorité de certification comme une **Autorité de certification secondaire**.
7. Pour le **Nom de l'autorité de certification**, tapez **Adatum-IssuingCA**.
8. Enregistrez le fichier de demande sur le disque local.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Installation d'un certificat d'autorité de certification secondaire

1. Sur LON-SVR1, installez le certificat **RootCA.cer** dans le magasin Autorité de certification racine de confiance.
2. Accédez au disque local (C:) et copiez les fichiers **AdatumRootCA.crl** et **LON-CA1 _AdatumRootCA.crt** sur **C:\inetpub\wwwroot\CertData**.
3. Copiez le fichier de demande **LON-SVR1.Adatum.com_Adatum- IssuingCA.req** sur **\\lon-ca1\C$**.
4. Basculez vers **LON-CA1**.
5. Depuis la console Autorité de certification sur LON-CA1, envoyez une nouvelle demande de certificat à l'aide du fichier .req que vous avez copié à l'étape 3.
6. Émettez le certificat et exportez-le au format p7b avec la chaîne complète. Enregistrez le fichier sous **\\lon-svr1\C$\SubCA.p7b**.
7. Basculez vers **LON-SVR1**.
8. Installez le certificat d'AC secondaire sur LON-SVR1 à l'aide de la console Autorité de certification.
9. Démarrez le service.

▶ Tâche 3 : Publication du certificat d'AC racine via la stratégie de groupe

1. Dans LON-DC1, depuis le Gestionnaire de serveur, ouvrez la **Console de gestion des stratégies de groupe**.
2. Modifiez **Default Domain Policy**.
3. Publiez le fichier **RootCA.cer** depuis **\\lon-svr1\C$** dans le magasin d'autorités de certification racines de confiance, qui se trouve dans Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégie de clé publique.

Résultats : Après avoir terminé cet exercice, vous aurez déployé et configuré une AC secondaire d'entreprise.

▶ Tâche 4 : Pour préparer l'atelier suivant

- Laisser tous les ordinateurs virtuels en fonctionnement pour l'atelier suivant. N'éteignez aucun ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Déploiement et gestion des modèles de certificats

Les modèles de certificats définissent la manière dont un certificat peut être demandé et son utilisation. Les modèles sont configurés dans l'AC et enregistrés dans la base de données Active Directory. Il existe différentes versions des modèles : l'AC d'entreprise Windows 2000 Server prend en charge la version 1 des modèles de certificats. Windows Server 2003 Enterprise Edition prend en charge les versions 1 et 2 des modèles et Windows Server 2008 Enterprise Edition prend en charge les versions 1, 2 et 3 des modèles de certificats. Windows Server 2012 propose la version 4 des modèles, mais prend toujours en charge les trois versions précédentes.

Deux types de catégories de modèle de certificat sont les utilisateurs et les ordinateurs, et chaque type de catégorie peut être utilisée à diverses fins. Vous pouvez attribuer les autorisations **Contrôle total**, **Lecture**, **Écriture**, **Inscription** et **Inscription automatique** aux modèles de certificats. Vous pouvez également mettre à jour des modèles de certificats en modifiant le modèle de certificat original, en copiant un modèle ou en remplaçant des modèles de certificats existants. Dans ce cours, vous apprendrez à gérer et déployer les modèles de certificats.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les modèles de certificats ;
- décrire les versions de modèle de certificat dans Windows Server 2012 ;
- configurer des autorisations de modèle de certificat ;
- configurer des paramètres de modèle de certificat ;
- décrire les options pour la mise à jour d'un modèle de certificat ;
- expliquer comment modifier et activer un modèle de certificat.

Que sont les modèles de certificats ?

Les modèles de certificats permettent aux administrateurs de personnaliser le méthode de distribution des certificats, de définir les objectifs des certificats et de mandater le type d'utilisation autorisée par un certificat. Les administrateurs peuvent créer des modèles, puis les déployer rapidement au niveau de l'entreprise à l'aide des utilitaires de gestion de ligne de commande ou d'interface graphique utilisateur intégrés.

Les modèles de certificats définissent

- Le format et le contenu d'un certificat
- Le processus de création et d'envoi d'une demande de certificat valide
- Les principes de sécurité autorisés pour lire, inscrire ou utiliser Autoenroll pour un certificat qui sera basé sur le modèle
- Les autorisations requises pour modifier un modèle de certificat

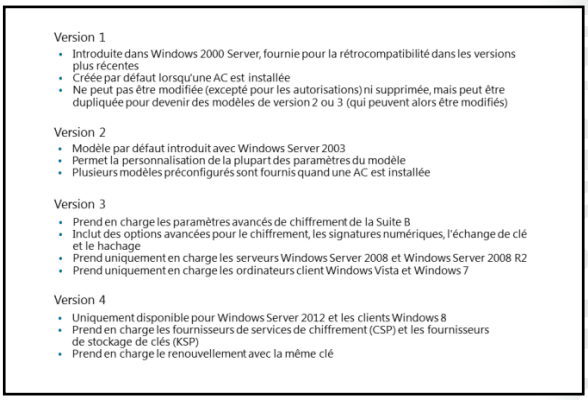
La liste DACL, associée à chaque modèle de certificat, définit quelles entités de la sécurité disposent des autorisations de lecture et de configuration du modèle, ainsi que d'inscription ou d'inscription automatique pour les certificats en fonction du modèle. Les modèles de certificats et leurs autorisations sont définies dans AD DS et valides au sein de la forêt. Si plusieurs AC d'entreprise sont exécutées dans la forêt Active Directory, les modifications apportées à l'autorisation auront un effet sur toutes les AC.

Lorsque vous définissez un modèle de certificat, cette définition doit être disponible pour toutes les AC de la forêt. Pour ce faire, enregistrez les informations sur le modèle de certificat dans le contexte d'appellation Configuration, où CN=Configuration et DC=ForestRootName. La réplication de ces informations dépend du calendrier de réplication d'Active Directory et le modèle de certificat peut ne pas être disponible pour toutes les AC avant la fin de la réplication. Le stockage et la réplication sont effectués automatiquement.

Remarque : Avant Windows Server 2008 R2, seules les éditions Entreprise de Windows Server prenaient en charge la gestion des modèles de certificats. Sous Windows Server 2008 R2 et Windows Server 2012, vous pouvez également gérer des modèles de certificats dans les éditions Standard.

Versions de modèle de certificat dans Windows Server 2012

L'AC dans l'autorité de certification Windows Server 2012 prend en charge quatre versions des modèles de certificats. Les versions 1, 2 et 3 des modèles de certificats proviennent de versions précédentes de Windows Server, alors que la version 4 est une nouveauté de Windows Server 2012.



Les versions de modèle de certificat correspondent à la version du système d'exploitation Windows Server. Windows 2000 Server, Windows Server 2003, Windows Server 2008 et Windows Server 2012 correspondent à la version 1, à la version 2, à la version 3 et à la version 4 respectivement.

En plus de correspondre aux versions du système d'exploitation Windows Server, les versions du modèle de certificat présentent également des différences fonctionnelles, comme suit :

- Le système d'exploitation Windows 2000 Advanced Server prend en charge la version 1 des modèles de certificats. La seule modification autorisée aux modèles de version 1 est le changement des autorisations pour autoriser ou interdire l'inscription du modèle de certificat. Lorsque vous installez une AC d'entreprise, des modèles de certificats version 1 sont créés par défaut. Depuis le 13 juillet 2010, Windows 2000 Server n'est plus pris en charge par Microsoft.
- Les systèmes d'exploitation Windows Server 2003 Enterprise Edition prennent en charge la version 1 et la version 2 des modèles. Vous pouvez personnaliser plusieurs paramètres dans les modèles de version 2. L'installation par défaut fournit quelques modèles préconfigurés de version 2. Vous pouvez ajouter des modèles de version 2 en fonction des besoins de votre organisation. Sinon, vous pouvez dupliquer un modèle de certificat de version 1 pour créer une nouvelle version 2 du modèle. Vous pouvez ensuite modifier et sécuriser le modèle de certificat de version 2 récemment créé. Lorsque de nouveaux modèles sont ajoutés à une AC d'entreprise Windows Server 2003, il s'agit par défaut de la version 2.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Les systèmes d'exploitation Windows Server 2008 Enterprise prennent en charge les nouveaux modèles de certificats de version 3. De plus, ils prennent en charge les versions 1 et 2. Les modèles de certificats de version 3 prennent en charge plusieurs fonctionnalités d'une AC d'entreprise Windows Server 2008, comme CNG. CNG prend en charge des algorithmes chiffrés Suite B comme le chiffrement courbe elliptique (ECC). Dans Windows Server 2008 Enterprise, vous pouvez dupliquer des modèles de versions 1 et 2 par défaut pour les mettre à niveau vers la version 3.

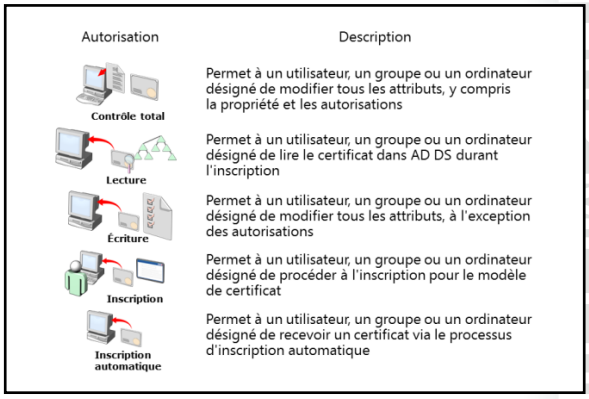
  Windows Server 2008 propose par défaut deux nouveaux modèles de certificats : authentification Kerberos et signature de réponse OCSP. Le système d'exploitation Windows Server 2008 R2 pouvait également prendre en charge des modèles de certificats. Lorsque vous utilisez des modèles de certificats de version 3, vous pouvez utiliser le chiffrement CNG et des algorithmes de hachage pour les demandes de certificat, les certificats émis et la protection des clés privées pour l'échange et l'archivage des clés.

- Les systèmes d'exploitation Windows Server 2012 prennent en charge les modèles de certificats de version 4 et toutes les autres versions des éditions antérieures de Windows Server. Ces modèles de certificats sont disponibles uniquement sous Windows Server 2012 et Windows 8. Pour permettre aux administrateurs de distinguer les fonctionnalités prises en charge par une version de système d'exploitation spécifique, l'onglet **Compatibilité** a été ajouté à l'onglet **Propriétés** du modèle de certificat. Il liste les options non disponibles dans les propriétés de modèle de certificat, en fonction des versions de système d'exploitation sélectionnées du client de certificat et de l'AC. Les modèles de certificats de version 4 prennent également en charge les CSP et les KSP. Ils peuvent également être configurés de manière à demander le renouvellement avec une même clé.

La mise à niveau des modèles de certificats est un processus qui s'applique uniquement lorsque l'AC a été mise à niveau de Windows Server 2008 ou 2008 R2 vers Windows Server 2012. Après la mise à niveau, vous pouvez mettre à niveau les modèles de certificats en démarrant la console du Gestionnaire d'AC et en cliquant sur **Oui** à l'invite de mise à jour.

Configuration des autorisations de modèle de certificat

Pour configurer des autorisations de modèle de certificat, vous devez définir la liste DACL sous l'onglet **Sécurité** pour chaque modèle de certificat. Les autorisations attribuées à un modèle de certificat définiront quels utilisateurs ou groupes peuvent lire, modifier, inscrire ou inscrire automatiquement ce modèle de certificat.



Vous pouvez attribuer les autorisations suivantes aux modèles de certificats :

- **Contrôle total**. L'autorisation **Contrôle total** permet à une entité de sécurité de modifier tous les attributs d'un modèle de certificat, notamment les autorisations pour le modèle de certificat lui-même. Il s'agit également de l'autorisation de modifier le descripteur de sécurité du modèle de certificat.

- **Lecture**. L'autorisation **Lecture** permet à un utilisateur ou un ordinateur d'afficher le modèle de certificat lors de l'inscription des certificats. L'autorisation **Lecture** est également requise par le serveur de certificat pour trouver les modèles de certificats dans AD DS.

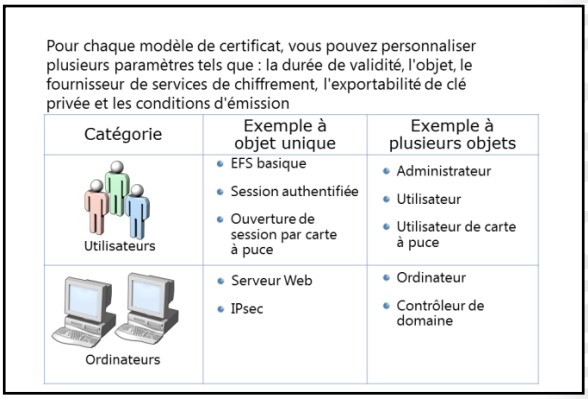
- **Écriture**. L'autorisation **Écriture** permet à un utilisateur ou un ordinateur de modifier les attributs d'un modèle de certificat, notamment les autorisations attribuées au modèle de certificat lui-même.
- **Inscription**. L'autorisation **Inscription** permet à un utilisateur ou un ordinateur d'inscrire un certificat sur la base du modèle de certificat. Toutefois, pour inscrire un certificat, vous devez disposer également de l'autorisation **Lecture** pour le modèle de certificat.
- **Inscription automatique**. L'autorisation **Inscription automatique** permet à un utilisateur ou un ordinateur de recevoir un certificat via le processus d'inscription automatique. Toutefois, l'autorisation **Inscription automatique** nécessite que l'utilisateur ou l'ordinateur dispose des autorisations de **Lecture** et d'**Inscription** pour un modèle de certificat.

Dans le cadre des meilleures pratiques, vous devez attribuer des autorisations de modèle de certificat uniquement à des groupes généraux ou universels. Ceci est dû au fait que les objets de modèle de certificat sont enregistrés dans le contexte d'appellation de configuration dans AD DS. Vous ne pouvez pas attribuer des autorisations à l'aide de groupes locaux de domaines situés dans un domaine Active Directory. Vous ne devez jamais attribuer des autorisations de modèle de certificat à des utilisateurs ou des ordinateurs individuels.

Dans le cadre des meilleures pratiques, l'autorisation de **Lecture** doit toujours être attribuée au groupe d'utilisateurs authentifiés. L'attribution de cette autorisation permet à tous les utilisateurs et ordinateurs d'afficher les modèles de certificats dans AD DS. L'attribution de cette autorisation permet également à l'AC exécutée dans le contexte Système d'un ordinateur d'afficher les modèles de certificats lors de l'attribution de certificats.

Configuration des paramètres de modèle de certificat

Outre la configuration des paramètres de sécurité pour les modèles de certificats, vous pouvez également configurer plusieurs autres paramètres pour chaque modèle. Toutefois, sachez que le nombre d'options configurables dépend de la version du modèle de certificat. Par exemple, des modèles de certificats de version 1 ne permettent pas de modifier d'autres paramètres que ceux liés à la sécurité, alors que des modèles de certificats d'une version supérieure vous permettent de configurer la plupart des options disponibles.



Windows Server 2012 propose plusieurs modèles de certificats par défaut pour la signature du code (pour les logiciels de signature numérique), le système EFS (pour le chiffrement de données) et la capacité des utilisateurs de se connecter à l'aide d'une carte à puce. Pour personnaliser un modèle pour votre société, dupliquez le modèle, puis modifiez la configuration du certificat.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Par exemple, vous pouvez configurer les éléments suivants :

- format et contenu d'un certificat sur la base de l'utilisation prévue du certificat ;

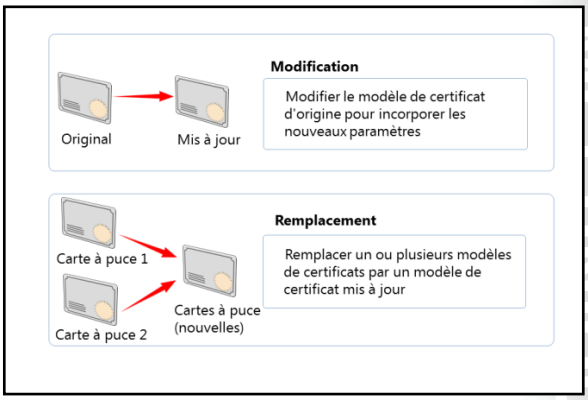
Remarque : L'utilisation prévue d'un certificat peut être associée à des utilisateurs ou des ordinateurs, en fonction des types d'implémentations de sécurité requis pour utiliser la PKI.

- Processus de création et d'envoi d'une demande de certificat valide
- CSP pris en charge
- Longueur de clé
- Période de validité
- Processus d'inscription ou conditions d'inscription

Vous pouvez également définir l'objectif du certificat dans les paramètres du certificat. Les modèles de certificats peuvent avoir les objectifs suivants :

- Usage unique. Un certificat à usage unique a un seul objectif, comme autoriser les utilisateurs à ouvrir une session à l'aide d'une carte à puce. Les organisations utilisent les certificats à usage unique lorsque la configuration du certificat diffère des autres certificats déployés. Par exemple, si tous les utilisateurs vont recevoir un certificat pour les ouvertures de session par carte à puce mais si seuls quelques groupes recevront un certificat pour le système EFS, les organisations conservent généralement ces certificats et modèles distincts pour s'assurer que les utilisateurs reçoivent uniquement les certificats requis.
- Usages multiples. Un certificat à usage multiple a plusieurs objectifs (souvent distincts) simultanément. Alors que certains modèles (comme le modèle Utilisateur) ont plusieurs objectifs par défaut, les organisations modifient souvent les modèles pour qu'ils répondent à des objectifs supplémentaires. Par exemple, si une société tente de publier des certificats pour trois objets, ces objets peuvent être combinés en un modèle de certificat unique pour soulager le travail administratif et la maintenance.

Options de mise à jour d'un modèle de certificat



La hiérarchie d'autorité de certification dans la plupart des organisations a un modèle de certificat pour chaque fonction. Par exemple, il peut y avoir un modèle de certificat pour le chiffrement de fichier et autre pour la signature de code. En outre, il peut y avoir quelques modèles qui couvrent des fonctions pour la plupart des groupes de la plupart des groupes de sujets.

En tant qu'administrateur informatique, il est possible que vous deviez modifier un modèle de certificat existant en raison des paramètres incorrects ou d'autres problèmes dans le modèle de certificat original. Il est également possible que vous deviez fusionner plusieurs modèles de certificats existants dans un modèle de unique.

Vous pouvez mettre à jour un modèle de certificat en modifiant le modèle ou en remplaçant le modèle existant :

- Modification du modèle de certificat d'origine. Pour modifier un modèle de certificat de version 2, 3 ou 4, vous devez apporter des modifications, puis les appliquer à ce modèle. Une fois les modifications apportées, tout certificat émis par une autorité de certification basé sur ce modèle de certificat inclura les modifications que vous avez apportées.
- Remplacement de modèles de certificats existants. La hiérarchie d'autorité de certification d'une organisation peut avoir plusieurs modèles de certificats qui propose la même fonctionnalité ou une fonctionnalité similaire. Dans ce cas, vous pouvez remplacer plusieurs modèles de certificats à l'aide d'un modèle de certificat unique. Pour cela, dans la console Modèles de certificats, vous pouvez désigner un nouveau modèle de certificat qui remplace les modèles de certificats existants.

Démonstration : Modification et activation d'un modèle de certificat

Dans cette démonstration, vous verrez comment modifier et activer un modèle de certificat.

Procédure de démonstration

Modifier et activer un modèle de certificat

1. Sur LON-SVR1, ouvrez la console **Modèles de certificats**.
2. Passez en revue la liste des modèles disponibles.
3. Ouvrez les **Propriétés** du modèle de certificat **IPsec**, et passez en revue les paramètres disponibles.
4. Dupliquez le modèle de certificat **Utilisateur Exchange**. Nommez-le **Exchange User Test1**, puis configurez-le pour remplacer le modèle **Utilisateur Exchange**.
5. Permettez aux utilisateurs authentifiés de s'inscrire pour le modèle **Exchange User Test1**.
6. Publiez le modèle sur LON-SVR1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Implémentation de la distribution et de la révocation de certificats

L'une des étapes du déploiement de la PKI dans votre organisation sera la définition des méthodes pour la distribution et l'inscription des certificats. En outre, pendant le processus de gestion de certificat, vous devriez parfois révoquer des certificats. Les raisons de la révocation de certificats sont notamment une clé compromise ou une personne quittant l'organisation. Vous devez vérifier que les clients réseau peuvent déterminer quels certificats sont révoqués avant d'accepter des demandes d'authentification. Pour vérifier l'évolutivité et la haute disponibilité, vous pouvez déployer le répondeur en ligne d'AD CS, qui fournit l'état de révocation des certificats. Dans ce cours, vous découvrirez des méthodes pour la distribution et la révocation des certificats.

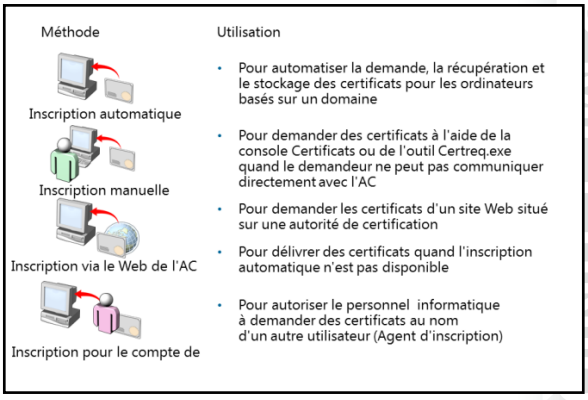
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options pour l'inscription de certificat ;
- décrire le fonctionnement de l'inscription automatique ;
- décrire l'agent d'inscription restreint ;
- expliquer la procédure de configuration de l'agent d'inscription restreint ;
- décrire le service d'inscription de périphériques réseau ;
- expliquer le fonctionnement de la révocation des certificats ;
- décrire les considérations relatives à la publication d'AIA et de CDP ;
- décrire un répondeur en ligne ;
- configurer le répondeur en ligne.

Options d'inscription de certificat

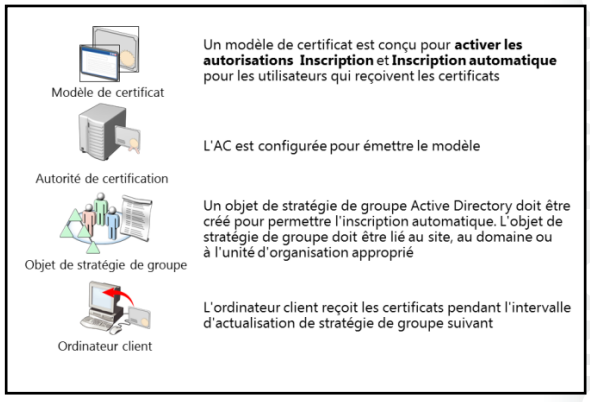
Sous Windows Server 2012, vous pouvez utiliser plusieurs méthodes pour inscrire un certificat d'ordinateur ou d'utilisateur. L'utilisation de ces méthodes varie en fonction des scénarios. Par exemple, vous utiliserez très probablement l'inscription automatique pour déployer en masse des certificats sur un grand nombre d'utilisateurs ou d'ordinateurs, alors que vous utiliserez très probablement l'inscription manuelle pour des certificats consacrés aux entités de sécurité spécifiques.



La liste suivante décrit les différentes méthodes d'inscription, et quand les utiliser :

- Inscription automatique. À l'aide de cette méthode, l'administrateur définit les autorisations et la configuration d'un modèle de certificat. Ces définitions permettent au demandeur de demander, de récupérer et de remplacer des certificats automatiquement sans interaction de l'utilisateur final. Cette méthode est utilisée pour des ordinateurs de domaine AD DS. Le certificat doit être configuré pour l'inscription automatique par la stratégie de groupe.
- Inscription manuelle. À l'aide de cette méthode, la clé privée et une demande de certificat sont générées sur un périphérique, tel qu'un service Web ou un ordinateur. La demande de certificat est ensuite transmise à l'autorité de certification pour générer le certificat faisant l'objet de la demande. Le certificat est ensuite rapatrié sur le périphérique en vue de son installation. Utilisez cette méthode lorsque le demandeur ne peut pas communiquer directement avec l'autorité de certification ou lorsque le périphérique ne prend pas en charge l'inscription automatique.
- Inscription via le Web de l'AC. À l'aide de cette méthode, vous pouvez activer une autorité de certification de site Web de sorte que les utilisateurs puissent obtenir des certificats. Pour utiliser l'inscription via le Web de l'AC, vous devez installer les services Internet (IIS) et le rôle de l'inscription via le Web sur l'autorité de certification d'AD CS. Pour obtenir un certificat, le demandeur ouvre une session sur le site Web, choisit le modèle de certificat approprié et envoie une demande. Si l'utilisateur a les autorisations appropriées pour s'inscrire pour le certificat, le certificat est émis automatiquement. La méthode d'inscription via le Web de l'autorité de certification devrait être utilisée pour délivrer des certificats quand l'inscription automatique ne peut pas être utilisée. Ceci peut se produire dans le cas d'une demande de certificat avancée. Cependant, dans certains cas, l'inscription automatique peut être utilisée pour certains certificats, mais pas pour tous les certificats.
- Inscription au nom (agent d'inscription). À l'aide de cette méthode, un administrateur d'autorité de certification crée un compte d'agent d'inscription pour un utilisateur. L'utilisateur avec des droits d'agent d'inscription peut alors s'inscrire pour des certificats au nom d'autres utilisateurs. Vous utiliseriez cette méthode, par exemple, si vous devez permettre à un gestionnaire de précharger des certificats d'ouverture de session de nouveaux employés sur des cartes à puce

Comment fonctionne l'inscription automatique ?



L'une des méthodes les plus utilisés pour le déploiement de certificats dans un environnement Active Directory est d'utiliser l'inscription automatique. Cette méthode constitue une manière automatisée de déployer des certificats aux utilisateurs et aux ordinateurs dans la PKI. Vous pouvez utiliser l'inscription automatique dans des environnements qui répondent à des exigences spécifiques, comme l'utilisation des modèles de certificats et de la stratégie de groupe dans AD DS. Toutefois, il est important de noter que vous ne pouvez pas utiliser l'inscription automatique avec une autorité de certification autonome. Vous devez avoir une AC d'entreprise disponible pour utiliser l'inscription automatique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'inscription automatique permet de déployer automatiquement des certificats basés sur des clés publiques pour des utilisateurs et des ordinateurs dans une organisation. L'administrateur de services de certificats duplique un modèle de certificat, puis configure les autorisations pour activer les autorisations **Inscription** et **Inscription automatique** pour les utilisateurs qui recevront les certificats. Les stratégies de groupe basées sur les domaines, telles que des stratégies basées sur l'ordinateur et l'utilisateur, peuvent activer et gérer l'inscription automatique.

Par défaut, la stratégie de groupe est appliquée quand vous redémarrez des ordinateurs, ou à l'ouverture de session des utilisateurs. De plus, par défaut, la stratégie de groupe est actualisée toutes les 90 minutes pour les membres du domaine. Ce paramètre de stratégie de groupe se nomme Client des services de certificats - Inscription automatique.

Un minuteur interne déclenche l'inscription automatique toutes les huit heures après la dernière activation d'inscription automatique. Le modèle de certificat pourrait spécifier l'interaction utilisateur pour chaque demande. Pour une telle demande, une fenêtre contextuelle s'affiche approximativement 60 secondes après que l'utilisateur ouvre une session.

De nombreux certificats peuvent être distribués sans que le client ne sache que l'inscription a lieu. Ceux-ci comprennent la plupart des types des certificats qui sont publiés pour les ordinateurs et services, aussi bien que de nombreux certificats publiés pour les utilisateurs.

Pour inscrire des clients automatiquement pour des certificats dans un environnement de domaine, vous devez :

- être membre des admins du domaine ou des administrateurs de l'entreprise, (ou équivalent), ce qui est le minimum requis pour réaliser cette procédure ;
- configurer un modèle de certificat avec des autorisations **Inscription automatique** ;
- configurer une stratégie d'inscription automatique pour le domaine.

Qu'est-ce que l'itinérance des informations d'identification ?

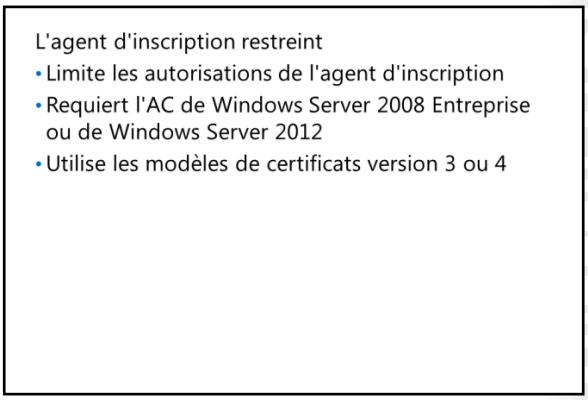
L'itinérance des informations d'identification permet aux organisations de stocker des certificats et des clés privées de AD DS, séparément de l'état d'application ou des informations de configuration. L'itinérance des informations d'identification utilise des mécanismes existants d'ouverture de session et d'inscription automatique pour télécharger des certificats et des clés sur un ordinateur local lorsqu'un utilisateur ouvre une session et, au besoin, les supprimer lorsque l'utilisateur se déconnecte. En outre, l'intégrité de ces informations d'identification est maintenue dans toutes les conditions, comme lors de la mise à jour des certificats ou lorsque les utilisateurs se connectent à plusieurs ordinateurs simultanément. Ceci évite le scénario dans lequel un utilisateur est inscrit automatiquement pour un certificat sur chaque nouvelle machine sur laquelle il ouvre une session.

L'itinérance des informations d'identification est déclenchée quand une clé privée ou un certificat dans le magasin de certificats local de l'utilisateur change, lorsque l'utilisateur verrouille ou déverrouille l'ordinateur et lorsque la stratégie de groupe est actualisée.

Toute la communication liée au certificat entre les composants de l'ordinateur local et entre l'ordinateur local et AD DS est signée et chiffrée. L'itinérance des informations d'identification est prise en charge par Windows 7 et les systèmes d'exploitation Windows plus récents.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce qu'un agent d'inscription restreint ?



Dans les versions antérieures de l'autorité de certification de Windows Server, telles que Windows Server 2003, il n'est pas possible de permettre à un agent d'inscription d'inscrire seulement un certain groupe d'utilisateurs. En conséquence, chaque utilisateur avec un certificat d'agent d'inscription peut s'inscrire au nom de n'importe quel utilisateur dans une organisation.

L'agent d'inscription restreint est une fonctionnalité qui a été proposée dans le système d'exploitation Windows Server 2008 Entreprise. Cette fonctionnalité vous permet de restreindre les autorisations pour les utilisateurs qui sont des agents d'inscription, de s'inscrire pour des certificats de carte à puce au nom d'autres utilisateurs.

En général, un ou plusieurs personnes autorisées au sein d'une organisation sont des agents d'inscription. Un certificat d'agent d'inscription doit être émis pour l'agent d'inscription afin que ce dernier puisse inscrire des utilisateurs pour l'obtention de certificats, au nom de ces utilisateurs. Les agents d'inscription sont en général membres des équipes de la sécurité d'entreprise, de la sécurité informatique ou d'assistance technique, parce que ces personnes peuvent déjà protéger des ressources précieuses. Dans certaines organisations, comme les banques qui ont beaucoup de services, l'assistance technique et les travailleurs de la sécurité peuvent ne pas être correctement situés pour effectuer cette tâche. Dans ce cas, la désignation d'un responsable de succursale ou d'un autre employé de confiance comme agent d'inscription est requise pour permettre la publication d'informations d'identification de carte à puce depuis plusieurs emplacements.

Sur une autorité de certification de Windows Server 2012, les fonctionnalités de l'agent d'inscription restreint permettent d'utiliser un agent d'inscription pour un ou plusieurs modèles de certificats. Pour chaque modèle de certificat, vous pouvez choisir au nom de quels utilisateurs ou groupes de sécurité l'agent d'inscription peut inscrire. Vous ne pouvez pas imposer un agent d'inscription selon une certaine unité d'organisation d'Active Directory ou le conteneur. Vous devez plutôt utiliser des groupes de sécurité.

Remarque : L'utilisation des agents d'inscription restreints affectera les performances de l'autorité de certification. Pour optimiser des performances, vous devriez réduire le nombre de comptes qui sont listés comme agents d'inscription. Vous réduisez le nombre de comptes dans la liste d'autorisations de l'agent d'inscription. Dans le cadre des meilleures pratiques, utilisez des comptes de groupe dans les deux listes au lieu des comptes d'utilisateurs individuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration de l'agent d'inscription restreint

Dans cette démonstration, vous allez apprendre à configurer l'agent d'inscription restreint.

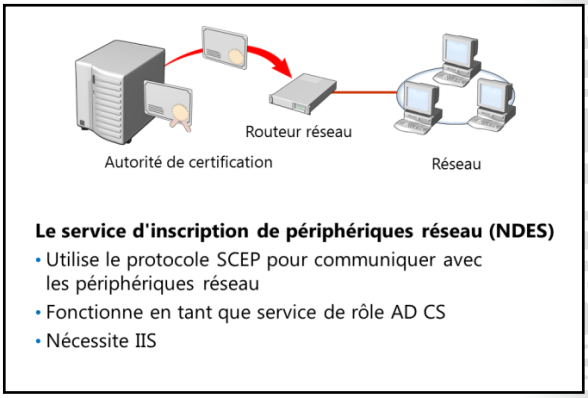
Procédure de démonstration

Configurer l'agent d'inscription restreint

1. Sur LON-SVR1, ouvrez la console **Modèles de certificats**.
2. Configurez **Allie Bellew** avec des autorisations permettant de s'inscrire pour un certificat d'agent d'inscription.
3. Publiez le modèle de certificat d'agent d'inscription.
4. Connectez-vous à LON-CL1 en tant que **Adatum\Allie** avec le mot de passe **Pa$$w0rd**.
5. Ouvrez une console **Microsoft Management (MMC)** et ajoutez le composant logiciel enfichable **Certificats**.
6. Demandez le certificat d'agent d'inscription.
7. Basculez vers **LON-SVR1**, puis ouvrez les propriétés **d'AdatumRootCA**.
8. Configurez l'agent d'inscription restreint de sorte qu'Allie puisse seulement délivrer des certificats sur la base du modèle **Utilisateur**, et seulement pour le groupe de sécurité **Marketing**.

Qu'est-ce que le service d'inscription de périphériques réseau ?

Le service d'inscription de périphériques réseau (NDES) est l'implémentation Microsoft du protocole d'inscription du certificat simple (SCEP). Le protocole SCEP est un protocole de communication qui permet aux logiciels qui s'exécutent sur des périphériques réseau, tels que des routeurs et des commutateurs, et qui ne pourraient pas sans cela s'authentifier sur le réseau, de s'inscrire afin d'obtenir des certificats x.509 auprès d'une autorité de certification.



Vous pouvez utiliser le service NDES comme filtre ISAPI (Internet Server API) sur IIS pour remplir les fonctions suivantes :

- créer et fournir des mots de passe d'inscription à usage unique pour les administrateurs ;
- récupérer des demandes en attente auprès de l'autorité de certification ;
- rassembler et traiter des demandes d'inscription SCEP pour le logiciel qui s'exécute sur des périphériques réseau.

Cette fonctionnalité s'applique aux organisations qui disposent de PKI avec une ou plusieurs AC basées sur Windows Server 2012 et qui souhaitent améliorer la sécurité pour leurs périphériques réseau. La sécurité de port, selon 802.1x, requiert des certificats installés sur des commutateurs et des points d'accès. Secure Shell (SSH), au lieu de Telnet, requiert un certificat sur le routeur, le commutateur ou le point d'accès. NDES est le service qui permet aux administrateurs d'installer des certificats sur des périphériques à l'aide de SCEP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'ajout de la prise en charge de NDES peut améliorer la flexibilité et l'évolutivité de la PKI d'une organisation. Par conséquent, cette fonctionnalité devrait intéresser les architectes, les planificateurs et les administrateurs PKI.

Avant d'installer NDES, vous devez définir :

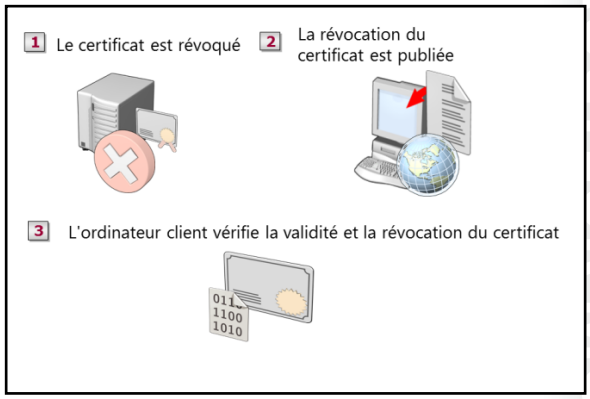
- si vous souhaitez configurer un compte d'utilisateur dédié au service ou utiliser le compte de service réseau ;
- le nom de l'autorité d'inscription NDES et le pays/la région à utiliser. (Ces informations sont incluses dans tous les certificats SCEP émis.) ;
- le fournisseur de services de chiffrement (CSP) à utiliser pour la clé de signature employée pour chiffrer la communication entre l'autorité de certification et l'autorité d'inscription ;
- le fournisseur de services de chiffrement (CSP) à utiliser pour la clé de chiffrement employée pour chiffrer la communication entre l'autorité d'inscription et le périphérique réseau ;
- la longueur de chacune de ces clés.

En outre, vous devez créer et configurer des modèles pour les certificats utilisés conjointement à NDES.

L'installation de NDES sur un ordinateur crée une autorité d'inscription et supprime tous les certificats d'autorité d'inscription préexistants sur l'ordinateur. Par conséquent, si vous envisagez d'installer NDES sur un ordinateur sur lequel une autre autorité d'inscription a déjà été configurée, toutes les demandes de certificat en attente doivent être traitées et tous les certificats non réclamés doivent être réclamés avant l'installation de NDES.

Comment fonctionne la révocation des certificats ?

La révocation est le processus qui vous permet de désactiver la validité d'un ou de plusieurs certificats. En initialisant le processus de révocation, vous publiez réellement une empreinte numérique de certificat dans la liste de révocation de certificats correspondante.



Les grandes lignes d'une vue d'ensemble du cycle de vie de révocation des certificats sont les suivantes :

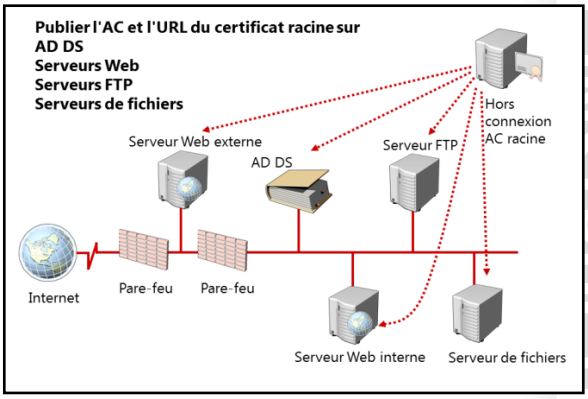
- Un certificat est révoqué depuis le composant logiciel enfichable MMC d'autorité de certification. Pendant la révocation, un code de raison et une date et heure sont spécifiés. C'est facultatif, mais recommandé.
- La liste de révocation de certificats est publiée à l'aide du composant logiciel enfichable MMC d'autorité de certification (ou la liste de révocation planifiée est publiée automatiquement selon la valeur configurée). Des listes de révocation de certificats peuvent être publiées dans AD DS, dans certains emplacements de dossier partagé ou sur un site Web.
- Quand des ordinateurs clients Windows sont présentés avec un certificat, ils utilisent un processus pour vérifier l'état de révocation en interrogeant l'autorité de certification de publication. Ce processus détermine si le certificat est révoqué, puis présente les informations à l'application demandant la vérification. L'ordinateur client Windows utilise l'un des emplacements de liste de révocation de certificats spécifiés dans le certificat pour contrôler sa validité.

Les systèmes d'exploitation Windows comprennent CryptoAPI, qui est responsable des processus de révocation des certificats et de contrôle de l'état. CryptoAPI utilise les phases suivantes dans le processus de contrôle du certificat :

- Détection de certificats. La détection de certificats rassemble des certificats d'autorité de certification, des informations d'AIA dans les certificats émis et des détails du processus d'inscription de certificat.
- Validation de chemin d'accès. La validation de chemin d'accès est le processus de vérification du certificat par la chaîne d'autorité de certification (ou *chemin d'accès*) jusqu'au certificat d'autorité de certification racine.
- Vérification de révocation. Tous les certificats de la chaîne du certificat sont contrôlés pour vérifier qu'aucun d'entre eux n'est révoqué.
- Récupération et mise en cache de réseau. La récupération de réseau est exécutée à l'aide d'OCSP. CryptoAPI est responsable de la vérification du cache local d'abord pour les informations de révocation et s'il n'y a aucune correspondance, il doit faire un appel utilisant OCSP, en fonction de l'URL fournie par le certificat émis.

Considérations relatives à la publication d'AIA et de CDP

Quand vous gérez ou publiez des certificats, il est important que vous configuriez correctement les extensions de certificat qui sont utilisées pour vérifier le certificat de l'autorité de certification, et le certificat qui est utilisé par l'utilisateur. Ces extensions, AIA et CDP, font partie de chaque certificat. Ils doivent indiquer des emplacements appropriés, ou la PKI peut ne pas fonctionner correctement.



Qu'est-ce que le système AIA ?

Les adresses AIA sont les URL dans les certificats qu'une autorité de certification délivre. Ces adresses indiquent au vérificateur d'un certificat où récupérer le certificat d'autorité de certification. Les URL d'accès d'AIA peuvent être HTTP, FTP, LDAP ou adresses de FICHIER.

Qu'est-ce que le système CDP ?

Le CDP est une extension de certificat qui indique d'où la liste de révocation des certificats pour une autorité de certification peut être récupérée. Il peut contenir aucune, une ou de nombreuses URL HTTP, de FICHIER ou LDAP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Publication AIA et CDP

Si vous utilisez seulement une autorité de certification en ligne, ces valeurs sont configurées localement par défaut sur l'autorité de certification. Cependant, si vous souhaitez déployer une autorité de certification racine hors connexion ou si vous souhaitez publier AIA et CDP dans un emplacementavec accès via Internet, vous devez reconfigurer ces valeurs de sorte qu'elles s'appliquent à tous les certificats publiés par l'autorité de certification racine. Les extensions AIA et CDP définissent l'emplacement où les applications clientes peuvent localiser les informations AIA et CDP pour l'autorité de certification racine. Le formatage et la publication des URL d'extension AIA et CDP sont en général identiques pour des autorités de certification racine et des autorités de certification secondaires. Vous pouvez publier le certificat d'autorité de certification racine et la liste de révocation de certificats aux emplacements suivants :

- AD DS
- Serveurs Web
- Serveurs FTP (File Transfer Protocol)
- Serveurs de fichiers

Points de publication

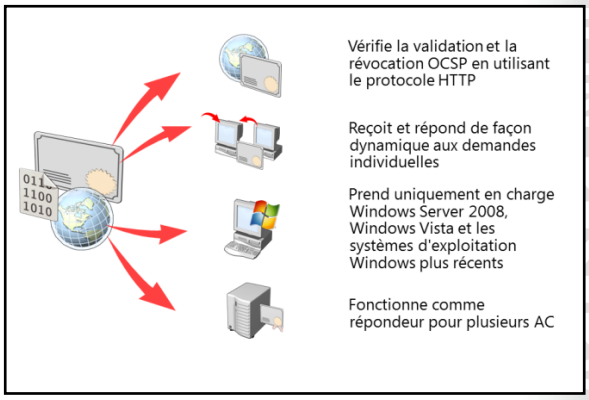
Pour garantir que tous les ordinateurs de la forêt pourront accéder aux informations, publiez le certificat et la liste de révocation de certificats de l'Autorité de certification racine hors connexion sur AD DS en utilisant la commande **Certutil**. Cette commande place le certificat et la liste CRL de l'Autorité racine dans le contexte de configuration/d'appellation qui est répliqué par Active Directory vers tous les contrôleurs de domaine de la forêt.

Pour les ordinateurs qui ne sont pas des membres d'un domaine AD DS, placez le certificat d'autorité de certification et la liste de révocation de certificats sur des serveurs Web à l'aide du protocole HTTP. Localisez les serveurs Web sur le réseau interne, et sur le réseau externe si les ordinateurs clients externes (ou les clients internes des réseaux externes) ont besoin de l'accès. C'est très important si vous utilisez en dehors de votre société des certificats émis en interne.

Vous pouvez également publier les certificats et les listes de révocation de certificats sur des adresses URL ftp:// et Fichier://, mais il est recommandé d'utiliser seulement des adresses URL LDAP et HTTP, parce que ce sont les formats URL les plus couramment pris en charge à des fins d'interopérabilité. La commande dans laquelle vous listez les extensions CDP et AIA est importante, parce que le moteur de chaînage de certificats recherche les URL de manière séquentielle. Si vos certificats sont en grande partie utilisés en interne, placez d'abord l'URL LDAP dans la liste.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce qu'un répondeur en ligne ?



À l'aide d'OCSP, un répondeur en ligne constitue pour les clients un moyen efficace de déterminer l'état de révocation d'un certificat. OCSP envoie des demandes d'état de certificat à l'aide de HTTP.

Les clients accèdent aux listes de révocation de certificats pour déterminer l'état de révocation d'un certificat. Les listes de révocation de certificats peuvent être grandes, et les clients peuvent passer beaucoup de temps à rechercher dans ces listes de révocation de certificats. Un répondeur en ligne peut rechercher dynamiquement ces listes de révocation de certificats pour les clients, et répond seulement au certificat demandé.

Vous pouvez utiliser un répondeur en ligne unique pour fournir des informations d'état de la révocation concernant des certificats émis par une autorité de certification unique ou par plusieurs autorités de certification. Cependant, vous pouvez utiliser plusieurs répondeurs en ligne pour distribuer les informations de révocation d'autorité de certification.

Vous pouvez installer un répondeur en ligne sur n'importe quel ordinateur qui exécute Windows Server 2008 Entreprise ou Windows Server 2012. Vous devriez installer un répondeur en ligne et une autorité de certification sur d'autres ordinateurs.

Les systèmes d'exploitation suivants peuvent utiliser le répondeur en ligne pour la validation de l'état de certificat :

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Vista®
- Windows 7
- Windows 8

Pour l'évolutivité et la haute disponibilité, vous pouvez déployer le répondeur en ligne dans une charge équilibrée à l'aide de l'équilibrage de la charge réseau (NLB), qui traite des demandes d'état de certificat. Vous pouvez surveiller et gérer chaque membre du tableau indépendamment. Pour configurer le répondeur en ligne, vous devez utiliser la console de gestion du répondeur en ligne.

Vous devez configurer les autorités de certification pour qu'elles incluent l'URL du répondeur en ligne dans l'extension AIA des certificats émis. Le client OCSP utilise cette URL pour valider l'état de certificat. Vous devez également publier le modèle de certificat de signature de réponse OCSP, de sorte que le répondeur en ligne puisse également inscrire ce certificat.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure d'installation et de configuration du répondeur en ligne.

Vous pouvez installer des répondeurs en ligne sur les ordinateurs qui exécutent Windows Server 2008 R2 ou Windows Server 2012. Vous devriez installer des répondeurs en ligne après les autorités de certification, mais avant de publier les certificats client. Les données de révocation des certificats proviennent d'une liste de révocation de certificats publiée. La liste de révocation de certificats publiée peut provenir d'une autorité de certification sur un ordinateur qui exécute Windows Server 2008 ou une version ultérieure, ou Windows Server 2003, ou d'une autorité de certification non-Microsoft.

Avant de configurer une autorité de certification afin de prendre en charge le service de répondeur en ligne, les éléments suivants doivent être présents :

- IIS doit être installé sur l'ordinateur pendant l'installation de répondeur en ligne. La configuration correcte des Services Internet (IIS) pour le répondeur en ligne s'installe automatiquement lorsque vous installez un répondeur en ligne.
- Un modèle de certificat de signature de réponse OCSP doit être configuré sur l'autorité de certification et l'inscription automatique doit être utilisée pour émettre un certificat de signature de réponse OCSP sur l'ordinateur sur lequel le répondeur en ligne sera installé.
- L'URL du répondeur en ligne doit être incluse dans l'extension AIA des certificats émis par l'autorité de certification. Cette URL est utilisée par le client de répondeur en ligne pour valider l'état des certificats.

Après avoir installé un répondeur en ligne, vous devez créer une configuration de révocation pour chaque autorité de certification et tous les certificats d'autorité de certification servis par un répondeur en ligne. Une configuration de révocation inclut tous les paramètres nécessaires pour répondre aux demandes d'état concernant des certificats émis à l'aide d'une clé d'autorité de certification spécifique. Ces paramètres de configuration sont les éléments suivants :

- Certificat d'autorité de certification. Ce certificat peut se trouver sur un contrôleur de domaine, dans le magasin de certificats local ou être importé à partir d'un fichier.
- Certificat de signature pour le répondeur en ligne. Ce certificat peut être sélectionné automatiquement, vous pouvez le sélectionner manuellement (ce qui implique une étape d'importation distincte à l'issue de l'ajout de la configuration de révocation) ou vous pouvez utiliser le certificat d'autorité de certification sélectionné.
- Fournisseur de révocation. Le fournisseur de révocation fournira les données de révocation utilisées par cette configuration. Ces informations sont entrées sous la forme d'une ou plusieurs URL auxquelles les listes de révocation de certificats standard et delta sont accessibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration d'un répondeur en ligne

Au cours de cette démonstration, vous allez apprendre à configurer un répondeur en ligne.

Procédure de démonstration

Configurer un répondeur en ligne

1. Sur LON-SVR1, le Gestionnaire de serveur permet d'ajouter un service de rôle de **répondeur en ligne** au rôle AD CS existant.
2. Configurez un nouvel emplacement de la distribution AIA sur **AdatumRootCA** : **http://lon-svr1/ocsp**.
3. Dans **AdatumRootCA**, publiez le modèle de certificat de signature de réponse OCSP, et permettez aux utilisateurs authentifiés de s'inscrire.
4. Ouvrez la console de **gestion du répondeur en ligne**.
5. Ajoutez la configuration de révocation pour **AdatumRootCA**.
6. Inscrivez un certificat de signature de réponse OCSP.
7. Assurez-vous que l'état de configuration de révocation affiche En cours.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 5
Gestion de la récupération de certificats

Pendant le cycle de vie de certificat, la récupération de clés ou de certificats est l'une des tâches de gestion les plus importantes. Si vous perdez vos clés publiques et privées, vous utilisez un agent d'archivage et de récupération de clés pour la récupération des données. Vous pouvez également utiliser des méthodes automatiques ou manuelles d'archivage et de récupération de clés pour que vous puissiez accéder aux données si vous perdez vos clés. Dans ce cours, vous découvrirez comment gérer l'archivage et la récupération de clés dans AD CS sous Windows Server 2012.

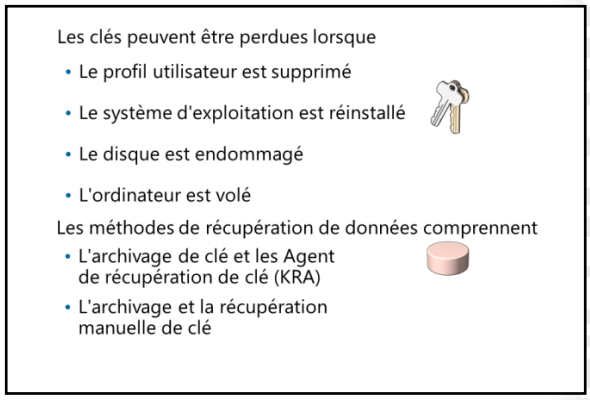
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le processus d'archivage et de récupération de clés ;
- configurer l'archivage de clés automatique ;
- configurer une autorité de certification pour l'archivage de clé ;
- Expliquer la récupération de clé ;
- Récupérer une clé privée perdue.

Vue d'ensemble de l'archivage et de la récupération de clés

Si vous perdez vos clés publiques et privées, vous ne pourrez pas accéder aux données chiffrées à l'aide de la clé publique du certificat. Il s'agit notamment d'EFS et de Secure/Multipurpose Internet Mail Extensions (S/MIME). Par conséquent, l'archivage et la récupération de clés publiques et privées sont importants.



Situations de perte de clés

Vous pouvez perdre la paire de clés dans les cas suivants :

- Le profil utilisateur est supprimé ou endommagé. Un fournisseur de services cryptographiques chiffre et stocke une clé privée dans le système de fichiers et dans le Registre locaux du dossier du profil utilisateur. La suppression ou l'endommagement du profil entraîne la perte des informations de la clé privée.
- Le système d'exploitation est réinstallé. Lorsque vous réinstallez le système d'exploitation, les profils utilisateur des installations antérieures sont perdus, y compris les informations de la clé privée.
- Le disque est endommagé. Si le disque dur est endommagé et si le profil utilisateur n'est pas disponible, les informations de la clé privée sont automatiquement perdues.
- L'ordinateur est volé. Si l'ordinateur d'un utilisateur est volé, le profil utilisateur contenant les informations de la clé privée n'est pas disponible.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Agents d'archivage et de récupération de clé

Vous utilisez l'archivage de clé et les agents de récupération de clé pour la récupération de données. Vous pouvez vérifier que les administrateurs d'autorité de certification peuvent récupérer des clés privées en les archivant. Les agents de récupération de clé sont des utilisateurs désignés qui peuvent récupérer le certificat d'origine, la clé privée et la clé publique ayant servi à chiffrer les données de la base de données de l'autorité de certification. Un modèle de certificat spécifique est appliqué à un KRA. Lorsque vous activez l'archivage de clé dans un modèle de certificat version 2, l'autorité de certification chiffre et stocke cette clé privée dans sa base de données. Lorsque l'autorité de certification a stocké la clé privée du sujet dans sa base de données, vous pouvez utiliser la récupération de clé pour récupérer une clé endommagée ou perdue.

Au cours du processus de récupération de clé, le gestionnaire de certificats récupère le fichier chiffré qui contient le certificat et la clé privée de la base de données de l'Autorité de certification. Ensuite, un agent de récupération de clé déchiffre la clé privée du fichier chiffré et rend le certificat et la clé privée à l'utilisateur.

Sécurité pour l'archivage de clé

Lorsque vous avez un AC configurée pour publier une certificat KRA, tout utilisateur disposant de l'autorisation **Lecture** et **Inscription** sur le modèle de certificat KRA peut s'inscrire et devenir agent de récupération de clé. Par conséquent, les admins du domaine et les administrateurs de l'entreprise reçoivent l'autorisation par défaut. Cependant, vous devez vérifier ce qui suit :

- Seuls les utilisateurs de confiance peuvent s'inscrire pour ce certificat.
- La clé de récupération de l'agent de récupération de clé est enregistrée de façon sécurisée.
- Le serveur sur lesquelles les clés sont archivées se trouve à un emplacement distinct et physiquement sécurisé.

Explication de l'archivage et de la récupération de clé

La récupération de clé implique que la partie de clé privée d'une paire de clés publique/privée peut être archivée et récupérée. La récupération de clés privées ne permet pas de récupérer de données ou de messages. Elle permet simplement à un utilisateur de récupérer des clés perdues ou endommagées, ou à un administrateur d'évaluer le rôle d'un utilisateur pour l'accès aux données ou la récupération de données. Dans de nombreuses applications, la récupération de données ne peut pas se produire sans effectuer en premier lieu la récupération de clé.

La procédure de récupération de clé est la suivante :

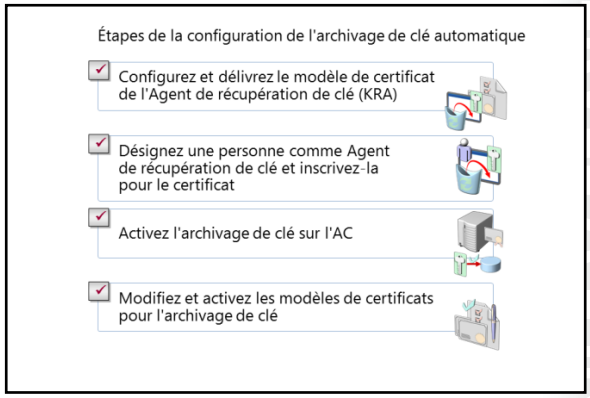
1. L'utilisateur demande un certificat à une autorité de certification et fournit une copie de la clé privée dans le cadre de la demande. L'autorité de certification, qui traite la demande, archive la clé privée chiffrée dans la base de données de l'autorité de certification et fournit un certificat au demandeur.
2. Le certificat émis peut être utilisé par une application telle qu'EFS pour chiffrer des fichiers sensibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Si, à un certain moment, la clé privée est perdue ou endommagée, l'utilisateur peut contacter le gestionnaire de certificats de la société pour récupérer la clé privée. Le gestionnaire de certificats, avec l'aide de l'agent de récupération de clé, récupère la clé privée, l'enregistre dans un format de fichier protégé et la renvoie à l'utilisateur.
4. Après que l'utilisateur enregistre la clé privée récupérée dans la banque locale des clés de l'utilisateur, elle peut être utilisée de nouveau par une application telle qu'EFS pour déchiffrer des fichiers chiffrés ou pour chiffrer de nouveaux fichiers.

Configuration de l'archivage de clé automatique

Avant que vous ne puissiez utiliser l'archivage de clé, vous devez effectuer plusieurs étapes de configuration. La fonctionnalité d'archivage de clé n'est pas activée par défaut, et vous devriez configurer l'autorité de certification et les modèles de certificats pour l'archivage de clé et la récupération de clé.



Les étapes suivantes détaillent le processus d'archivage de clé automatique :

1. configurer le modèle de certificat de l'agent de récupération de clé ; Seuls les administrateurs de l'entreprise ou les administrateurs du domaine sont autorisés à demander un certificat d'agent de récupération de clé. Si vous souhaitez inscrire un autre utilisateur avec un certificat d'agent de récupération de clé, vous devez le spécifier sur la liste DACL du modèle.
2. Configurez les gestionnaires de certificats.
   a. L'autorité de certification définit une personne comme gestionnaire de certificats, le cas échéant. Le gestionnaire de certificats conserve habituellement une clé privée pour les certificats KRA valides. Par défaut, l'administrateur de l'autorité de certification est un gestionnaire de certificats pour tous les utilisateurs, excepté pour les cas avec une autre définition explicite. Cependant, comme meilleure pratique, vous devriez séparer ces deux rôles si possible.
   b. Un dirigeant d'autorité de certification est défini en tant que gestionnaire de certificats. Cet utilisateur dispose de l'autorisation de sécurité pour délivrer et gérer des certificats. Les autorisations de sécurité sont configurées dans une AC dans le composant logiciel enfichable MMC de l'autorité de certification, dans la boîte de dialogue **Propriétés de l'AC**, depuis l'onglet **Sécurité**.
   c. Un agent de récupération de clé n'est pas nécessairement un dirigeant d'autorité de certification ou un gestionnaire de certificats. Ces rôles peuvent être segmentés en tant que rôles distincts. Un agent de récupération de clé est une personne qui conserve une clé privée pour un certificat KRA valide.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Activer KRA.
    a. Connectez-vous comme administrateur du serveur ou comme administrateur de l'autorité de certification si la séparation des rôles est activée.
    b. Dans la console Autorité de certification, cliquez avec le bouton droit sur le nom de l'AC, puis cliquez sur **Propriétés**. Pour permettre l'archivage de clé, sous l'onglet **Agents de récupération**, cliquez sur **Archiver la clé**.
    c. Par défaut, l'autorité de certification utilise un KRA. Cependant, vous devez d'abord sélectionner le certificat KRA pour que l'autorité de certification commence l'archivage en cliquant sur **Ajouter**.
    d. Le système recherche les certificats KRA valides, puis affiche les certificats KRA disponibles. Ceux-ci sont en général publiés dans AD DS par une AC d'entreprise pendant l'inscription. Des certificats KRA sont enregistrés sous le conteneur de KRA de la branche Services de clé publique de la partition de configuration dans AD DS. Puisque l'autorité de certification délivre plusieurs certificats KRA, chaque certificat KRA sera ajouté à l'attribut d'utilisateur à valeurs multiples de l'objet d'autorité de certification.
    e. Sélectionnez un certificat, puis cliquez sur **OK**. Assurez-vous que vous avez sélectionné le certificat souhaité.
    f. Après que vous avez ajouté un ou plusieurs certificats KRA, cliquez sur **OK**. Les certificats KRA sont seulement traités au démarrage du service.
4. Configurez des modèles d'utilisateur.
    a. Dans la console MMC des modèles de certificats, cliquez avec le bouton droit sur le modèle d'archivage de clé, puis cliquez sur **Propriétés**.
    b. Pour toujours appliquer l'archivage de clé pour l'AC, dans la boîte de dialogue **Propriétés**, sous l'onglet **Traitement de la demande**, activez la case à cocher **Archive la clé privée de cryptage du sujet**. Dans des AC Windows Server 2008 ou postérieures, sélectionnez l'option **Utiliser un algorithme symétrique avancé pour envoyer la clé à l'autorité de certification**.

Démonstration : Configuration d'une autorité de certification pour l'archivage de clé

Dans cette démonstration, vous allez apprendre à configurer une autorité de certification pour l'archivage de clé.

Procédure de démonstration

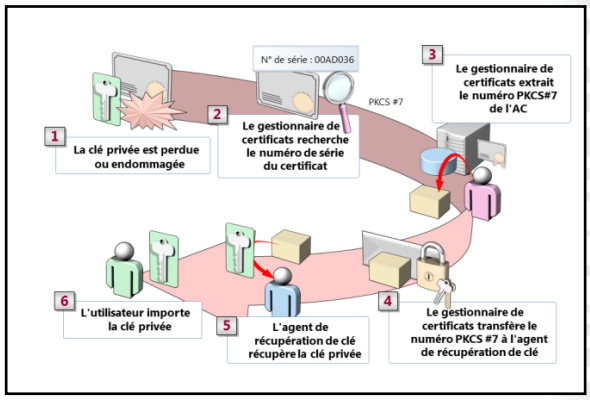
Configurer l'archivage de clé automatique

1. Configurez **AdatumRootCA** pour délivrer des certificats d'agent de récupération de clé sans approbation.
2. Inscrivez l'**administrateur** pour le certificat d'agent de récupération de clé.
3. Configurez **AdatumRootCA** pour utiliser le certificat inscrit dans l'étape 2 comme agent de récupération de clé.
4. Configurez le modèle de certificat de **Utilisateur Exchange Test 1** pour activer l'archivage de clé.
5. Configurez **AdatumRootCA** pour activer l'archivage de clé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Récupération d'une clé perdue

La récupération de clé se déroule en plusieurs étapes, et vous devez respecter strictement la procédure pour récupérer des clés archivées. La procédure de récupération de clé est la suivante :



1. Recherche de candidats de récupération. Vous aurez besoin de deux informations pour exécuter la récupération de clé. D'abord, le gestionnaire de certificats ou l'administrateur de l'autorité de certification localise l'entrée correcte de certificat dans la base de données de l'autorité de certification. Ensuite, le gestionnaire de certificats ou l'administrateur de l'autorité de certification obtient le numéro de série de l'entrée correcte de certificat et du certificat KRA requis pour la récupération de clé.
2. Récupérez le BLOB PKCS #7 de la base de données. C'est la première moitié de l'étape de récupération de clé. Un gestionnaire de certificats ou un administrateur de l'autorité de certification récupère le BLOB correct de la base de données de l'autorité de certification. Le certificat et la clé privée chiffrée à récupérer sont présents dans le BLOB PKCS #7. La clé privée est chiffrée avec la clé publique d'un ou de plusieurs KRA.
3. Récupérez le matériel de clé et enregistrez-le dans PKCS #12 (.pfx). C'est la seconde moitié de l'étape de récupération de clé. Le support d'une des clés privées du KRA déchiffre la clé privée à récupérer. Le support génère également un fichier .pfx protégé par mot de passe qui contient le certificat et la clé privée.

Importez les clés récupérées. Le fichier .pfx protégé par mot de passe est délivré à l'utilisateur final. Cet utilisateur importe le fichier .pfx dans le magasin de certificats utilisateur local. De plus, le KRA ou un administrateur peut réaliser cette partie de la procédure au nom de l'utilisateur.

Démonstration : Récupération d'une clé privée perdue (en option)

Dans cette démonstration, vous allez apprendre à récupérer une clé privée perdue.

Procédure de démonstration

Récupérer une clé privée perdue

1. Inscrivez l'administrateur pour le certificat Exchange User Test1.
2. Supprimez le certificat du magasin personnel de l'administrateur pour simuler la perte de la clé.
3. Sur LON-SVR1 dans la console d'autorité de certification, récupérez le numéro de série du certificat perdu.

```
Utilisez la commande Certutil -getkey <serialnumber> outputblob pour générer le
fichier blob.
Utilisez la commande Certutil -recoverkey outputblob recover.pfx pour récupérer la clé
privée.
```

4. Importez la clé privée de nouveau dans le magasin personnel de l'administrateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Déploiement et gestion de certificats

Scénario

Alors que la société A. Datum Corporation s'est développée, ses besoins de sécurité ont également augmenté. Le département sécurité est notamment intéressé par l'activation d'un accès sécurisé aux sites Web critiques et par la fourniture d'une sécurité supplémentaire pour des fonctionnalités comme EFS, les cartes à puce et la fonctionnalité DirectAccess de Windows 7 et Windows 8. Pour faire face à ces exigences de sécurité, A. Datum a décidé d'implémenter une PKI à l'aide du rôle AD CS sous Windows Server 2012.

En tant que l'un des principaux administrateurs réseau chez A. Datum, vous êtes chargé de l'implémentation du déploiement d'AD CS. Vous déploierez la hiérarchie d'autorité de certification, développerez les procédures et processus pour la gestion des modèles de certificats et déploierez et révoquerez des certificats.

Objectifs

- configurer des modèles de certificats ;
- configurer l'inscription de certificat ;
- configurer la révocation de certificats ;
- configurer et exécuter l'archivage et la récupération de clé privée.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-SVR2** **22412B-LON-CA1** **22412B-LON-CL1**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Tous les ordinateurs virtuels nécessaires pour cet atelier doivent fonctionner depuis l'atelier précédent.

Exercice 1 : Configuration de modèles de certificats

Scénario

Après le déploiement de l'infrastructure d'autorité de certification, l'étape suivante est le déploiement des modèles de certificats requis dans l'organisation. D'abord, A. Datum souhaite implémenter un nouveau certificat de serveur Web et des certificats de carte à puce pour des utilisateurs. La société souhaite également implémenter de nouveaux certificats sur le serveur Web LON-SVR2.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un nouveau modèle basé sur le modèle de serveur Web
2. Créer un modèle de certificat pour les utilisateurs avec inscription de cartes à puce.
3. Configurez les modèles pour qu'ils puissent être publiés
4. Mettez à jour le certificat de serveur Web sur le serveur Web LON-SVR2

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Créer un nouveau modèle basé sur le modèle de serveur Web

1. Sur LON-SVR1, depuis la console Autorité de certification, ouvrez la console **Modèles de certificats**.
2. Dupliquez le modèle **Serveur Web**.
3. Créez un nouveau modèle et nommez-le **Serveur Web d'Adatum**.
4. Configurez la validité pour **3 années**.
5. Configurez la clé privée comme exportable.

▶ Tâche 2 : Créer un modèle de certificat pour les utilisateurs avec inscription de cartes à puce

1. Dans la console Modèles de certificats, dupliquez le modèle de certificat **Utilisateur**.
2. Nommez le nouveau modèle **Utilisateur de carte à puce Adatum**.
3. Sous l'onglet **Nom du sujet**, désactivez les cases à cocher **Inclure le nom de compte de messagerie dans le nom du sujet** et **Nom de messagerie électronique**.
4. Ajoutez **Ouverture de session par carte à puce** aux stratégies d'application du nouveau modèle de certificat.
5. Configurez ce nouveau modèle pour remplacer le modèle **Utilisateur**.
6. Permettez aux utilisateurs authentifiés de **lire**, de s'**inscrire** et de s'**inscrire automatiquement** pour ce certificat.
7. Fermez la console Modèles de certificats.

▶ Tâche 3 : Configurez les modèles pour qu'ils puissent être publiés

- Configurez **LON-SVR1** pour qu'il délivre des certificats basés sur les modèles **Utilisateur de carte à puce Adatum** et **Serveur Web d'Adatum**.

▶ Tâche 4 : Mettez à jour le certificat de serveur Web sur le serveur Web LON-SVR2

1. Ouvrez une session sur **LON-SVR2** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Actualisez la stratégie de groupe et redémarrez le serveur en cas de besoin.
3. Depuis le Gestionnaire de serveur, ouvrez le **Gestionnaire des services Internet (IIS)**.
4. Inscrivez-vous pour un certificat de domaine à l'aide des paramètres suivants :
   - Nom commun : **lon-svr2.adatum.com**
   - Organisation : **Adatum**
   - Unité d'organisation : **Informatique**
   - Ville : **Seattle**
   - Department/région : **WA**
   - Pays/région : **US**
   - Nom convivial : **lon-svr2**
5. Créez une liaison HTTPS pour le site Web par défaut, et associez-la au nouveau certificat.

Résultats : Après avoir terminé cet exercice, vous aurez créé et publié de nouveaux modèles de certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration de l'inscription de certificats

Scénario

L'étape suivante de l'implémentation de la PKI chez A. Datum est la configuration de l'inscription de certificat. A. Datum souhaite activer différentes options pour distribuer les certificats. Les utilisateurs devraient pouvoir s'inscrire automatiquement, et les utilisateurs de carte à puce devraient obtenir leurs cartes à puce auprès des agents d'inscription. Adatum a octroyé des droits d'agent d'inscription pour le groupe du service marketing à l'utilisateur Allie Bellew.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer une inscription automatique pour des utilisateurs
2. Vérifiez l'inscription automatique
3. Configurez l'agent d'inscription pour des certificats de carte à puce

▶ Tâche 1 : Configurer une inscription automatique pour des utilisateurs

1. Sur LON-DC1, ouvrez **Gestion des stratégies de groupe**.
2. Modifiez la **Default Domain Policy**.
3. Accédez à **Configuration utilisateur**, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, et cliquez pour mettre en surbrillance **Stratégies de clé publique**.
4. Activez l'option **Client des services de certificats - Inscription automatique**, ainsi que **Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués** et **Mettre à jour les certificats qui utilisent les modèles de certificats**.
5. Activez **Client des services de certificats - Stratégie d'inscription des certificats**.
6. Fermez l'Éditeur de gestion des stratégies de groupe et la console GPMC.

▶ Tâche 2 : Vérifiez l'inscription automatique

1. Sur LON-SVR1, ouvrez **Windows PowerShell** et utilisez **gpupdate /force** pour actualiser la stratégie de groupe.
2. Ouvrez une console mmc.exe et ajoutez le composant logiciel enfichable de **certificats** concentré sur le compte d'utilisateur.
3. Vérifiez que vous avez été publié un certificat selon le modèle **Utilisateur de carte à puce Adatum**.

▶ Tâche 3 : Configurez l'agent d'inscription pour des certificats de carte à puce

1. Sur LON-SVR1, depuis la console Autorité de certification, ouvrez la console **Modèles de certificats**.
2. Permettez à **Allie Bellew (Allie@adatum.com)** de s'inscrire pour un certificat d'agent d'inscription.
3. Publiez le modèle de certificat d'**agent d'inscription**.
4. Connectez-vous à **LON-CL1** comme **Allie** et inscrivez-vous pour un certificat d'agent d'inscription.
5. Sur LON-SVR1, ouvriez les propriétés d'**Adatum-IssuingCA** et configurez **Agent d'inscription restreint** pour qu'Allie puisse uniquement publier des certificats basés sur **Utilisateur de carte à puce Adatum**, pour le groupe de sécurité **Marketing**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré et vérifié l'inscription automatique pour des utilisateurs, et configuré un agent d'inscription pour des cartes à puce.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Configuration de la révocation de certificats

Scénario

Dans le cadre de la configuration de l'infrastructure de certificat, A. Datum souhaite configurer des composants de révocation sur des autorités de certification nouvellement établies. Vous configurerez des composants de liste de révocation de certificats et de répondeur en ligne.

Les tâches principales de cet exercice sont les suivantes :

1. Configuration de la distribution de la liste de révocation de certificats
2. Installation et configuration d'un répondeur en ligne

▶ Tâche 1 : Configuration de la distribution de la liste de révocation de certificats

1. Sous LON-SVR1, dans la console Autorité de certification, cliquez avec le bouton droit sur **Certificats révoqués**, puis cliquez sur **Propriétés**.
2. Définissez l'intervalle de publication de la liste de révocation des certificats sur **1 Jours**, et l'intervalle pour **Publier la liste de révocation de certificats delta** sur **1 Heures**.
3. Passez en revue les emplacements CDP sur **Adatum-IssuingCA**.

▶ Tâche 2 : Installation et configuration d'un répondeur en ligne

1. Sur LON-SVR1, le Gestionnaire de serveur permet d'ajouter un service de rôle de **répondeur en ligne** au rôle AD CS existant.
2. Lorsque le message affiche que l'installation a réussi, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
3. Configurez le répondeur en ligne.
4. Sur LON-SVR1, ouvrez la console **Autorité de certification**.
5. Configurez le nouvel emplacement de la distribution AIA sur **Adatum-IssuingCA** : **http://lon-svr1/ocsp**.
6. Dans **Adatum-IssuingCA**, publiez le modèle de certificat de signature de réponse OCSP, et permettez aux utilisateurs **authentifiés** de s'inscrire.
7. Ouvrez la console de **gestion du répondeur en ligne**.
8. Ajoutez la configuration de révocation pour **Adatum-IssuingCA**.
9. Inscrivez un certificat de signature de réponse OCSP.
10. Assurez-vous que l'état de configuration de révocation est **En cours**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré des paramètres de révocation de certificat.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Configuration de la récupération de clé

Scénario

Dans le cadre de l'établissement d'une PKI, vous souhaitez configurer et tester des procédures pour la récupération de clés privées. Vous souhaitez attribuer un certificat KRA pour un administrateur, et configurer d'AC et de modèles de certificats spécifiques pour permettre l'archivage de clé. En outre, vous souhaitez tester une procédure pour la récupération de clé.

Les tâches principales de cet exercice sont les suivantes :

1. Configuration de l'autorité de certification pour délivrer des certificats d'agent de récupération de clé
2. Acquisition du certificat KRA
3. Configuration de l'autorité de certification pour permettre la récupération de clé
4. Configuration d'un modèle personnalisé pour l'archivage de clé
5. Vérification de la fonctionnalité d'archivage de clé

▶ Tâche 1 : Configuration de l'autorité de certification pour délivrer des certificats d'agent de récupération de clé

1. Sur LON-SVR1, dans la console Autorité de certification, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
2. Dans la console Modèles de certificats, ouvrez la boîte de dialogue **Propriétés de certificat d'agent de récupération de clé**.
3. Sous l'onglet **Conditions d'émission**, désactivez la case à cocher **Approbation du gestionnaire de certificat de l'autorité de certification**.
4. Sous l'onglet **Sécurité**, notez que seuls les Admins du domaine et les administrateurs de l'entreprise ont l'autorisation **Inscription**.
5. Cliquez avec le bouton droit sur le dossier **Modèles de certificats** et activez le modèle **Agent de récupération de clé**.

▶ Tâche 2 : Acquisition du certificat KRA

1. Créez une fenêtre de console MMC pour laquelle le composant logiciel enfichable des certificats est chargé pour l'utilisateur actuel.
2. Utilisez l'Assistant Inscription de certificat pour demander un nouveau certificat et pour inscrire le certificat KRA.
3. Actualisez la fenêtre de console et affichez le KRA dans le magasin personnel.

▶ Tâche 3 : Configuration de l'autorité de certification pour permettre la récupération de clé

1. Sous LON-SVR1, dans la console Autorité de certification, ouvrez la boîte de dialogue **Propriétés de : Adatum-IssuingCA**.
2. Sous l'onglet **Agents de récupération**, cliquez sur **Archiver la clé**, puis ajoutez le certificat à l'aide de la boîte de dialogue **Sélection de l'agent de récupération de clé**.
3. Redémarrez les services de certificats lorsque vous y êtes invité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configuration d'un modèle personnalisé pour l'archivage de clé

1. Sur LON-SVR1, ouvrez la console Modèles de certificats.
2. Dupliquez le modèle utilisateur et nommez-le **Archiver l'utilisateur**.
3. Sous l'onglet **Traitement de la demande**, définissez l'option pour **Archive la clé privée de chiffrement du sujet**. À l'aide de l'option d'archivage de clé, le KRA peut obtenir la clé privée du magasin de certificats.
4. Cliquez sur l'onglet **Nom du sujet** et désactivez les cases à cocher **Nom de messagerie électronique** et **Inclure le nom de compte de messagerie dans le nom du sujet**.
5. Ajoutez **Archiver le modèle utilisateur** comme nouveau modèle de certificat à publier.

▶ Tâche 5 : Vérification de la fonctionnalité d'archivage de clé

1. Ouvrez une session sur **LON-CL1** en tant qu'**Adatum\Aidan**, en utilisant le mot de passe **Pa$$w0rd**.
2. Créez une fenêtre de console MMC qui comprend le composant logiciel enfichable Certificats.
3. Demandez et inscrivez un nouveau certificat sur la base du modèle **Archiver l'utilisateur**.
4. Depuis le magasin personnel, recherchez le certificat Archiver l'utilisateur.
5. Supprimez le certificat pour qu'Aidan simule une clé perdue.
6. Basculez vers **LON-SVR1**.
7. Ouvrez la console **Autorité de certification**, développez **Adatum-IssuingCA**, puis cliquez sur le magasin de **Certificats délivrés**.
8. Dans la console Autorité de certification, notez le numéro de série du certificat qui a été émis pour Aidan Delaney.
9. Sous LON-SVR1, ouvrez une invite de commandes, et tapez la commande suivante :

```
Certutil –getkey <numéro de série> outputblob
```



Remarque : Remplacez le numéro de série par le numéro de série que vous avez noté.

10. Vérifiez que le fichier **Outputblob** s'affiche désormais dans le dossier C:\Utilisateurs\Administrateur.
11. Pour convertir le fichier **Outputblob** en un fichier importable .pfx, à l'invite de commandes, tapez la commande suivante :

```
Certutil–recoverkey outputblob aidan.pfx.
```

12. Entrez le mot de passe **Pa$$w0rd** pour le certificat.
13. Vérifiez la création de la clé récupérée dans le dossier C:\Utilisateurs\Administrateur.
14. Basculez sur l'ordinateur **LON-CL1**.
15. Ouvrez le **Centre Réseau et partage** dans le Panneau de configuration, pour activer le partage de fichiers et d'imprimantes pour les profils de réseau public ou invité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Repassez à **LON-SVR1**, puis copiez et collez le fichier **aidan.pfx** dans la racine du lecteur C sur LON-CL1.
17. Basculez vers **LON-CL1** et importez le certificat **aidan.pfx**.
18. Vérifiez que le certificat s'affiche dans le magasin personnel.

Résultats : Après avoir terminé cet exercice, vous aurez implémenté l'archivage de clé et testé la récupération de clé privée.

▶ Pour préparer le module suivant :

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-CL1**, **22412B-LON-SVR1**, **22412B-LON-CA1** et **22412B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quelles sont certaines raisons pour lesquelles une organisation utiliserait la PKI ?

Question : Quelles sont certaines raisons pour lesquelles une organisation utiliserait une autorité de certification racine d'entreprise ?

Question : Citez les conditions pour utiliser l'inscription automatique pour des certificats.

Question : Quelles sont les étapes pour configurer un répondeur en ligne ?

Méthode conseillée :

- En déployant l'infrastructure d'autorité de certification, déployez une autorité de certification racine autonome (non joint au domaine) et une autorité de certification d'entreprise secondaire (autorité de certification de publication). Après que l'autorité de certification secondaire d'entreprise reçoit un certificat d'autorité de certification racine, mettez l'autorité de certification racine hors connexion.
- Délivrez un certificat pour l'autorité de certification racine pendant une longue période, comme 15 ou 20 ans.
- Utilisez l'inscription automatique pour les certificats qui sont très utilisés.
- Utilisez un agent d'inscription restreint dès que possible.
- Utilisez les cartes à puce virtuelles pour améliorer la sécurité de l'ouverture de session.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
L'emplacement du certificat d'Autorité de certification qui est spécifié dans l'extension d'accès à l'information d'autorité n'est pas configuré pour inclure le suffixe de nom de certificat. Les clients peuvent ne pas pouvoir localiser la version correcte du certificat d'autorité de certification de publication pour générer une chaîne de certificats, et la validation de certificat peut échouer.	
L'autorité de certification n'est pas configurée pour inclure des emplacements de point de distribution de liste de révocation de certificats dans les extensions des certificats émis. Les clients peuvent ne pas pouvoir localiser une liste de révocation de certificats pour contrôler l'état de révocation d'un certificat, et la validation de certificat peut échouer.	
L'autorité de certification a été installée comme AC d'entreprise, mais des paramètres de stratégie de groupe pour l'inscription automatique d'utilisateur n'ont pas été activés. Une AC d'entreprise peut utiliser l'inscription automatique pour simplifier l'émission et le renouvellement de certificats. Si l'inscription automatique n'est pas activée, l'émission et le renouvellement de certificats peuvent ne pas se produire comme prévu.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Problèmes réels et scénarios

Contoso, Ltd souhaite déployer la PKI pour prendre en charge et sécuriser plusieurs services. Elle a décidé d'utiliser des services de certificats Windows Server 2012 comme plateforme pour la PKI. Les certificats seront principalement utilisés pour EFS, la signature numérique et des serveurs Web. Puisque les documents qui seront chiffrés sont importants, il est crucial d'avoir une stratégie de récupération après sinistre en cas de perte de clé. En outre, les clients qui auront accès aux parties sécurisées du site Web de la société ne doivent recevoir aucun avertissement sur leurs navigateurs.

1. Quel type de déploiement Contoso devrait-elle choisir ?
2. Quel type de certificats Contoso devrait-elle utiliser pour EFS et la signature numérique ?
3. Quel type de certificats Contoso devrait-elle utiliser pour un site Web ?
4. Comment Contoso vérifiera-t-elle que les données chiffrées par EFS ne sont pas perdues si un utilisateur perd un certificat ?

Outils

- Console Autorité de certification
- Console Modèles de certificats
- Console Certificats
- Certutil.exe

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7

Implémentation des services AD RMS (Active Directory Rights Management Services)

Table des matières :

Vue d'ensemble du module **7-1**

Leçon 1 : Vue d'ensemble d'AD RMS **7-2**

Leçon 2 : Déploiement et gestion d'une infrastructure d'AD RMS **7-8**

Leçon 3 : Configuration de la protection du contenu AD RMS **7-15**

Leçon 4: Configuration d'un accès externe à AD RMS **7-22**

Atelier pratique : Implémentation AD RMS **7-27**

Contrôle des acquis et éléments à retenir **7-35**

Vue d'ensemble du module

Les services Active Directory® Management Services (AD RMS) fournissent une méthode pour protéger le contenu qui va au-delà des dispositifs de stockage de chiffrement en utilisant le chiffrement de lecteur Windows® BitLocker® ou des fichiers individuels de chiffrement en utilisant le système de fichiers EFS (Encrypting File System). AD RMS fournit une méthode pour protéger des données en transit ou non, et garantit qu'elles sont accessibles seulement aux utilisateurs autorisés pour une durée spécifique.

Ce module vous présente AD RMS. Il décrit également comment déployer AD RMS, comment configurer la protection du contenu et comment rendre les documents protégés par AD RMS disponibles aux utilisateurs externes.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- fournir une vue d'ensemble d'AD RMS ;
- déployer et gérer une infrastructure d'AD RMS ;
- configurer la protection du contenu AD RMS ;
- configurer un accès externe à AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble d'AD RMS

Avant de déployer AD RMS, vous devez savoir comment AD RMS fonctionne, quels composants sont compris dans un déploiement des services AD RMS et comment vous devez déployer AD RMS. Vous devez également comprendre les concepts derrière divers certificats et licences AD RMS.

Cette leçon fournit une vue d'ensemble d'AD RMS et les scénarios dans lesquels vous pouvez l'utiliser pour protéger les données confidentielles de votre organisation.

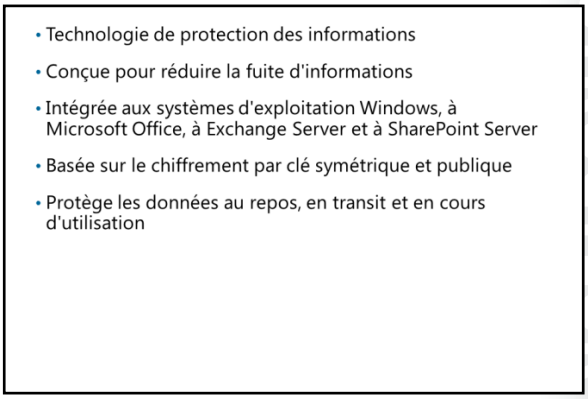
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire AD RMS ;
- expliquer les scénarios dans lesquels vous pouvez utiliser AD RMS ;
- lister les composants d'AD RMS ;
- lister les différents certificats et licences AD RMS ;
- expliquer le fonctionnement d'AD RMS.

Qu'est-ce qu'AD RMS ?

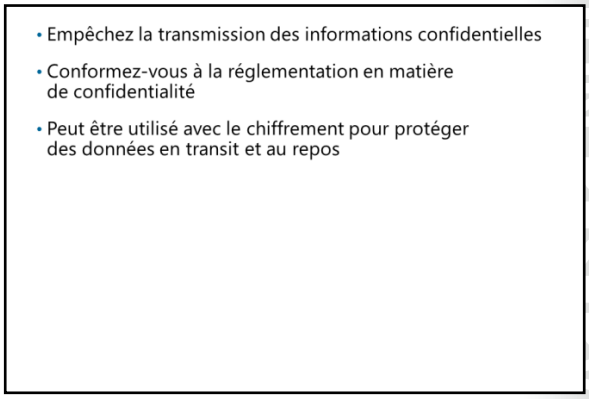
AD RMS est une technologie de protection de l'information qui est conçue pour réduire les fuites de données potentielles. *La fuite de données* est la transmission non autorisée d'informations, soit à des personnes de l'organisation, soit à des personnes en dehors de l'organisation, qui ne devraient pas pouvoir accéder à ces informations. AD RMS s'intègre aux produits et systèmes d'exploitation Microsoft® comprenant Windows Server®, Microsoft Exchange Server, Microsoft SharePoint® Serveur et la suite Microsoft Office.



AD RMS peut protéger des données en transit et au repos. Par exemple, AD RMS peut protéger des documents qui sont envoyés comme messages électroniques en garantissant qu'un message ne peut pas être ouvert même s'il est par erreur adressé au mauvais destinataire. Vous pouvez également utiliser AD RMS pour protéger des données qui sont enregistrées sur des périphériques tels que les lecteurs USB amovibles. Un inconvénient des autorisations de fichier et dossier est qu'une fois le fichier copié vers un autre emplacement, les autorisations originales ne s'appliquent plus. Un fichier qui est copié sur un lecteur USB héritera des autorisations présentes sur le périphérique de destination. Une fois copié, un fichier qui était en lecture seule peut être rendu modifiable en changeant les autorisations de fichier et de dossier. Avec AD RMS, le fichier peut être protégé dans n'importe quel emplacement, indépendamment des autorisations de fichier et de dossier qui accordent l'accès. Avec AD RMS, seuls les utilisateurs qui sont autorisés à ouvrir le fichier pourront afficher le contenu de ce fichier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Scénarios d'utilisation d'AD RMS



La principale utilisation pour AD RMS est de contrôler la distribution des informations confidentielles. Vous pouvez utiliser AD RMS en association avec des techniques de chiffrement pour sécuriser les données quand elles sont stockées ou en transit. Il peut y avoir beaucoup de raisons de contrôler la distribution des informations confidentielles, comme devoir vérifier que seuls les membres du personnel autorisés ont accès à un fichier, en garantissant que des messages électroniques sensibles ne puissent pas être transférés ou que les détails d'un projet non publié ne soient pas rendus publiques. Prenez les scénarios suivants :

Scénario 1

Le président-directeur général (PDG) copie un fichier tableur contenant les formules d'indemnisation des cadres d'une organisation provenant d'un dossier protégé sur un serveur de fichiers vers le lecteur USB personnel du PDG. En rentrant chez lui, le PDG laisse le lecteur USB dans le train, où une personne sans rapport avec l'organisation le trouve. Sans AD RMS, celui qui trouve le lecteur USB peut ouvrir le fichier. Avec AD RMS, il est possible de s'assurer que le fichier ne peut pas être ouvert par des utilisateurs non autorisés.

Scénario 2

Un document interne doit être visualisable par un groupe de personnes autorisées au sein de l'organisation. Ces personnes ne doivent pas pouvoir modifier ou imprimer le document. S'il est possible d'utiliser la fonctionnalité native de Microsoft Office Word pour restreindre ces fonctionnalités, y procéder exige que chaque personne possède un compte Windows Live®. Avec AD RMS, vous pouvez configurer ces autorisations selon des comptes existants dans les services de domaine Active Directory (AD DS).

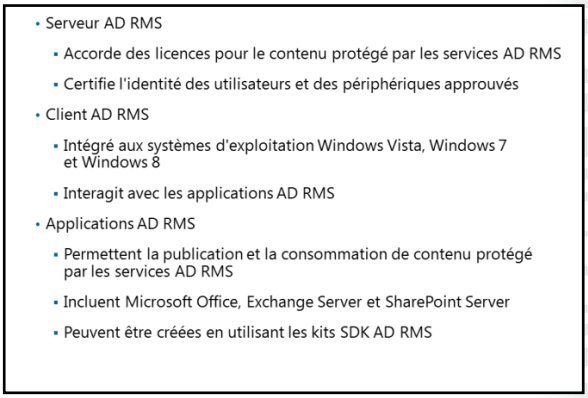
Scénario 3

Les personnes de l'organisation ne doivent pas pouvoir transférer des messages électroniques sensibles qui ont été attribués à une classification particulière. Avec AD RMS, vous pouvez autoriser un expéditeur à attribuer une classification particulière à un nouveau message électronique, et cette classification garantira que le destinataire ne puisse pas transférer le message.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des composants AD RMS

Le cluster de certification racine d'AD RMS est le premier serveur AD RMS que vous déployez dans une forêt. Le cluster de certification racine d'AD RMS gère tout le trafic d'octroi de licence et de certification pour le domaine dans lequel il est installé. AD RMS stocke des données de configuration dans une base de données Microsoft SQL Server® ou dans la base de données interne de Windows. Dans de grands environnements, la base de données SQL Server est hébergée sur un serveur qui est séparé du serveur qui héberge le rôle AD RMS.



Des clusters d'administration de licences AD RMS sont utilisés dans les environnements distribués. Les clusters d'administration de licences ne fournissent pas la certification, mais permettent la distribution des licences qui sont utilisées pour la consommation et la publication de contenu. Des clusters d'administration de licences sont souvent déployés dans de grandes filiales dans les organisations qui utilisent AD RMS.

Serveur AD RMS

Les serveurs AD RMS doivent être des membres d'un domaine AD DS. Quand vous installez AD RMS, des informations sur l'emplacement du cluster sont publiées sur AD DS vers un emplacement appelé le point de connexion de service. Les ordinateurs qui sont membres du domaine interrogent le point de connexion de service pour déterminer l'emplacement des services AD RMS.

Client AD RMS

Le client AD RMS est généré dans les systèmes d'exploitation Windows Vista®, Windows 7 et Windows 8. Le client AD RMS autorise à des applications AD RMS d'appliquer la fonctionnalité dictée par le modèle AD RMS. Sans client AD RMS, les applications AD RMS ne pourraient pas interagir avec contenu protégé par les services AD RMS.

Applications AD RMS

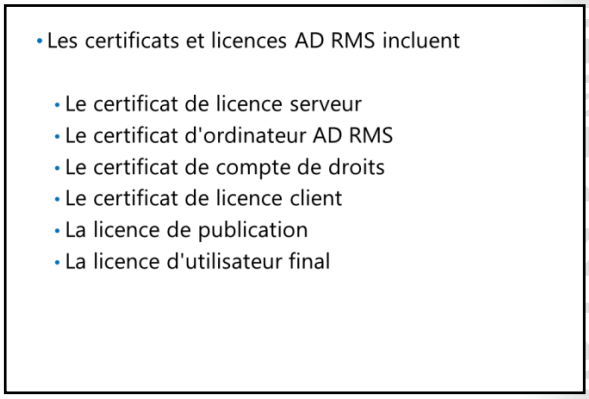
Les applications AD RMS permettent à des utilisateurs de créer et consommer du contenu protégé par les services AD RMS. Par exemple, Microsoft Outlook® permet à des utilisateurs d'afficher et de créer des messages électroniques protégés. Office Word permet aux utilisateurs d'afficher et de créer des documents protégés de traitement de texte. Microsoft fournit un kit de développement logiciel (SDK) AD RMS pour permettre aux développeurs d'activer leurs applications afin de prendre en charge la protection du contenu par AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Certificats et licences AD RMS

Pour comprendre comment AD RMS fonctionne, vous devez être familiarisé avec ses différents types de certificats et de licences. Chacun de ces certificats et licences fonctionne d'une manière différente. Quelques certificats, tels que le certificat de licence serveur (SLC), sont très importants et vous devez les sauvegarder régulièrement.



SLC

Le SLC est généré quand vous créez le cluster AD RMS. Il a une validité de 250 ans. Le SLC permet au cluster AD RMS d'émettre :

- des SLC à d'autres serveurs du cluster ;
- des certificats de compte de droits aux clients ;
- des certificats de licence client ;.
- des licences de publication ;
- des licences d'utilisation ;
- des modèles de stratégies de droits.

La clé publique du SLC chiffre la clé de contenu dans une licence de publication. Cela permet au serveur AD RMS d'extraire la clé de contenu et d'émettre des licences d'utilisateur final en fonction de la clé de publication.

Certificat d'ordinateur AD RMS

Le certificat d'ordinateur AD RMS est utilisé pour identifier un ordinateur ou un périphérique approuvé. Ce certificat identifie le référentiel sécurisé de l'ordinateur client. La clé publique du certificat d'ordinateur chiffre la clé privée du certificat de compte de droits. La clé privée du certificat d'ordinateur déchiffre les certificats de compte de droits.

Certificat de compte de droits

Le certificat de compte de droits (RAC) identifie un utilisateur spécifique. La durée de validité par défaut pour un certificat de compte de droits est de 365 jours. Les certificats de comptes de droits peuvent seulement être publiés aux utilisateurs dans AD DS dont les comptes d'utilisateur ont des adresses de messagerie qui sont associées à ces derniers. Un certificat de compte de droits est publié la première fois qu'un utilisateur essaye d'accéder à un contenu protégé par les services AD RMS. Vous pouvez régler la durée de validité par défaut en utilisant le nœud de stratégies de certificat de compte de droits de la console AD RMS.

Un certificat de compte de droits provisoire a une durée de validité de 15 minutes. Les certificats de comptes de droits provisoires sont publiés quand un utilisateur accède à du contenu protégé par les services AD RMS à partir d'un ordinateur qui n'est pas membre de la même forêt ou forêt approuvée que le cluster AD RMS. Vous pouvez régler la durée de validité par défaut en utilisant le nœud de stratégies de certificat de compte de droits de la console AD RMS.

AD RMS prend en charge les certificats de comptes de droits supplémentaires suivants :

- les certificats de comptes de droits de services AD FS (Active Directory Federation Services) sont publiés pour les utilisateurs fédérés. Ils ont une validité de sept jours.
- Deux types de certificat de compte de droits Windows Live ID sont pris en charge. Les certificats de comptes de droits Windows Live ID utilisé sur les ordinateurs privés ont une validité de six mois ; les certificats de comptes de droits Windows Live ID utilisés sur les ordinateurs publics sont valides jusqu'à ce que l'utilisateur ferme sa session.

Certificat de licence client

Un certificat de licence client permet à un utilisateur de publier du contenu protégé par les services AD RMS quand l'ordinateur client n'est pas connecté au même réseau que le cluster AD RMS. La clé publique de certificat de licence client chiffre la clé de contenu symétrique et l'inclut dans la licence de publication qu'elle émet. La clé privée du certificat de licence client signe toutes les licences de publication qui sont publiées quand le client n'est pas connecté au cluster AD RMS.

Des certificats de licence client sont liés au certificat de compte de droits spécifique d'un utilisateur. Si un autre utilisateur qui n'a pas obtenu de certificat de compte de droits tente de publier du contenu protégé par les services AD RMS à partir du même client, il ne le pourra pas jusqu'à ce que le client soit connecté au cluster AD RMS et puisse émettre un certificat de compte de droits à l'utilisateur.

Licence de publication

Une licence de publication (PL) détermine les droits qui s'appliquent au contenu protégé par les services AD RMS. Par exemple, la licence de publication détermine si l'utilisateur peut modifier, imprimer ou enregistrer un document. La licence de publication contient la clé de contenu ; celle-ci est chiffrée en utilisant la clé publique du service de gestion de licences. Elle contient également l'URL et la signature numérique du serveur AD RMS.

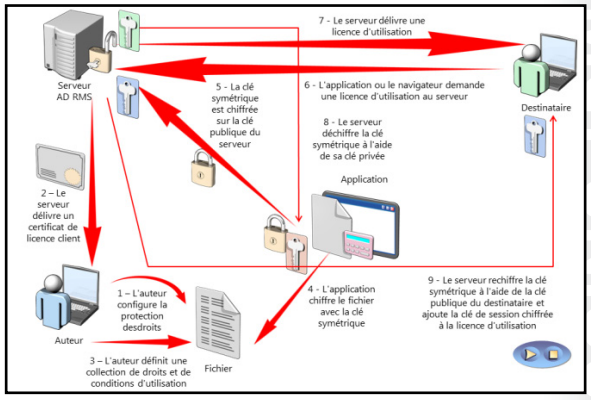
Licence d'utilisateur final

Une licence d'utilisateur final est requise pour consommer le contenu protégé par les services AD RMS. Le serveur AD RMS émet une licence d'utilisateur final par utilisateur par document. Des licences d'utilisateur final sont mises en cache par défaut.

Comment AD RMS fonctionne-t-il ?

AD RMS fonctionne de la façon suivante :

1. La première fois que l'auteur du document configure la protection des droits pour le document, un certificat de licence client sera demandé par le serveur AD RMS.
2. Le serveur fournit alors le certificat de licence client au client.
3. Quand l'auteur reçoit le certificat du serveur AD RMS, il ou elle peut configurer des droits d'utilisation sur le document.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Quand l'auteur configure des droits d'utilisation, l'application chiffre le fichier avec une clé symétrique.
5. Cette clé symétrique est chiffrée sur la clé publique du serveur AD RMS qui est utilisé par l'auteur.
6. Le destinataire du fichier l'ouvre à l'aide d'une application ou d'un navigateur AD RMS. Il n'est pas possible d'ouvrir du contenu protégé par les services AD RMS à moins que l'application ou le navigateur ne prenne en charge AD RMS. Si le destinataire ne possède pas de certificat de compte sur le dispositif actuel, c'est à ce stade qu'un certificat est fourni à l'utilisateur. L'application ou le navigateur communique une demande de licence d'utilisation au serveur AD RMS de l'auteur.
7. Le serveur AD RMS détermine si le destinataire est autorisé. Si le destinataire est autorisé, le serveur AD RMS émet une licence d'utilisation.
8. Le serveur AD RMS déchiffre la clé symétrique qui a été chiffrée dans l'étape 3, en utilisant sa clé privée.
9. Le serveur AD RMS re-chiffre la clé symétrique en utilisant la clé publique du destinataire et ajoute la clé de session chiffrée à la licence d'utilisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Déploiement et gestion d'une infrastructure d'AD RMS

Avant de déployer AD RMS, il est important d'avoir un plan de déploiement qui est approprié pour l'environnement de votre organisation. Le déploiement des services AD RMS dans une forêt à domaine unique est différent du déploiement des services AD RMS dans des scénarios où vous devez prendre en charge la publication et la consommation du contenu dans plusieurs forêts, vers des organisations partenaires approuvées ou sur l'Internet public. Avant de déployer AD RMS, vous devez également comprendre les configurations requises du client et avoir une stratégie appropriée pour sauvegarder et récupérer AD RMS.

Cette leçon fournit une vue d'ensemble du déploiement d'AD RMS et des étapes que vous devez suivre pour sauvegarder, récupérer et désaffecter une infrastructure AD RMS.

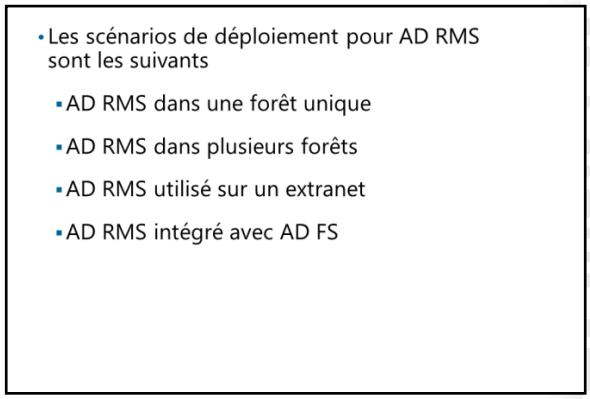
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire des scénarios de déploiement des services AD RMS ;
- configurer le cluster AD RMS ;
- expliquer comment installer le premier serveur d'un cluster AD RMS ;
- décrire la configuration requise du client AD RMS ;
- expliquer comment implémenter une stratégie de sauvegarde et de restauration AD RMS ;
- expliquer comment désaffecter et supprimer AD RMS.

Scénarios de déploiement AD RMS

Un déploiement des services AD RMS se compose d'un ou plusieurs serveurs appelés un *cluster*. Un cluster AD RMS n'est pas un cluster de basculement facilement disponible. Quand vous déployez AD RMS, vous devez héberger le serveur de sorte qu'il soit hautement disponible. AD RMS est généralement déployé comme ordinateur virtuel hautement disponible.



Quand vous déployez AD RMS dans une forêt unique, vous avez un cluster AD RMS unique. C'est la forme la plus commune de déploiement des services AD RMS. Vous ajoutez autant de serveurs au cluster AD RMS que nécessaire, pour fournir une capacité supplémentaire.

Quand vous déployez AD RMS dans plusieurs forêts, chaque forêt doit avoir son propre cluster racine AD RMS. Il est nécessaire de configurer des domaines de publication approuvés AD RMS pour garantir que le contenu AD RMS peut être protégé et consommé dans les diverses forêts.

Vous pouvez également déployer AD RMS sur des emplacements extranet. Dans ce déploiement, le serveur de licences AD RMS est accessible aux hôtes sur Internet. Vous utilisez ce type de déploiement pour prendre en charge la collaboration avec des utilisateurs externes.

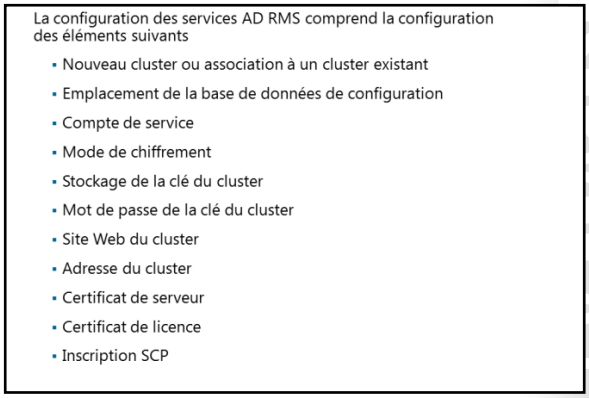
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez déployer AD RMS avec AD FS ou Microsoft Federation Gateway. Dans ce scénario, les utilisateurs tirent profit de l'identité fédérée pour publier et consommer le contenu protégé par des droits.

Il est recommandé de ne pas déployer AD RMS sur un contrôleur de domaine. Vous pouvez seulement déployer AD RMS sur un contrôleur de domaine si le compte du service est un membre du groupe Administrateurs du domaine.

Configuration du cluster AD RMS

Une fois que vous avez déployé le rôle de serveur AD RMS, vous devez configurer le cluster AD RMS avant qu'il soit possible d'utiliser AD RMS. La configuration du cluster AD RMS implique la configuration des composants suivants :



1. Cluster AD RMS. Choisissez de créer un nouveau cluster racine AD RMS ou de rejoindre un cluster existant.
2. Base de données de configuration. Choisissez d'utiliser une instance SQL Server existante dans laquelle enregistrer la base de données de configuration AD RMS ou configurer et installer la base de données interne Windows localement. Vous pouvez utiliser SQL Server 2008, SQL Server 2008 R2 ou SQL Server 2012 pour prendre en charge un déploiement des services AD RMS dans Windows Server 2012. Il est recommandé d'utiliser une base de données SQL Server qui est hébergée sur un serveur distinct.
3. Compte de service. Microsoft recommande d'utiliser un compte d'utilisateur du domaine standard avec des autorisations supplémentaires. Vous pouvez utiliser un compte de service géré comme compte de service AD RMS.
4. Mode de chiffrement. Choisissez la force du chiffrement utilisé avec AD RMS.
   - Le mode de chiffrement 2 utilise les clés RSA 2048 bits et les hachages SHA-256.
   - Le mode de chiffrement 1 utilise les clés RSA 1045 bits et les hachages SHA-1.
5. Stockage de clé de cluster. Choisissez l'endroit où la clé de cluster est enregistrée. Vous pouvez l'enregistrer dans AD RMS ou utiliser un fournisseur de services de chiffrement spécial (CSP). Si vous choisissez d'utiliser un fournisseur de services de chiffrement et souhaitez ajouter des serveurs supplémentaires, vous devez distribuer la clé manuellement.
6. Mot de passe de clé de cluster. Ce mot de passe chiffre la clé de cluster et est requis si vous souhaitez joindre d'autresserveurs AD RMS au cluster ou si vous souhaitez restaurer le cluster à partir de la sauvegarde.
7. Site Web de cluster. Choisissez quel site Web sur le serveur local hébergera le site Web de cluster AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Adresse du cluster. Spécifiez le nom de domaine complet (FQDN) à utiliser avec le cluster. Vous avez le choix entre un site Web chiffré avec Secure Sockets Layer (SSL) et chiffré sans SSL. Si vous choisissez un chiffrement sans SSL, vous ne pourrez pas ajouter la prise en charge de la fédération d'identité. Une fois que vous avez défini l'adresse et le port du cluster, vous ne pouvez pas les modifier sans supprimer complètement AD RMS.
9. Certificat de licence. Choisissez le nom convivial que le SLC utilisera. Il doit représenter la fonction du certificat.
10. Enregistrement d'un point de connexion de service. Choisissez si le point de connexion de service est inscrit dans AD DS quand le cluster AD RMS est créé. Le point de connexion de service permet aux ordinateurs qui sont membres du domaine de localiser automatiquement le cluster AD RMS. Seuls les utilisateurs qui sont membres du groupe Administrateurs de l'entreprise peuvent inscrire le point de connexion de service. Vous pouvez effectuer cette étape après la création du cluster AD RMS ; vous ne devez pas l'effectuer pendant le processus de configuration.

Démonstration : Installation du premier serveur d'un cluster AD RMS

Dans cette démonstration, vous verrez comment déployer AD RMS sur un ordinateur qui exécute Windows Server 2012.

Procédure de démonstration

Configurer un compte de service

1. Utilisez le Centre d'administration Active Directory pour créer une unité d'organisation (OU) nommée **Comptes de service** dans le domaine adatum.com.
2. Créez un nouveau compte d'utilisateur dans l'unité d'organisation Comptes de service en indiquant les propriétés suivantes :
   - Prénom : **ADRMSSVC**
   - Nom d'ouverture de session de l'utilisateur principal : **ADRMSSVC**
   - Mot de passe : **Pa$$w0rd**
   - Confirmer le mot de passe : **Pa$$w0rd**
   - Le mot de passe n'expire jamais : **Activé**
   - L'utilisateur ne peut pas changer de mot de passe : **Activé**

Préparer un DNS

- Utilisez la console du Gestionnaire DNS pour créer un enregistrement de ressource hôte (A) dans la zone adatum.com avec les propriétés suivantes :
  - Nom : **adrms**
  - Adresse IP : **172.16.0.21**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Installer le rôle AD RMS

1. Connectez-vous à LON-SVR1 avec le compte **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Utilisez l'Assistant Ajout de rôles et de fonctionnalités pour ajouter le rôle AD RMS à LON-SVR1 en utilisant l'option suivante :
   - Services de rôle : **Services du serveur AD RMS**

Configurer AD RMS

1. Dans le Gestionnaire de serveur, à partir du nœud **AD RMS**, cliquez sur **Plus** pour commencer la configuration de post-déploiement d'AD RMS.
2. Dans l'Assistant de Configuration d'AD RMS, fournissez les informations ci-dessous :
   - **Créer un nouveau cluster racine AD RMS**
   - **Utiliser la base de données interne de Windows sur ce serveur**
   - **Utiliser Adatum\ADRMSSVC comme compte de service**
   - Mode de chiffrement : **Mode de chiffrement 2**
   - Stockage de clé de cluster : **Utiliser le stockage de clé AD RMS géré de manière centralisée**
   - Mot de passe de clé de cluster : **Pa$$w0rd**
   - Site Web de cluster : **Site Web par défaut**
   - Type de connexion : **Utiliser une connexion non chiffrée**
   - Nom de domaine complet : **http://adrms.adatum.com**
   - Port : **80**
   - Certificat de licence : **Adatum AD RMS**
   - Enregistrer un point de connexion de service AD RMS : **Enregistrer le point de connexion de service maintenant**
3. Déconnectez-vous de LON-SVR1.

Remarque : Vous devez vous déconnecter avant de pouvoir gérer AD RMS

Configuration requise pour le client AD RMS

Le contenu d'AD RMS peut seulement être publié et consommé par des ordinateurs qui exécutent le client AD RMS. Toutes les versions des systèmes d'exploitation clients Windows Vista, Windows 7 et Windows 8 comprennent le logiciel client AD RMS. Les systèmes d'exploitation Windows Server 2008, Windows Server 2008 R2 et Windows Server 2012 comprennent également le client AD RMS.
Ces systèmes d'exploitation n'exigent pas de configuration supplémentaire pour consommer et publier le contenu protégé par AD RMS.

- Client inclus dans les systèmes d'exploitation Windows Vista, Windows 7 et Windows 8
- Client inclus dans les systèmes d'exploitation Windows Server 2008, Windows Server 2008 R2 et Windows Server 2012
- Client téléchargeable pour les versions précédentes des systèmes d'exploitation Windows et pour Mac OS X
- Les applications AD RMS comprennent Office 2007, Office 2010 et Office 2013
- Exchange Server 2007, Exchange Server 2010 et Exchange Server 2013 prennent en charge les services AD RMS
- Le client AD RMS a besoin d'une licence d'accès client RMS

Le logiciel client AD RMS est téléchargeable sur les ordinateurs qui exécutent le système d'exploitation Microsoft Windows XP et Mac OS X. Ce logiciel client doit être installé avant qu'il soit possible pour les utilisateurs de ces systèmes d'exploitation de consommer et de publier du contenu protégé par –AD RMS.

AD RMS requiert des applications compatibles. Les applications serveur qui prennent en charge AD RMS comprennent ce qui suit :

- Microsoft Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013
- Microsoft Office SharePoint Server 2007
- SharePoint Server 2010
- SharePoint Server 2013

Les applications clientes, comme celles comprises dans Microsoft Office 2003, Office 2007, Office 2010 et Office 2013, peuvent publier et consommer du contenu protégé par les services AD RMS. Vous pouvez utiliser le kit de développement logiciel AD RMS pour créer des applications qui peuvent publier et consommer le contenu protégé par AD RMS. La Visionneuse XPS et Windows Internet Explorer® sont également en mesure d'afficher du contenu protégé par AD RMS.

 **Remarque :** Microsoft a sorti la nouvelle version du logiciel client AD RMS : AD RMS Client 2.0. Il est possible de le télécharger à partir du centre de téléchargement Microsoft. Notamment, la nouvelle version fournit un nouveau kit de développement logiciel que vous pouvez également télécharger à partir du Centre de téléchargement Microsoft. Le nouveau kit de développement logiciel AD RMS fournit un mécanisme simple pour que les développeurs créent des applications et des solutions qui protègent et consomment le contenu critique. Avec le nouveau kit de développement logiciel il est maintenant possible d'activer les droits d'applications et de solutions beaucoup plus rapidement et plus facilement qu'avant.

Ajout de licences client AD RMS

Pour utiliser des services RMS dans votre environnement AD DS, vous devez avoir des licences d'accès client (CAL) Windows Rights Management. Ces licences d'accès client sont différentes des CAL Windows Server dont vous avez besoin pour connecter le client au serveur. Chaque utilisateur qui créera ou utilisera des fichiers protégés par des droits devra avoir une licence d'accès client utilisateur RMS. Sinon, vous pouvez également utiliser les CAL du périphérique RMS pour les ordinateurs qui seront utilisés pour créer et afficher le contenu protégé par RMS.

Si vous devez partager votre contenu protégé par RMS en dehors de votre organisation, vous devrez acquérir une licence de connecteur externe RMS. Cette licence donne à des organismes le droit d'autoriser à un nombre illimité d'utilisateurs externes d'accéder ou d'utiliser à une copie unique sous licence du logiciel de serveur RMS sans avoir besoin d'acquérir des licences d'accès client pour chaque utilisateur externe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémentation d'une stratégie de sauvegarde et de restauration AD RMS

- Faites une sauvegarde de la clé privée et des certificats
- Assurez-vous que la base de données AD RMS est sauvegardée régulièrement
- Exportez les modèles pour les sauvegarder
- Exécutez le serveur AD RMS comme ordinateur virtuel et effectuez la sauvegarde complète du serveur

Pour empêcher toute perte de données,vous devez vérifier que le serveur AD RMS est sauvegardé de telle manière qu'il puisse être récupéré en cas de corruption de fichier ou de défaillance du serveur. Si le serveur AD RMS devient inaccessible, tout le contenu protégé par les services AD RMS devient également inaccessible.

Une stratégie simple pour implémenter la sauvegarde et la restauration d'AD RMS est d'exécuter le serveur AD RMS comme ordinateur virtuel, puis d'utiliser un produit de sauvegarde d'entreprise tel que le gestionnaire de protection des données Microsoft System Center 2012 pour effectuer des copies de sauvegarde régulières de l'ordinateur virtuel. Certains des composants importants qui requièrent des copies de sauvegarde sont la clé privée, les certificats, la base de données d'AD RMS et des modèles. Vous pouvez également effectuer une sauvegarde de serveur entier, en exécutant AD RMS sur un ordinateur virtuel.

Il est recommandé de sauvegarder la clé privée d'AD RMS et tous les certificats utilisés par AD RMS. La méthode la plus simple pour y procéder est d'exporter les certificats vers un emplacement sûr. Vous devez également sauvegarder la base de données d'AD RMS régulièrement. La méthode que vous utilisez pour faire cela varie selon si AD RMS utilise SQL Server ou la base de données interne Windows. Pour sauvegarder des modèles, configurez les modèles à exporter vers un dossier partagé, puis sauvegardez ces modèles.

Quand vous effectuez la récupération du rôle AD RMS, il peut être nécessaire de supprimer l'objet **ServiceConnectionPoint** d'AD DS. Vous devez le faire si vous récupérez un serveur de configuration racine d'AD RMS et que le serveur tente de se mettre en service en tant que serveur d'administration de licences.

Désaffectation et suppression d'AD RMS

- Désaffectez un cluster AD RMS avant de le supprimer
  - La désaffectation fournit une clé qui déchiffre le contenu AD RMS précédemment publié
  - Laissez le serveur désaffecté jusqu'à ce que tout le contenu protégé par les services AD RMS soit migré
- Exportez le certificat de licence serveur avant de désinstaller le rôle AD RMS

Avant de supprimer un serveur AD RMS, vous devez désaffecter ce serveur. La désaffectation d'AD RMS met le cluster dans un état où les consommateurs de contenu protégé par AD RMS peuvent obtenir des clés spéciales qui déchiffrent ce contenu, indépendamment des restrictions existantes qui ont été imposées à l'utilisation de ce contenu. Si vous n'avez pas de période de désaffectation et si vous supprimez simplement le serveur AD RMS, le contenu protégé par AD RMS deviendra alors inaccessible.

Pour désaffecter AD RMS, procédez comme suit :

1. Connectez-vous au serveur qui héberge AD RMS et que vous souhaitez désaffecter.
2. Modifiez la liste de contrôle d'accès (ACL) du fichier decommissioning.asmx. Accordez au groupe Tout le monde l'autorisation **Lecture et exécution** sur le fichier. Ce fichier est enregistré dans le dossier %systemdrive%\inetpub\wwwroot_wmcs\decomission.
3. Dans la console AD RMS, développez le nœud **Stratégies de sécurité**, puis cliquez sur le nœud **Désaffectation**.
4. Dans le volet Actions, cliquez sur **Activer la désaffectation**.
5. Cliquez sur **Désaffectation**.
6. Lorsque vous êtes invité à confirmer que vous souhaitez désaffecter le serveur, cliquez sur **Oui**.

Après la fin du processus de désaffectation d'AD RMS, vous devez exporter le certificat de licence serveur avant de désinstaller le rôle AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration de la protection du contenu AD RMS

AD RMS utilise des modèles de stratégie de droits pour appliquer un ensemble cohérent de stratégies pour protéger le contenu. En configurant AD RMS, vous devez développer des stratégies pour garantir que les utilisateurs peuvent encore accéder au contenu protégé à partir d'un ordinateur qui n'est pas connecté au cluster AD RMS. Vous devez également développer des stratégies pour empêcher certains utilisateurs de pouvoir accéder au contenu protégé par les services AD RMS et des stratégies pour garantir que le contenu protégé peut être récupéré au cas où il expire, le modèle est supprimé ou si l'auteur du contenu n'est plus disponible.

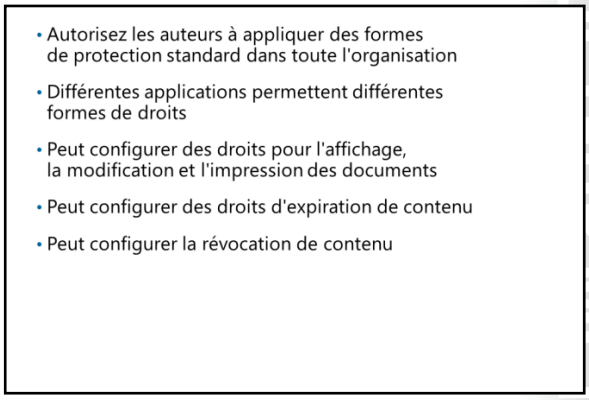
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire la fonction des modèles de stratégie de droits ;
- expliquer comment créer un modèle de stratégie de droits ;
- expliquer comment implémenter des stratégies pour garantir que des modèles de stratégie de droits sont disponibles pour une utilisation hors connexion ;
- décrire les stratégies d'exclusion ;
- expliquer comment créer une stratégie d'exclusion pour exclure une application ;
- implémenter un groupe de super utilisateurs d'AD RMS.

Que sont les modèles de stratégies de droits ?

Les modèles de stratégie de droits vous permettent de configurer des méthodes standard d'implémentation des stratégies AD RMS dans l'organisation. Par exemple, vous pouvez configurer des modèles standard qui accordent des droits d'affichage uniquement, bloquent la capacité de modifier, d'enregistrer et d'imprimer, ou si utilisé avec Exchange Server, bloquent la capacité de transférer ou de répondre aux messages.



Les modèles de stratégie de droits sont créés en utilisant la console AD RMS. Ils sont enregistrés dans la base de données d'AD RMS et peuvent également être enregistrés au format XML. Quand le contenu est consommé, le client utilise AD RMS pour vérifier qu'il a la dernière version du modèle.

Un auteur de document peut choisir de protéger le contenu en appliquant un modèle existant. Cela est fait en utilisant une application prenant en charge AD RMS. Par exemple, dans Office Word, vous appliquez un modèle à l'aide de la fonction **Protéger le document**. Quand vous faites cela, Office Word interroge AD DS pour déterminer l'emplacement du serveur AD RMS. Une fois l'emplacement du serveur AD RMS acquis, les modèles qui sont à la disposition de l'auteur de contenu peuvent être utilisés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les modèles AD RMS prennent en charge les droits suivants :

- **Contrôle total**. Donne à un utilisateur le contrôle total sur un document protégé par AD RMS.
- **Afficher**. Donne à un utilisateur la capacité d'afficher un document protégé par AD RMS.
- **Modifier**. Permet à un utilisateur de modifier un document protégé par AD RMS.
- **Enregistrer**. Permet à un utilisateur d'utiliser la fonction **Enregistrer** avec un document protégé par AD RMS.
- **Exporter (Enregistrer sous)**. Permet à un utilisateur d'utiliser la fonction **Enregistrer sous** avec un document protégé par AD RMS.
- **Imprimer**. Permet d'imprimer un document protégé par AD RMS.
- **Transférer**. Utilisé avec Exchange Server. Permet au destinataire d'un message protégé par AD RMS de transférer ce message.
- **Répondre**. Utilisé avec Exchange Server. Permet au destinataire d'un message protégé par AD RMS de répondre à ce message.
- **Répondre à tous**. Utilisé avec Exchange Server. Permet au destinataire d'un message protégé par AD RMS d'utiliser la fonction Répondre à tous pour ce message.
- **Extraire**. Permet à l'utilisateur de copier des données à partir du fichier. Si ce droit n'est pas accordé, l'utilisateur ne peut pas copier de données à partir du fichier.
- **Autoriser les macros**. Permet à l'utilisateur d'utiliser des macros.
- **Afficher les droits**. Permet à l'utilisateur d'afficher les droits attribués.
- **Modifier les droits**. Permet à l'utilisateur de modifier les droits attribués.

Les droits peuvent seulement être accordés et ne peuvent pas être explicitement refusés. Par exemple, pour vérifier qu'un utilisateur ne peut pas imprimer un document, le modèle associé au document ne doit pas comprendre le droit **Imprimer**.

Les administrateurs peuvent également créer des droits personnalisés qui peuvent être utilisés avec des applications prenant en charge AD RMS.

Les modèles AD RMS peuvent également être utilisés pour configurer des documents avec les propriétés suivantes :

- **Expiration du contenu**. Détermine quand le contenu expire. Les options sont les suivantes :
  - **Jamais**. Le contenu n'expire jamais.
  - **Expire à une date particulière**. Le contenu expire à une date et heure particulières.
  - **Expire après**. Le contenu expire un nombre de jours particulier après sa création.
- **Expiration de la licence d'utilisation**. Détermine l'intervalle de temps au cours duquel la licence d'utilisation expirera et une nouvelle devra être acquise.
- **Permettre aux utilisateurs d'afficher le contenu protégé à l'aide d'un composant additionnel du navigateur**. Permet d'afficher le contenu en utilisant un composant additionnel du navigateur. Ne requiert pas que l'utilisateur ait une application prenant en charge AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- **Demander une nouvelle licence d'utilisation à chaque accès au contenu**. Quand vous activez cette option, la mise en cache côté client est désactivée. Cela signifie que le document ne peut pas être consommé quand l'ordinateur est hors connexion.
- **Stratégies de révocation**. Permet l'utilisation d'une liste de révocation. Cela permet à un auteur de révoquer l'autorisation de consommer le contenu. Vous pouvez spécifier combien de fois la liste de révocation est activée, une fois toutes les 24 heures étant la valeur par défaut.

Une fois qu'un modèle de stratégie AD RMS est appliqué à un document, toutes les mises à jour de ce modèle seront également appliquées à ce document. Par exemple, si vous avez un modèle sans stratégie de contenu d'expiration qui est utilisé pour protéger des documents et que vous modifiez ce modèle pour inclure une stratégie de contenu d'expiration, ces documents protégés auront maintenant une stratégie d'expiration. Des modifications de modèle sont répercutées quand la licence d'utilisateur final est acquise. Si les licences d'utilisateur final sont configurées pour ne pas expirer et que l'utilisateur qui accède au document a déjà une licence, alors elles peuvent ne pas recevoir le modèle mis à jour.

 **Remarque :** Vous devez éviter de supprimer des modèles car les documents qui utilisent ces modèles deviendront inaccessibles à tout le monde excepté aux membres du groupe de super utilisateurs. Il est recommandé d'archiver les modèles au lieu de les supprimer.

Vous pouvez afficher les droits associés à un modèle en sélectionnant le modèle dans la console AD RMS, puis dans le menu Actions en cliquant sur **Afficher un résumé des droits**.

Démonstration : Création d'un modèle de stratégie de droits

Dans cette démonstration, vous verrez comment créer un modèle de stratégie de droits qui permet à des utilisateurs d'afficher un document, mais sans exécuter d'autres actions.

Procédure de démonstration

- Dans la console AD RMS, utilisez le nœud de modèle de stratégie de droits pour créer un modèle de stratégie de droits distribué avec les propriétés suivantes :
  - Langue : **français (France)**
  - Nom : **ReadOnly**
  - Description : **Accès en lecture seule. Aucune copie ou impression.**
  - Utilisateurs et droits : **executives@adatum.com**
  - Droits pour n'importe qui : **Vue**
  - **Octroyer le contrôle total au propriétaire (auteur) sans date d'expiration**
  - Expiration du contenu : Expire après **7** jours
  - Expiration de la licence d'utilisation : Expire après **7** jours
  - Demander une nouvelle licence d'utilisation à chaque accès au contenu (désactiver la mise en cache côté client) : **Activé**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fourniture de modèles de stratégie de droits pour une utilisation hors connexion

Si les utilisateurs comptent publier des modèles connectés à AD RMSquand ils ne sont pas connectés au réseau, vous devez vérifier qu'ils ont accès à une copie locale des modèles de stratégie de droits disponibles.

- Assurez-vous que les modèles sont publiés dans un dossier partagé
- Activez la tâche planifiée (automatisée) de gestion des modèles de stratégie de droits AD RMS
- Modifiez la clé de Registre et spécifiez l'emplacement du dossier partagé

Vous pouvez configurer les ordinateurs pour qu'ils obtiennent et enregistrent automatiquement les modèles de stratégie de droits publiés, de sorte qu'ils soient disponibles hors connexion. Pour activer cette fonctionnalité, les ordinateurs doivent exécuter les systèmes d'exploitation Windows suivants :

- Windows Vista avec Service Pack 1 (SP1) ou version plus récente
- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Pour activer cette fonctionnalité, dans le Planificateur de tâches, activez la **Tâche planifiée (automatisée) Gestion des modèles de stratégie de droits d'AD RMS**, puis modifiez la clé de registre suivante :

```
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DRM
```

Fournissez l'emplacement suivant pour que les modèles soient enregistrés :

%LocalAppData%\Microsoft\DRM\Modèles

Quand des ordinateurs qui exécutent ces systèmes d'exploitation sont connectés au domaine, le client AD RMS interroge le cluster AD RMS pour avoir de nouveaux modèles ou des mises à jour pour les modèles existants.

Comme alternative à la distribution de modèles, vous pouvez également utiliser des dossiers partagés comme solution de stockage des modèles. Vous pouvez configurer un dossier partagé pour les modèles en procédant comme suit :

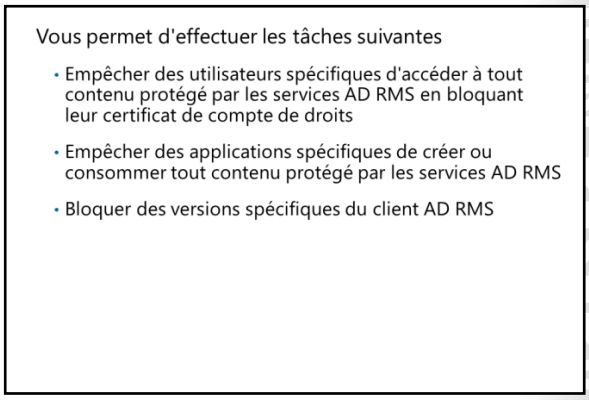
1. Dans la console Active Directory Rights Management Services, cliquez avec le bouton droit sur le nœud **Modèles de stratégie de droits**, puis cliquez sur **Propriétés**.
2. Sur la boîte de dialogue **Propriétés des modèles de stratégie de droits**, spécifiez l'emplacement du dossier partagé vers lequel des modèles seront publiés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les stratégies d'exclusion ?

Les stratégies d'exclusion vous permettent d'empêcher des comptes d'utilisateur, des logiciels clients ou des applications spécifiques d'utiliser AD RMS.



Exclusion d'utilisateurs

La stratégie d'exclusion d'utilisateurs vous permet de configurer AD RMS de sorte que des comptes d'utilisateurs spécifiques, qui sont identifiés selon des adresses de messagerie, ne puissent pas obtenir de licences d'utilisation. Vous y procédez en ajoutant le certificat de compte de droits de chaque utilisateur à la liste d'exclusion. L'exclusion d'utilisateurs est désactivée par défaut. Une fois que vous avez activé l'exclusion d'utilisateurs, vous pouvez exclure des certificats de comptes de droits spécifiques.

Vous pouvez utiliser l'exclusion d'utilisateurs au cas où vous devriez rejeter un utilisateur spécifique du contenu protégé par AD RMS. Par exemple, quand les utilisateurs quittent l'organisation, vous pouvez exclure leurs certificats de comptes de droits pour vous assurer qu'ils ne peuvent pas accéder au contenu protégé. Vous pouvez bloquer des certificats de comptes de droits qui sont attribués à des utilisateurs internes et externes.

Exclusion d'applications

L'exclusion d'application vous permet d'empêcher des applications spécifiques, comme Office PowerPoint®, de créer ou de consommer du contenu protégé par AD RMS. Vous spécifiez des applications selon des noms exécutables. Vous spécifiez également une version minimum et maximum de l'application. L'exclusion d'applications est désactivée par défaut.

Remarque : Il est possible de contourner l'exclusion d'applications en renommant un fichier exécutable.

Exclusion de référentiels sécurisés

L'exclusion de référentiels sécurisés vous permet d'exclure des clients AD RMS, comme ceux utilisés avec les systèmes d'exploitation spécifiques tels que Windows XP et Windows Vista. L'exclusion de référentiels sécurisés est désactivée par défaut. Une fois que vous avez activé l'exclusion de versions de référentiels sécurisés, vous devez spécifier la version minimum du référentiel sécurisé qui peut être utilisée avec le cluster AD RMS.

Documentation supplémentaire : Pour en savoir plus au sujet de l'activation des stratégies d'exclusion, consultez la rubrique Activation des stratégies d'exclusion à l'adresse http://go.microsoft.com/fwlink/?LinkId=270031

Démonstration : Création d'une stratégie d'exclusion pour exclure une application

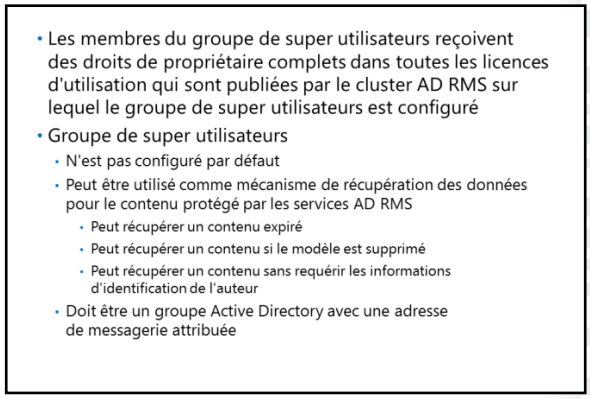
Dans cette démonstration, vous verrez comment exclure l'application Office PowerPoint d'AD RMS.

Procédure de démonstration

1. Dans la console AD RMS, activez l'exclusion d'applications.
2. Dans la boîte de dialogue **Exclure l'application**, saisissez les informations suivantes :
   - Nom de fichier d'application : **Powerpnt.exe**
   - Version minimale : **14.0.0.0**
   - Version maximale : **16.0.0.0**

Groupe de super utilisateurs d'AD RMS

Le groupe de super utilisateurs AD RMS est un rôle spécial et les membres de ce groupe ont le contrôle total sur tout le contenu protégé par des droits et géré par le cluster. Les membres du groupe de super utilisateurs reçoivent des droits de propriétaire complets dans toutes les licences d'utilisation qui sont publiées par le cluster AD RMS sur lequel le groupe de super utilisateurs est configuré. Cela signifie que les membres de ce groupe peuvent déchiffrer n'importe quel fichier de contenu protégé par des droits et en enlever cette protection.



Le groupe de super utilisateurs d'AD RMS fournit un mécanisme de récupération des données pour le contenu protégé par les services AD RMS. Ce mécanisme est utile au cas où vous devriez récupérer des données protégées par AD RMS, comme quand le contenu a expiré, quand un modèle a été supprimé ou quand vous n'avez pas d'accès.

Les membres du groupe de super utilisateurs reçoivent des licences d'utilisation de propriétaire pour tout le contenu qui est protégé par le cluster AD RMS sur lequel ce groupe particulier de super utilisateurs est activé. Les membres du groupe de super utilisateurs peuvent réinitialiser le mot de passe de la clé privée du serveur AD RMS.

Puisque les membres du groupe de super utilisateurs peuvent accéder à tout le contenu protégé par AD RMS, vous devez faire particulièrement attention quand vous gérez l'appartenance à ce groupe. Si vous choisissez d'utiliser le groupe de super utilisateurs d'AD RMS, vous devez envisager d'implémenter une stratégie de groupes restreints et de l'auditer pour limiter l'appartenance au groupe, et devez vérifier toutes les modifications qui sont apportées. L'activité des super utilisateurs est écrite dans le journal d'événements des applications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le groupe de super utilisateurs est désactivé par défaut. Vous activez le groupe de super utilisateurs en procédant comme suit :

1. Dans la console AD RMS, développez le nœud du serveur, puis cliquez sur **Stratégies de sécurité**.
2. Dans la zone Stratégies de sécurité, sous Super utilisateurs, cliquez sur **Modifier les paramètres de super utilisateur**.
3. Dans le volet Actions, cliquez sur **Activer les super utilisateurs**.

Pour définir un groupe particulier en tant que groupe de super utilisateurs :

1. Dans la zone Stratégies de sécurité\Super utilisateurs, cliquez sur **Modifier le groupe des super utilisateurs**.
2. Fournissez l'adresse de messagerie associée au groupe de super utilisateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Configuration d'un accès externe à AD RMS

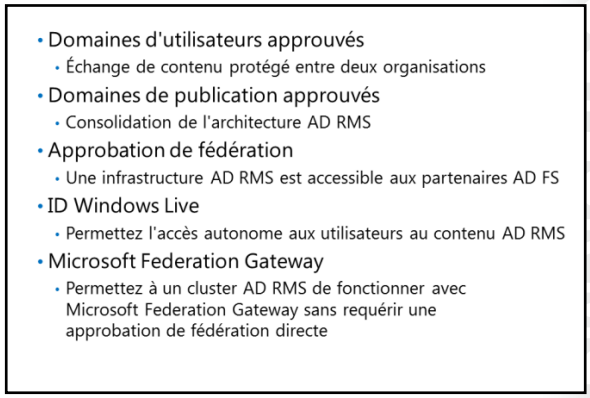
Vous pouvez souvent trouver nécessaire de fournir aux utilisateurs qui ne font pas partie de l'organisation l'accès au contenu protégé par AD RMS. Cela pourrait être une situation dans laquelle un utilisateur externe est un entrepreneur qui a besoin de l'accès aux matériaux sensibles ou une organisation partenaire dans laquelle vos utilisateurs auront besoin de l'accès au contenu protégé publié par leur serveur AD RMS. AD RMS fournit un certain nombre d'options différentes pour accorder aux utilisateurs externes l'accès au contenu protégé.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options disponibles pour rendre le contenu protégé par AD RMS accessible aux utilisateurs externes ;
- expliquer comment implémenter des domaines d'utilisateurs approuvés ;
- lister les étapes nécessaires pour déployer les domaines de publication approuvés ;
- décrire les étapes nécessaires pour configurer AD RMS de sorte à partager le contenu protégé avec des utilisateurs qui ont des identifiants Windows Live ;
- déterminer la solution appropriée pour partager le contenu protégé par AD RMS avec des utilisateurs externes.

Options d'activation des utilisateurs externes ayant accès à AD RMS



Les stratégies d'approbation permettent aux utilisateurs qui sont externes à votre organisation de consommer le contenu protégé par les services AD RMS. Par exemple, une stratégie d'approbation peut permettre à des utilisateurs dans des environnements Apportez vos propres terminaux (Bring Your Own Device, BYOD) de consommer contenu protégé par les services AD RMS, même si ces ordinateurs ne sont pas des membres du domaine AD DS de l'organisation. Les approbations AD RMS sont désactivées par défaut et vous devez les activer avant de pouvoir les utiliser. AD RMS prend en charge les stratégies d'approbation suivantes.

Domaines d'utilisateurs approuvés

Les Domaines d'utilisateurs approuvés (TUD) permettent à un cluster AD RMS de traiter des demandes pour les certificats de licence client ou de licences d'utilisation de la part de personnes qui ont leurs certificats de comptes de droits émis par un cluster AD RMS différent. Par exemple, A. Datum Corporation et Trey Research sont des organisations distinctes qui ont déployé chacune AD RMS. Les TUD permettent à chaque organisation de publier et de consommer du contenu protégé par les services AD RMS vers et à partir de l'organisation partenaire sans devoir implémenter des approbations AD DS ou AD FS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Domaines de publication approuvés

Les Domaines de publication approuvés (TPD) permettent à un cluster AD RM d'émettre des licences d'utilisateur final vers du contenu qui utilise des licences de publication qui sont publiées par un cluster AD RMS différent. Les TPD consolident l'infrastructure AD RMS existante.

Approbation de fédération

L'approbation fédérée fournit l'authentification unique (SSO) pour des technologies de partenaire. Les partenaires fédérés peuvent consommer le contenu protégé par les services AD RMS sans déployer leur propre infrastructure AD RMS. L'approbation fédérée requiert le déploiement d'AD FS.

Approbation Windows Live ID

Vous pouvez utiliser Windows Live ID pour permettre aux utilisateurs autonomes disposant de comptes Windows Live ID de consommer du contenu protégé par les services AD RMS généré par des utilisateurs dans votre organisation. Cependant, les utilisateurs Windows Live ID ne peuvent pas créer de contenu qui est protégé par le cluster AD RMS.

Microsoft Federation Gateway

Microsoft Federation Gateway permet à un cluster AD RMS de traiter des demandes de publication et de consommation de contenu protégé par les services AD RMS provenant d'organisations externes, en acceptant les jetons d'authentification basés sur des revendications de Microsoft Federation Gateway. Plutôt que de configurer une approbation de fédération, chaque organisation a une relation avec Microsoft Federation Gateway. Microsoft Federation Gateway agit comme un courtier d'approbation.

Documentation supplémentaire : Pour en savoir plus au sujet des stratégies d'approbation AD RMS, consultez la page http://go.microsoft.com/fwlink/?LinkId=270032.

Implémentation de la réplication TUD

TUD permet à AD RMS de traiter les demandes des utilisateurs qui ont leurs certificats de comptes de droits émis par différents déploiements des services AD RMS. Vous pouvez utiliser des exclusions avec chaque TUD pour bloquer l'accès d'utilisateurs et de groupes spécifiques.

- Permet à AD RMS de traiter les demandes pour les utilisateurs ayant des certificats de compte de droits de différents clusters AD RMS
- Domaines d'utilisateur approuvé (TUD)
  - Prennent en charge les exclusions pour les utilisateurs individuels et les groupes
  - Peuvent être à sens unique ou bidirectionnels
- Doit exporter le TUD du partenaire avant d'importer le TUD localement

Afin de configurer AD RMS pour prendre en charge le traitement des demandes des utilisateurs qui ont leurs certificats de comptes de droits émis par différents déploiements des services AD RMS, vous ajoutez l'organisation à la liste des TUD. Les TUD peuvent être unidirectionnels, où l'organisation A représente un TUD de l'organisation B, ou bidirectionnel, où l'organisation A et l'organisation B sont les TUD de l'un et l'autre. Dans des déploiements unidirectionnels, il est possible que les utilisateurs du TUD consomment le contenu du déploiement AD RMS local, mais ils ne peuvent pas publier du contenu protégé par les services AD RMS à l'aide du cluster AD RMS local.

Vous devez activer la connexion anonyme au service de gestion de licences AD RMS dans Internet Information Services (IIS) lors de l'utilisation du TUD. En fait, accéder au service requiert par défaut l'authentification en utilisant l'authentification Windows intégrée.

Pour ajouter un TUD, exécutez la procédure ci-dessous :

1. Le TUD du déploiement des services AD RMS que vous souhaitez approuver doit avoir été déjà exporté, et le fichier doit être disponible. (Les fichiers TUD utilisent l'extension .bin.)
2. Dans la console AD RMS, développez **Stratégies d'approbation**, puis cliquez sur **Domaines d'utilisateurs approuvés**.
3. Dans le volet Actions, cliquez sur **Importer le domaine d'utilisateur approuvé**.
4. Dans la boîte de dialogue **Domaine d'utilisateur approuvé**, saisissez le chemin d'accès au fichier TUD exporté avec l'extension .bin.
5. Fournissez un nom pour identifier ce TUD. Si vous avez configuré la fédération, vous pouvez également choisir d'étendre l'approbation aux utilisateurs fédérés du serveur importé.

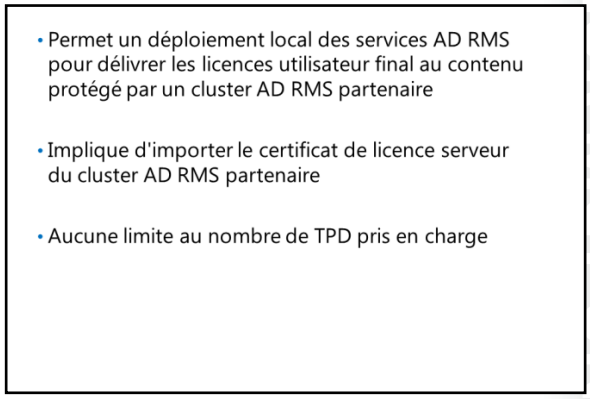
Vous pouvez également utiliser l'applet de commande Windows PowerShell **Import-RmsTUD**, qui fait partie du module ADRMSADMIN Windows PowerShell, pour ajouter un TUD.

Pour exporter un TUD, exécutez la procédure ci-dessous :

1. Dans la console AD RMS, développez **Stratégies d'approbation**, puis cliquez sur **Domaines d'utilisateurs approuvés**.
2. Dans le volet Actions, cliquez sur **Exporter le domaine d'utilisateur approuvé**.
3. Enregistrez le fichier TUD avec un nom descriptif.

Vous pouvez également utiliser l'applet de commande Windows PowerShell **Export-RmsTUD** pour exporter un TUD du serveur AD RMS.

Implémentation de la réplication TPD



Vous pouvez utiliser un TPD pour installer une relation d'approbation entre deux déploiements des services AD RMS. Un TPD AD RMS, qui est un déploiement AD RMS local, peut accorder des licences d'utilisateur final pour le contenu publié en utilisant le déploiement AD RMS du domaine de publication approuvé. Par exemple, Contoso, Ltd et A. Datum Corporation sont configurés comme étant des partenaires de TPD. Un TPD permet à des utilisateurs du déploiement AD RMS de Contoso de consommer le contenu publié en utilisant le déploiement AD RMS d'A. Datum, à l'aide des licences d'utilisateur final qui sont accordées par le déploiement des services AD RMS de Contoso.

Vous pouvez supprimer un TPD à tout moment. Quand vous faites cela, les clients du déploiement des services AD RMS distant ne pourront pas émettre de licences d'utilisateur final pour accéder au contenu protégé par votre cluster AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Quand vous configurez un TPD, vous importez le SLC d'un autre cluster AD RMS. Les TPD sont enregistrés au format .xml et sont protégés par des mots de passe.

Pour exporter un TPD, exécutez la procédure ci-dessous :

1. Dans la console AD RMS, développez **Stratégies d'approbation**, puis cliquez sur **Domaines de publication approuvés**.
2. Dans le volet Résultats, cliquez sur le certificat du domaine AD RMS que vous souhaitez exporter, puis dans le volet Actions, cliquez sur **Exporter le domaine de publication approuvé**.
3. Choisissez un mot de passe fort et un nom de fichier pour le TPD.

Quand vous exportez un TPD, il est possible de le sauvegarder en tant que fichier TPD compatible avec V1. Cela permet d'importer le TPD dans les organisations qui utilisent des clusters AD RMS sur des versions antérieures du système d'exploitation Windows Server, telles que la version disponible dans Windows Server 2003. Vous pouvez également utiliser l'applet de commande Windows PowerShell **Export-RmsTPD** pour exporter un TPD.

Pour importer un TPD, exécutez la procédure ci-dessous :

1. Dans la console AD RMS, développez **Stratégies d'approbation**, puis cliquez sur **Domaines de publication approuvés**.
2. Dans le volet Actions, cliquez sur **Importer le domaine de publication approuvé**.
3. Spécifiez le chemin d'accès du fichier du domaine de publication approuvé que vous souhaitez importer.
4. Entrez le mot de passe pour ouvrir le fichier du domaine de publication approuvé et saisissez un nom complet qui identifie le TPD.

Vous pouvez également utiliser l'applet de commande Windows PowerShell **Import-RmsTPD** pour importer un TPD.

Documentation supplémentaire : Pour en savoir plus au sujet de l'importation des TPD, consultez la rubrique Ajouter un domaine de publication approuvé à l'adresse http://go.microsoft.com/fwlink/?LinkId=270033.

Partage de documents protégés par AD RMS à l'aide de Windows Live ID

Vous pouvez utiliser Windows Live ID comme moyen de fournir des certificats de comptes de droits aux utilisateurs qui ne font pas partie de votre organisation.

Pour approuver les certificats de comptes de droits basés sur Windows Live ID, procédez comme suit :

1. Dans la console AD RMS, développez **Stratégies d'approbation**, puis cliquez sur **Domaines d'utilisateurs approuvés**.
2. Dans le volet Actions, cliquez sur **Approuver Windows Live ID**.

- Fournissez des certificats de compte de droits aux utilisateurs qui ne font pas partie d'une organisation
- Les utilisateurs avec des comptes Windows Live ID peuvent consommer du contenu protégé par les services AD RMS
- Les utilisateurs avec des comptes Windows Live ID ne peuvent pas publier du contenu protégé par les services AD RMS

Pour exclure des domaines de messagerie Windows Live ID spécifiques, cliquez avec le bouton droit sur le certificat Windows Live ID, cliquez sur **Propriétés**, puis cliquez sur l'onglet **ID Windows Live exclus**. Vous pouvez alors saisir les comptes Windows Live ID que vous souhaitez exclure pour qu'ils n'obtiennent pas de certificat de compte de droits.

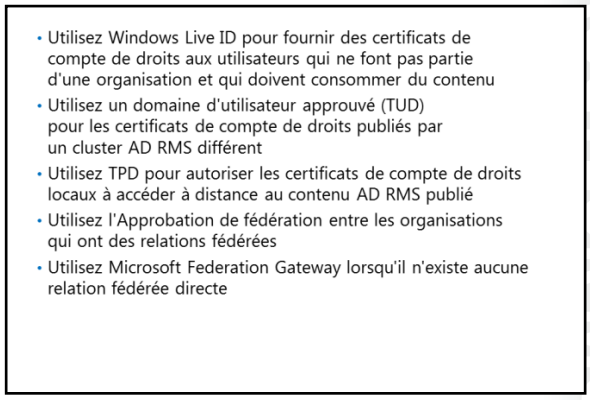
Pour permettre à des utilisateurs avec des comptes Windows Live ID d'obtenir des certificats de comptes de droits à partir de votre cluster AD RMS, vous devez configurer IIS pour prendre en charge l'accès anonyme. Pour cela, procédez comme suit :

1. Sur le serveur AD RMS, ouvrez la console Gestionnaire des services Internet.
2. Naviguez jusqu'au nœud **Sites\Site Web par défaut_wmcs**, cliquez avec le bouton droit sur le répertoire virtuel **Licence**, puis cliquez sur **Basculer vers l'affichage du contenu**.
3. Cliquez avec le bouton droit sur **license.asmx**, puis cliquez sur **Basculer vers l'affichage du contenu**.
4. Double-cliquez sur **Authentification**, puis activez **Authentification anonyme**.
5. Répétez cette étape pour le fichier **ServiceLocator.asmx**.

Documentation supplémentaire : Pour en savoir plus au sujet de l'utilisation de Windows Live ID établir des certificats de compte des droits pour les utilisateurs, consultez la page http://go.microsoft.com/fwlink/?LinkId=270034.

Éléments à prendre en compte pour implémenter l'accès d'un utilisateur externe à AD RMS

Le type d'accès externe que vous configurez dépend des types d'utilisateurs externes qui ont besoin d'un accès au contenu de votre organisation.



Quand vous déterminez quelle méthode utiliser, considérez les questions suivantes :

- L'utilisateur externe appartient-il à une organisation qui a un déploiement AD RMS existant ?
- L'organisation de l'utilisateur externe a-t-elle une approbation fédérée existante avec l'organisation interne ?
- L'organisation de l'utilisateur externe a-t-elle établi des relations avec Microsoft Federation Gateway ?
- L'utilisateur externe doit-il publier du contenu protégé par les services AD RMS qui est accessible par les titulaires de certificat de compte de droits internes ?

Il est possible que les organisations puissent utiliser une solution avant d'en adopter une autre. Par exemple, pendant les étapes initiales, seul un nombre restreint d'utilisateurs externes peut avoir besoin de l'accès au contenu protégé par AD RMS. Dans ce cas, l'utilisation de comptes Windows Live ID pour les certificats de compte de droits peut être appropriée. Quand de plus grands nombres d'utilisateurs externes d'une organisation unique ont besoin de l'accès, une solution différente peut être appropriée. L'avantage financier qu'une solution apporte à une organisation doit dépasser le coût d'implémentation de cette solution.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation AD RMS

Scénario

En raison de la nature hautement confidentielle de la recherche qui est exécutée au sein d'A. Datum Corporation, l'équipe chargée de la sécurité chez A. Datum souhaite implémenter une sécurité supplémentaire pour certains des documents que le département Recherche crée. L'équipe chargée de la sécurité s'inquiète que toute personne avec un accès **Lecture** aux documents puisse modifier et distribuer les documents de quelque façon souhaitée. L'équipe chargée de la sécurité voudrait fournir un niveau de protection supplémentaire qui reste avec le document même s'il est déplacé sur le réseau ou à l'extérieur du réseau.

En tant qu'un des administrateurs réseau principaux chez A. Datum, vous devez organiser et implémenter une solution AD RMS qui fournira le niveau de protection demandé par l'équipe chargée de la sécurité. La solution AD RMS doit fournir de nombreuses options différentes qui peuvent être adaptées pour une grande variété d'entreprise et d'exigences de sécurité.

Objectifs

- installer et configurer les services AD RMS (Active Directory Rights Management Services) ;
- configurer des modèles AD RMS ;
- implémenter des stratégies d'approbation AD RMS ;
- vérifier le déploiement AD RMS.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-CL1** **22412B-MUN-DC1** **22412B-MUN-CL1**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez l'étape 2 et 3 pour **22412B-LON-SVR1**, **22412B-MUN-DC1**, **22412B-LON-CL1** et **22412B-MUN-CL1**. Ne vous connectez pas tant qu'il ne vous a pas été demandé de le faire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Installation et configuration AD RMS

Scénario

La première étape du déploiement AD RMS chez A. Datum est de déployer un serveur unique dans un cluster AD RMS. Vous commencerez en configurant les enregistrements DNS appropriés et le compte de service AD RMS, puis continuerez avec l'installation et la configuration du premier serveur AD RMS. Vous activerez également le groupe de super utilisateurs des services AD RMS.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le DNS (Domain Name System) et le compte de service Active Directory® Rights Management Services (AD RMS)
2. Installer et configurer le rôle de serveur AD RMS
3. Configurer le groupe de super utilisateurs des services AD RMS

▶ Tâche 1 : Configurer le DNS (Domain Name System) et le compte de service Active Directory® Rights Management Services (AD RMS)

1. Connectez-vous à **LON-DC1** à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Utilisez le Centre d'administration Active Directory pour créer une unité d'organisation (OU) nommée **Comptes de service** dans le domaine adatum.com.
3. Créez un nouveau compte d'utilisateur dans l'unité d'organisation Comptes de service en indiquant les propriétés suivantes :
   - Prénom : **ADRMSSVC**
   - Nom d'ouverture de session de l'utilisateur principal : **ADRMSSVC**
   - Mot de passe : **Pa$$w0rd**
   - Confirmer le mot de passe : **Pa$$w0rd**
   - Le mot de passe n'expire jamais : **Activé**
   - L'utilisateur ne peut pas changer de mot de passe : **Activé**
4. Dans le conteneur Utilisateurs, créez un groupe de sécurité global nommé **ADRMS_SuperUtilisateurs**. Définissez l'adresse de messagerie de ce groupe comme **ADRMS_SuperUsers@adatum.com**.
5. Dans le conteneur Utilisateurs, créez un nouveau groupe de sécurité global nommé **Cadres**. Définissez l'adresse de messagerie de ce groupe comme **executives@adatum.com**.
6. Ajoutez les comptes d'utilisateurs **Aidan Delaney** et **Bill Malone** au groupe Cadres.
7. Utilisez la console du Gestionnaire DNS pour créer un enregistrement de ressource hôte (**A**) dans la zone adatum.com avec les propriétés suivantes :
   - Nom : **adrms**
   - Adresse IP : **172.16.0.21**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Installer et configurer le rôle de serveur AD RMS

1. Connectez-vous à **LON-SVR1** à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Utilisez l'Assistant Ajout de rôles et de fonctionnalités pour ajouter le rôle AD RMS à LON-SVR1 en utilisant l'option suivante :
   - Services de rôle : **Services AD RMS (Active Directory Rights Management Services)**
3. À partir du nœud AD RMS du Gestionnaire de serveur, cliquez sur **Autres** pour commencer la configuration de post-déploiement d'AD RMS.
4. Dans l'Assistant de Configuration d'AD RMS, fournissez les informations ci-dessous :
   - **Créer un nouveau cluster racine AD RMS**
   - **Utiliser la base de données interne de Windows sur ce serveur**
   - Compte de service : **Adatum\ADRMSSVC**
   - Mode de chiffrement : **Mode de chiffrement 2**
   - Stockage de clé de cluster : **Utiliser le stockage de clé AD RMS géré de manière centralisée**
   - Mot de passe de clé de cluster : **Pa$$w0rd**
   - Site Web de cluster : **Site Web par défaut**
   - Type de connexion : **Utiliser une connexion non chiffrée**
   - Nom de domaine complet : **http://adrms.adatum.com**
   - Port : **80**
   - Certificat de licence : **Adatum AD RMS**
   - Enregistrer un point de connexion de service AD RMS : **Enregistrer le point de connexion de service maintenant**
5. Utilisez la console du Gestionnaire des services Internet (IIS) pour activer l'authentification anonyme sur les répertoires virtuels **Default Web Site_wmcs** et **Default Web Site_wmcs\licensing**.
6. Déconnectez-vous de LON-SVR1.

Remarque : Vous devez vous déconnecter avant de pouvoir gérer AD RMS. Cet atelier utilise le port 80 pour des raisons pratiques. Dans des environnements de production, vous protégeriez AD RMS en utilisant une connexion chiffrée.

▶ Tâche 3 : Configurer le groupe de super utilisateurs des services AD RMS

1. Connectez-vous à **LON-SVR1** à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Ouvrez la console **AD RMS**.
3. À partir de la console **AD RMS**, activez les super utilisateurs.
4. Définissez le groupe **ADRMS_SuperUtilisateurs** en tant que groupe de super utilisateurs.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré les services AD RMS.

Exercice 2 : Configuration des modèles AD RMS

Scénario

Après le déploiement du serveur AD RMS, vous devez maintenant configurer les modèles de stratégie de droits et les stratégies d'exclusion pour l'organisation. Vous déploierez alors les deux composants.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un nouveau modèle de stratégie de droits
2. Configurer la distribution des modèles de stratégie de droits
3. Configurer une stratégie d'exclusion

▶ Tâche 1 : Configurer un nouveau modèle de stratégie de droits

- Sur LON-SVR1, utilisez le nœud Modèle de stratégie de droits de la console AD RMS pour créer un modèle de stratégie de droits distribué avec les propriétés suivantes :
  - Langue : **français (France)**
  - Nom : **ReadOnly**
  - Description : **Accès en lecture seule. Aucune copie ou impression**
  - Utilisateurs et droits : **executives@adatum.com**
  - Droits pour n'importe qui : **Vue**
  - **Octroyer le contrôle total au propriétaire (auteur) sans date d'expiration**
  - Expiration du contenu : **7** jours
  - Expiration de la licence d'utilisation : **7** jours
  - Demander une nouvelle licence d'utilisation : **à chaque accès au contenu (désactiver la mise en cache côté client)**

▶ Tâche 2 : Configurer la distribution des modèles de stratégie de droits

1. Sur LON-SVR1, ouvrez une invite **Windows PowerShell** et émettez les commandes suivantes, appuyant sur Entrée après chaque ligne :

```
New-Item c:\rmstemplates -ItemType Directory
New-SmbShare -Name RMSTEMPLATES -Path c:\rmstemplates -FullAccess ADATUM\ADRMSSVC
New-Item c:\docshare -ItemType Directory
New-SmbShare -Name docshare -Path c:\docshare -FullAccess “tout le monde”
```

2. Dans la console Active Directory Rights Management Services, définissez l'emplacement du fichier des modèles de stratégie de droits sur **\\LON-SVR1\RMSTEMPLATES**.
3. Dans l'Explorateur de fichiers, affichez le dossier de c:\rmstemplates. Vérifiez que le modèle **ReadOnly.xml** est présent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer une stratégie d'exclusion

1. Dans la console AD RMS, activez l'exclusion d'applications.
2. Dans la boîte de dialogue **Exclure l'application**, saisissez les informations suivantes :
   - Nom de fichier d'application : **Powerpnt.exe**
   - Version minimale : **14.0.0.0**
   - Version maximale : **16.0.0.0**

Résultats : Après avoir terminé cet exercice, vous aurez configuré les modèles AD RMS.

Exercice 3 : Implémentation des stratégies d'approbation AD RMS

Scénario

Dans le cadre du déploiement des services AD RMS, vous devez vérifier que la fonctionnalité AD RMS est étendue au déploiement des services AD RMS de Trey Research. Vous configurerez les stratégies d'approbation requises, puis validerez que vous pouvez partager le contenu protégé entre les deux organisations.

Les tâches principales de cet exercice sont les suivantes :

1. Exporter la stratégie des domaines d'utilisateurs approuvés
2. Exporter la stratégie des domaines de publication approuvés
3. Importer la stratégie de domaine d'utilisateur approuvé à partir du domaine partenaire
4. Importer la stratégie des domaines de publication approuvés à partir du domaine partenaire

▶ Tâche 1 : Exporter la stratégie des domaines d'utilisateurs approuvés

1. Sur LON-SVR1, ouvrez une invite Windows PowerShell et émettez les commandes suivantes, appuyant sur Entrée après chaque ligne :

```
New-Item c:\export -ItemType Directory
New-SmbShare -Name Export -Path c:\export -FullAccess “tout le monde”
```

2. Utilisez la console AD RMS pour exporter la stratégie des TUD vers le serveur de partage **\\LON-SVR1\export** au format **ADATUM-TUD.bin**.
3. Connectez-vous à MUN-DC1 à l'aide du compte **TREYRESEARCH\Administrateur** et du mot de passe **Pa$$w0rd**.
4. Sur MUN-DC1, ouvrez la console AD RMS.
5. Exportez la stratégie de **Domaines d'utilisateurs approuvés** vers le serveur de partage **\\LON-SVR1\export** au format **TREYRESEARCH-TUD.bin**.
6. Sur MUN-DC1, ouvrez une invite **Windows PowerShell**, puis exécutez la commande suivante, puis appuyez sur Entrée :

```
Add-DnsServerConditionalForwarderZone -MasterServers 172.16.0.10 -Name adatum.com
```

▶ Tâche 2 : Exporter la stratégie des domaines de publication approuvés

1. Basculez vers **LON-SVR1**.
2. Utilisez la console AD RMS pour exporter la stratégie des TPD vers le serveur de partage **\\LON-SVR1\export** au format **ADATUM-TPD.xml**. Protégez ce fichier en utilisant le mot de passe **Pa$$w0rd**.
3. Basculez vers **MUN-DC1**.
4. Utilisez la console AD RMS pour exporter la stratégie des TPD vers le serveur de partage **\\LON-SVR1\export** au format **TREYRESEARCH-TPD.xml**. Protégez ce fichier en utilisant le mot de passe **Pa$$w0rd**.

▶ Tâche 3 : Importer la stratégie de domaine d'utilisateur approuvé à partir du domaine partenaire

1. Basculez vers **LON-SVR1**.
2. Importez la stratégie de TUD pour Trey Research en important le fichier **\\LON-SVR1\export\treyresearch-tud.bin**. Utilisez le nom complet **TreyResearch**.
3. Basculez vers **MUN-DC1**.
4. Importez la stratégie de TUD pour Trey Research en important le fichier **\\LON-SVR1\export\adatum-tud.bin**. Utilisez le nom complet **Adatum**.

▶ Tâche 4 : Importer la stratégie des domaines de publication approuvés à partir du domaine partenaire

1. Basculez vers **LON-SVR1**.
2. Importez le TPD Trey Research en important le fichier **\\LON-SVR1\export\treyresearch-tpd.xml**, en utilisant le mot de passe **Pa$$w0rd** et le nom complet **Trey Research**.
3. Basculez vers **MUN-SVR1**.
4. Importez le TPD Adatum en important le fichier **\\LON-SVR1\export\adatum-tpd.xml**, en utilisant le mot de passe **Pa$$w0rd** et le nom complet **Adatum**.

Résultats : À la fin de cet exercice, vous aurez implémenté des stratégies d'approbation AD RMS.

Exercice 4 : Vérification du déploiement AD RMS

Scénario

Comme étape finale du déploiement, vous validerez que la configuration fonctionne correctement.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un document protégé par des droits
2. Vérifier l'accès interne au contenu protégé
3. Ouvrir le document protégé par des droits en tant qu'utilisateur non autorisé
4. Ouvrir et modifier le document protégé par des droits en tant qu'utilisateur autorisé au sein de Trey Research

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Créer un document protégé par des droits

1. Connectez-vous à **LON-CL1** à l'aide du compte **Adatum\Aidan** et du mot de passe **Pa$$w0rd**.
2. Ouvrez **Microsoft Word 2010**.
3. Créez un document nommé **Cadres seulement**.
4. Dans le document, saisissez le texte suivant :

   Ce document est pour les cadres seulement, il ne doit pas être modifié.
5. À partir de l'élément Autorisations, choisissez de restreindre l'accès. Accordez à **bill@adatum.com** l'autorisation de lire le document.
6. Enregistrez le document dans le serveur de partage **\\lon-svr1\docshare**.
7. Déconnectez-vous de LON-CL1.

▶ Tâche 2 : Vérifier l'accès interne au contenu protégé

1. Connectez-vous à **LON-CL1** avec le compte **Adatum\Bill** et le mot de passe **Pa$$w0rd**.
2. Dans le dossier **\\lon-svr1\docshare**, ouvrez le document **Executives Only**.
3. Lorsque vous y êtes invité, fournissez les informations d'identification **Adatum\Bill** avec le mot de passe **Pa$$w0rd**.
4. Vérifiez que vous ne pouvez pas modifier ni enregistrer le document.
5. Sélectionnez une ligne de texte dans le document.
6. Cliquez avec le bouton droit sur la ligne de texte. Vérifiez que vous ne pouvez pas modifier ce texte.
7. Affichez les autorisations du document.
8. Déconnectez-vous de LON-CL1.

▶ Tâche 3 : Ouvrir le document protégé par des droits en tant qu'utilisateur non autorisé

1. Ouvrez une session sur **LON-CL1** en tant qu'**Adatum\Carol** en utilisant le mot de passe **Pa$$w0rd**.
2. Dans le dossier **\\lon-svr1\docshare**, essayez d'ouvrir le document **Cadres seulement**.
3. Vérifiez que Carol n'a pas l'autorisation d'ouvrir le document.
4. Déconnectez-vous de LON-CL1.

▶ Tâche 4 : Ouvrir et modifier le document protégé par des droits en tant qu'utilisateur autorisé au sein de Trey Research

1. Connectez-vous à **LON-CL1** avec le compte **Adatum\Aidan** et le mot de passe **Pa$$w0rd**.
2. Ouvrez **Microsoft Word 2010**.
3. Créez un nouveau document nommé **\\LON-SVR1\docshare\TreyResearch-Confidential.docx**.
4. Dans le document, saisissez le texte suivant :

   Ce document est pour Trey Research seulement, il ne doit pas être modifié.
5. Restreignez l'autorisation de sorte qu'**april@treyresearch.net** puisse ouvrir le document.

6. Connectez-vous à **MUN-CL1** en tant que **TREYRESEARCH\April** avec le mot de passe **Pa$$w0rd**.
7. Utilisez l'Explorateur de fichiers pour naviguer jusqu'à **\\LON-SVR1\docshare**. Utilisez les informations d'identification **Adatum\Administrateur** et **Pa$$w0rd** pour vous connecter.
8. Copiez le document **TreyReserch-Confidential.docx** sur le bureau.
9. Tenter d'ouvrir le document. Quand vous y êtes invité, saisissez les informations d'identification suivantes, activez la case à cocher **Mémoriser ces informations**, puis cliquez sur **OK** :
   - Nom d'utilisateur : **April**
   - Mot de passe : **Pa$$w0rd**
10. Vérifiez que vous pouvez ouvrir le document, mais que vous ne pouvez pas apporter de modifications à ce document.
11. Affichez les autorisations que le compte **april@treyresearch.com** a pour le document.

Résultats : Après avoir terminé cet exercice, vous aurez vérifié que le déploiement des services AD RMS est réussi.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-MUN-DC1**, **22412B-LON-CL1** et **22412B-MUN-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quels sont les avantages d'avoir un certificat SSL installé sur le serveur AD RMS quand vous effectuez la configuration AD RMS ?

Question : Vous devez permettre d'accéder au contenu protégé par les services AD RMS à cinq utilisateurs qui sont des entrepreneurs indépendants et qui ne sont pas des membres de votre organisation. Quelle méthode devez-vous utiliser pour fournir cet accès ?

Question : Vous souhaitez empêcher des utilisateurs de protéger le contenu Office PowerPoint en utilisant des modèles AD RMS. Quelles mesures devez-vous prendre pour accomplir cet objectif ?



Méthode conseillée :

- Avant de déployer AD RMS, vous devez analyser les exigences stratégiques de votre organisation et créer les modèles nécessaires. Vous devez rencontrer les utilisateurs pour les informer de la fonctionnalité AD RMS et pour demander également des commentaires sur les types de modèles dont ils aimeraient disposer.
- Contrôlez strictement l'appartenance au groupe de super utilisateurs. Les utilisateurs présents dans ce groupe peuvent accéder à tout le contenu protégé. Accorder l'appartenance à ce groupe à un utilisateur lui donne un accès complet à tout le contenu protégé par AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8

Implémentation des services AD FS (Active Directory Federation Services)

Table des matières :

Vue d'ensemble du module **8-1**

Leçon 1 : Vue d'ensemble d'AD FS **8-2**

Leçon 2 : Déploiement d'AD FS **8-14**

Leçon 3 : Implémentation d'AD FS pour une seule organisation **8-22**

Leçon 4 : Déploiement d'AD FS dans un scénario de fédération B2B **8-29**

Atelier pratique : Implémentation des services AD FS (Active Directory Federation Services) **8-36**

Contrôle des acquis et éléments à retenir **8-46**

Vue d'ensemble du module

Les services AD FS (Active Directory® Federation Services) de Windows Server® 2012 fournissent la flexibilité nécessaire aux organisations qui souhaitent permettre à leurs utilisateurs de se connecter aux applications qui peuvent être situées sur le réseau local, dans une société partenaire ou dans un service en ligne. Avec les services AD FS, une organisation peut gérer ses propres comptes d'utilisateurs et les utilisateurs doivent se souvenir d'un seul jeu d'informations d'identification. Toutefois, ces informations d'identification peuvent être utilisées pour fournir l'accès à un grand choix d'applications, qui peuvent se trouver dans un grand nombre d'emplacements.

Ce module fournit une vue d'ensemble des services AD FS, puis décrit de manière détaillée comment configurer les services AD FS dans un seul scénario d'organisation et dans un scénario d'organisation partenaire.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire les services AD FS ;
- expliquer comment configurer les conditions préalables des services AD FS et déployer ces services ;
- décrire comment implémenter des services AD FS pour une seule organisation ;
- déployer AD FS dans un scénario de fédération B2B.

Leçon 1
Vue d'ensemble d'AD FS

AD FS est l'implémentation Microsoft d'une infrastructure de fédération d'identités qui permet aux organisations d'établir des approbations de fédération et de partager des ressources au-delà des limites de l'organisation et des services de domaine Active Directory (AD DS). AD FS est conforme aux normes des services Web courants pour activer l'interopérabilité avec des solutions de fédération d'identités fournies par d'autres fournisseurs.

AD FS est conçu pour traiter un grand nombre de scénarios d'entreprise, dans lesquels les mécanismes d'authentification typiques utilisés dans une seule organisation ne fonctionnent pas. Cette leçon fournit une vue d'ensemble des concepts et des normes implémentés dans AD FS et également des scénarios d'entreprise qui peuvent être traités avec AD FS.

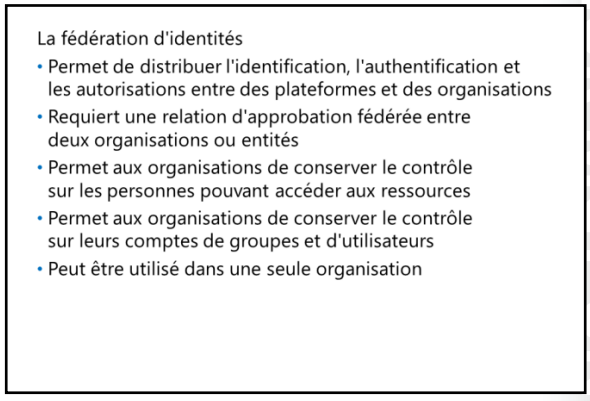
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire la fédération d'identités ;
- décrire l'identité basée sur les revendications ;
- décrire les services Web ;
- décrire les services AD FS ;
- expliquer comment AD FS active l'authentification unique (SSO) au sein d'une seule organisation ;
- expliquer comment AD FS active l'authentification unique (SSO) entre les partenaires professionnels ;
- expliquer comment AD FS active l'authentification unique (SSO) entre les services sur site et basés sur le cloud.

Qu'est-ce que la fédération d'identités ?

La fédération d'identités active la distribution de l'identification, de l'authentification et de l'autorisation entre des organisations et des plateformes. Vous pouvez implémenter la fédération d'identités au sein d'une seule organisation pour permettre l'accès aux diverses applications Web, ou entre deux organisations qui ont une relation d'approbation entre elles.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour établir un partenariat de fédération d'identités, les deux partenaires créent une relation d'approbation fédérée. Cette approbation fédérée est basée sur une relation professionnelle actuelle et permet aux organisations d'implémenter des processus métier identifiés dans la relation professionnelle.

Remarque : Une approbation fédérée n'est pas identique à l'approbation de forêt que les organisations peuvent configurer entre les forêts AD DS. Dans une approbation fédérée, les serveurs AD FS de deux organisations ne doivent jamais communiquer directement entre eux. En outre, toutes les communications d'un déploiement de fédération s'effectuent via HTTPS, vous n'avez donc pas besoin d'ouvrir plusieurs ports sur tous les pare-feu pour activer la fédération.

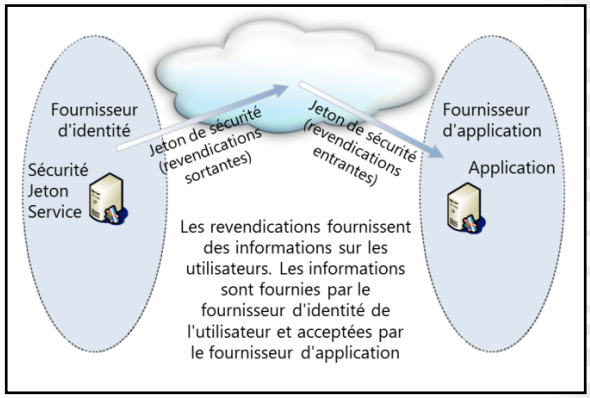
Dans le cadre de l'approbation fédérée, chaque partenaire définit les ressources accessibles et la méthode d'accès. Par exemple, pour mettre à jour des prévisions de ventes, un commercial devra peut-être collecter des informations à partir de la base de données d'un fournisseur hébergée sur le réseau du fournisseur. L'administrateur du domaine du commercial est chargé de vérifier que les commerciaux appropriés sont membres du groupe qui a besoin de l'accès à la base de données du fournisseur. L'administrateur de l'organisation dans laquelle la base de données se trouve est chargé de vérifier que les employés du partenaire ont accès uniquement aux données dont ils ont besoin.

Dans une solution de fédération d'identités, les identités des utilisateurs et leurs informations d'identification associées sont enregistrées, conservées et gérées par l'organisation dans laquelle l'utilisateur se trouve. Dans le cadre de l'approbation de fédération d'identités, chaque organisation définit également comment les identités des utilisateurs sont partagées de façon sécurisée pour restreindre l'accès aux ressources. Chaque partenaire doit définir les services qu'il met à la disposition des partenaires de confiance et des clients, ainsi que les organisations et les utilisateurs de confiance. Chaque partenaire doit également définir les types d'informations d'identification et de demandes qu'il accepte et sa stratégie de confidentialité afin de garantir que les informations confidentielles ne sont pas accessibles via l'approbation.

Vous pouvez également utiliser la fédération d'identités au sein d'une seule organisation. Par exemple, une organisation peut prévoir de déployer plusieurs applications Web qui requièrent une authentification. À l'aide d'AD FS, l'organisation peut implémenter une solution d'authentification pour toutes les applications, ce qui facilite l'accès à l'application des utilisateurs de plusieurs domaines ou forêts internes. Vous pouvez également étendre la solution aux partenaires externes dans l'avenir, sans modifier l'application.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que l'identité basée sur les revendications ?



L'authentification basée sur les revendications est conçue pour résoudre les problèmes en étendant les mécanismes typiques d'authentification et d'autorisation en dehors des limites associées à ce mécanisme. Par exemple, dans la plupart des organisations, lorsque les utilisateurs se connectent au réseau, ils sont authentifiés par un contrôleur de domaine AD DS. Un utilisateur qui fournit les bonnes informations d'identification au contrôleur de domaine se voit accorder un jeton de sécurité. Les applications qui s'exécutent sur des serveurs dans le même environnement AD DS font confiance aux jetons de sécurité fournis par les contrôleurs de domaine AD DS, car les serveurs peuvent communiquer avec les mêmes contrôleurs de domaine dans lesquels les utilisateurs sont authentifiés.

Le problème avec ce type d'authentification est qu'il ne s'étend pas facilement en dehors des limites de la forêt AD DS. Même s'il est possible d'implémenter l'authentification Kerberos ou les approbations NTLM entre deux forêts AD DS, les ordinateurs clients et les contrôleurs de domaine de chaque côté de l'approbation doivent communiquer avec les contrôleurs de domaine de l'autre forêt pour prendre des décisions relatives à l'authentification et à l'autorisation. Cette communication requiert le trafic réseau envoyé sur plusieurs ports, ces ports doivent donc être ouverts sur tous les pare-feu entre les contrôleurs de domaine et les autres ordinateurs. Le problème devient encore plus compliqué quand les utilisateurs doivent accéder aux ressources hébergées dans des systèmes basés sur le cloud, tels que Windows Azure™ ou Microsoft® Office 365.

L'authentification basée sur les revendications fournit un mécanisme permettant de séparer l'authentification et l'autorisation des utilisateurs des applications individuelles. Avec l'authentification basée sur les revendications, les utilisateurs peuvent s'authentifier sur un service d'annuaire situé au sein de leur organisation et se voir accorder une revendication basée sur cette authentification. La revendication peut alors être présentée à une application qui s'exécute dans une organisation différente. L'application est conçue pour activer l'accès des utilisateurs aux informations ou aux fonctionnalités, en fonction des revendications présentées. Toutes les communications s'effectuent également via HTTPS.

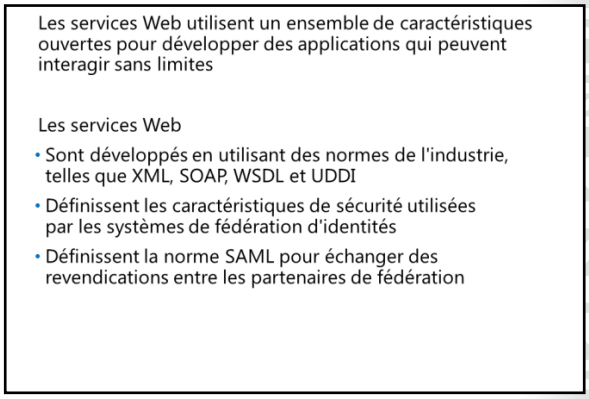
La revendication utilisée dans l'authentification basée sur les revendications est une déclaration faite à propos d'un utilisateur qui est défini dans une organisation ou une technologie et approuvé dans une autre organisation ou technologie. La revendication peut inclure de nombreuses informations. Par exemple, la revendication peut définir l'adresse de messagerie de l'utilisateur, le nom d'utilisateur principal (UPN) et les informations sur les groupes spécifiques auxquels l'utilisateur appartient. Ces informations sont recueillies à partir du mécanisme d'authentification lorsque l'utilisateur a réussi à s'authentifier.

L'organisation qui gère l'application définit les types de revendications qui seront acceptés par l'application. Par exemple, l'application peut avoir besoin de l'adresse de messagerie de l'utilisateur pour vérifier l'identité de l'utilisateur. Elle peut alors ensuite utiliser l'appartenance au groupe présentée dans la revendication pour déterminer le niveau d'accès de l'utilisateur au sein de l'application.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des services Web

Pour que l'authentification basée sur les revendications fonctionne, les organisations doivent se mettre d'accord sur le format des échanges de revendications. Au lieu de demander à chaque entreprise de définir ce format, un ensemble de spécifications largement identifiées comme *services Web* a été développé. Toute organisation qui souhaite implémenter une solution d'identité fédérée peut utiliser cet ensemble de spécifications.



Les services Web sont un ensemble de spécifications utilisées pour générer des applications et des services connectés, dont la fonctionnalité et les interfaces sont exposées aux utilisateurs potentiels via des normes de technologie Web tels que XML, SOAP, WSDL (Web Services Description Language) et HTTP. L'objectif de la création des applications Web utilisant des services Web consiste à simplifier l'interopérabilité des applications entre plusieurs plateformes de développement, technologies et réseaux.

Pour améliorer l'interopérabilité, les services Web sont définis par un ensemble de normes du secteur. Les services Web sont basés sur les normes suivantes :

- La plupart des services Web utilisent le code XML pour transmettre des données via HTTP(S). Avec XML, les développeurs peuvent créer leurs propres balises personnalisées, et de cette façon simplifier la définition, la transmission, la validation et l'interprétation des données entre les applications et les organisations.
- Les services Web exposent une fonctionnalité utile aux utilisateurs Web via un protocole Web standard. Dans la plupart des cas, le protocole utilisé est SOAP, qui est le protocole de communication pour les services Web XML. SOAP est une spécification qui définit le format XML des messages et décrit essentiellement à quoi ressemble un document XML valide.
- Les services Web fournissent un moyen de décrire leurs interfaces de façon assez détaillée pour permettre à un utilisateur de créer une application cliente afin de communiquer avec le service. Cette description est généralement fournie dans un document XML appelé document WSDL. En d'autres termes, un fichier WSDL est un document XML qui décrit un ensemble de messages SOAP et la façon dont les messages sont échangés.
- Les services Web sont enregistrés de sorte que les utilisateurs potentiels puissent les trouver facilement. Ceci est réalisé grâce aux fonctionnalités UDDI (Description, découverte et intégration universelles). Une entrée de répertoire UDDI est un fichier XML qui décrit une entreprise et les services qu'elle propose.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Spécifications de sécurité WS-*

Les spécifications des services Web (également appelées spécifications WS-*) possèdent plusieurs composants. Toutefois, les spécifications les plus appropriées d'un environnement AD FS sont les spécifications WS-Security. Les spécifications qui font partie des spécifications WS-Security incluent ce qui suit :

- WS-Security : sécurité des messages SOAP et profil de jeton du certificat X.509. WS-Security décrit les améliorations apportées à la messagerie SOAP. Ces améliorations fournissent l'intégrité, la confidentialité et l'authentification unique des messages. WS-Security fournit également un mécanisme à usage général et encore extensible pour associer des jetons de sécurité à des messages et à un mécanisme pour encoder les jetons de sécurité binaires, spécifiquement les certificats X.509 et les tickets Kerberos dans les messages SOAP.
- WS-Trust. WS-Trust définit les extensions qui s'appuient sur la norme WS-Security pour demander et délivrer des jetons de sécurité et pour gérer les relations d'approbation.
- WS-Federation. WS-Federation définit les mécanismes utilisés par WS-Security pour permettre la fédération d'identités, d'authentifications et d'autorisations basée sur des attributs entre les différents domaines d'approbation.
- Profil de demandeur passif WS-Federation. Cette extension de WS-Security décrit comment les clients passifs, tels que les navigateurs Web, peuvent acquérir des jetons à partir d'un serveur de fédération et comment les clients peuvent soumettre les jetons à un serveur de fédération. Les demandeurs passifs de ce profil sont limités au protocole HTTP ou HTTPS.
- Profil de demandeur actif WS-Federation. Cette extension WS-Security décrit comment des clients actifs, tels que des applications d'appareils mobiles basées sur SOAP, peuvent être authentifiés et autorisés, et comment les clients peuvent envoyer les revendications dans un scénario de fédération.

SAML (Security Assertion Markup Language)

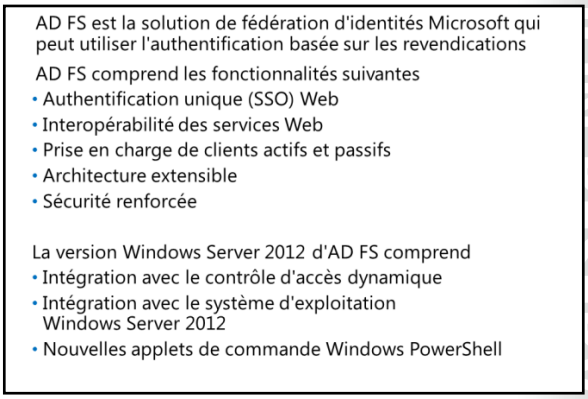
SAML (Security Assertion Markup Language) est une norme basée sur XML permettant l'échange des revendications entre un fournisseur d'identité et un fournisseur de services ou d'applications. SAML suppose qu'un utilisateur a été authentifié par un fournisseur d'identité et que ce dernier a rempli les informations de revendication appropriées dans le jeton de sécurité. Lorsque l'utilisateur est authentifié, le fournisseur d'identité passe une assertion SAML au fournisseur de services. En se basant sur cette assertion, le fournisseur de services peut prendre des décisions d'autorisation et de personnalisation au sein d'une application. La communication entre les serveurs de fédération est basée sur un document XML qui stocke le certificat X.509 pour la signature de jetons, et le jeton SAML 1.1 ou SAML 2.0.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce qu'AD FS ?

AD FS est l'implémentation Microsoft d'une solution de fédération d'identités qui utilise l'authentification basée sur les revendications. AD FS fournit les mécanismes permettant d'implémenter le fournisseur d'identité et les composants du fournisseur de services dans un déploiement de fédération d'identités.



AD FS offre les fonctionnalités suivantes :

- Fournisseur de revendications d'entreprise pour des applications basées sur les revendications. Vous pouvez configurer un serveur AD FS en tant que fournisseur de revendications, ce qui signifie qu'il peut émettre des revendications à propos des utilisateurs authentifiés. Cela permet à une organisation de fournir à ses utilisateurs l'accès aux applications prenant en charge les revendications dans une autre organisation à l'aide de l'authentification unique (SSO).
- Fournisseur de services de fédération pour la fédération d'identité entre les domaines. Ce service offre l'authentification unique (SSO) Web fédérée sur les domaines, renforçant ainsi la sécurité et réduit la charge des administrateurs informatiques.

Remarque : La version d'AD FS pour Windows Server 2012 est basée sur la version 2.0 d'AD FS, qui est la seconde génération d'AD FS publiée par Microsoft. La première version, AD FS 1.0, nécessitait l'installation d'agents Web AD FS sur tous les serveurs Web qui utilisaient AD FS et fournissait l'authentification prenant en charge les revendications et étant basée sur les jetons NT. AD FS 1.0 ne prenait pas en charge les clients actifs, mais prend en charge les jetons SAML.

Fonctionnalités AD FS

Voici quelques fonctionnalités clés d'AD FS :

- Authentification unique (SSO) Web. De nombreuses organisations ont déployé AD DS. Après l'authentification sur AD DS via l'authentification Windows intégrée, les utilisateurs peuvent accéder à toutes les autres ressources auxquelles ils ont l'autorisation d'accéder au sein des limites de forêt AD DS. AD FS étend cette fonction à l'intranet ou aux applications Internet, permettant aux clients, partenaires et fournisseurs d'avoir une expérience utilisateur similaire simplifiée lorsqu'ils accèdent aux applications Web d'une organisation.
- Interopérabilité des services Web. AD FS est compatible avec les spécifications des services Web. AD FS utilise la spécification de fédération de WS-*, appelée WS-Federation. Cette spécification permet aux environnements qui n'utilisent pas le modèle d'identité Windows d'être fédérés aux environnements Windows.

- Prise en charge de clients actifs et passifs. Puisqu'AD FS est basé sur l'architecture WS-*, il prend en charge les communications fédérées entre tous les points de terminaison activés pour WS, y compris les communications entre les serveurs et les clients passifs, tels que les navigateurs. AD FS sur Windows Server 2012 permet également l'accès à tous les clients actifs basés sur SOAP, tels que les serveurs, les téléphones mobiles, les assistants numériques personnels (PDA) et les applications de bureau. AD FS implémente le profil de demandeur passif WS-Federation et certaines normes du profil de demandeur actif WS-Federation pour la prise en charge des clients.
- Architecture extensible. AD FS fournit une architecture extensible qui prend en charge divers types de jetons de sécurité, y compris les jetons SAML et l'authentification Kerberos via l'authentification Windows intégrée, et la possibilité d'effectuer des transformations de revendications personnalisées. Par exemple, AD FS peut effectuer une conversion d'un type de jeton vers un autre, ou ajouter une logique métier personnalisée en tant que variable d'une demande d'accès. Les organisations peuvent utiliser cette extensibilité afin de modifier AD FS pour coexister avec leur infrastructure de sécurité et leurs stratégies d'entreprise actuelles.
- Sécurité renforcée. AD FS permet d'augmenter la sécurité des solutions fédérées en déléguant la responsabilité de la gestion des comptes à l'organisation la plus proche de l'utilisateur. Chaque organisation individuelle d'une fédération continue à gérer ses propres identités et est apte à partager et à accepter en toute sécurité les identités et les informations d'identification des sources des autres membres.

 **Documentation supplémentaire :** Pour obtenir des informations sur les différents produits de fédération d'identité qui peuvent interagir avec AD FS et des guides étape par étape sur la façon de configurer les produits, consultez le guide étape par étape et le guide pratique AD FS 2.0 à l'adresse http://go.microsoft.com/fwlink/?LinkId=270035.

Nouvelles fonctionnalités dans Windows Server 2012 AD FS

La version d'AD FS pour Windows Server 2012 comprend plusieurs nouvelles fonctionnalités :

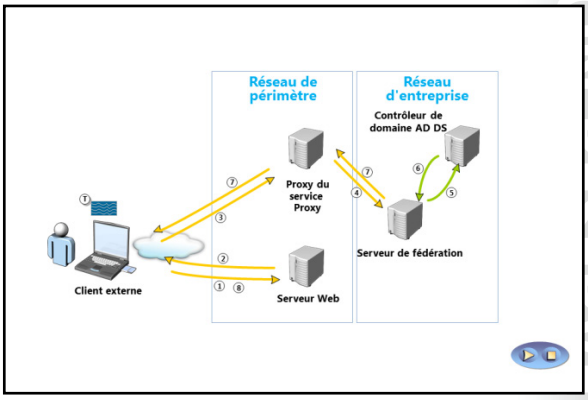
- Intégration avec le système d'exploitation Windows Server 2012. Dans Windows Server 2012, AD FS est inclus en tant que rôle serveur que vous pouvez installer à l'aide du Gestionnaire de serveur. Quand vous installez le rôle serveur, tous les composants requis du système d'exploitation s'installent automatiquement.
- Intégration avec le contrôle d'accès dynamique. Lors du déploiement du contrôle d'accès dynamique, vous pouvez configurer les revendications de l'utilisateur et du périphérique qui sont émises par des contrôleurs de domaine AD DS. AD FS peut consommer les revendications AD DS que les contrôleurs de domaine émettent. Cela signifie qu'AD FS peut prendre les décisions d'autorisation selon les comptes d'utilisateurs et les comptes d'ordinateurs.
- Applets de commande Windows PowerShell® pour l'administration d'AD FS. Windows Server 2012 fournit plusieurs nouvelles applets de commande Windows PowerShell que vous pouvez utiliser pour installer et configurer le rôle serveur AD FS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment AD FS active l'authentification unique (SSO) dans une seule organisation

Pour de nombreuses organisations, la configuration de l'accès aux applications et aux services ne nécessite pas forcément le déploiement d'AD FS. Si tous les utilisateurs sont des membres de la même forêt AD DS et si toutes les applications sont exécutées sur les serveurs qui appartiennent à la même forêt, vous pouvez généralement utiliser l'authentification AD DS pour fournir l'accès à l'application. Cependant, dans plusieurs scénarios, vous pouvez utiliser AD FS pour améliorer l'expérience de l'utilisateur en autorisant l'authentification unique (SSO) :



- Les applications ne nécessitent pas d'être exécutées sur les serveurs Windows ou sur tout serveur qui prend en charge l'authentification AD DS ou sur les serveurs Windows Server qui ne sont pas joints au domaine. Les applications peuvent nécessiter des services Web ou SAML pour l'authentification et l'autorisation.
- Les grandes organisations ont souvent plusieurs domaines et forêts qui peuvent provenir de fusions et d'acquisitions ou en raison d'exigences de sécurité. Les utilisateurs de plusieurs forêts peuvent nécessiter l'accès aux mêmes applications.
- Les utilisateurs en dehors du bureau peuvent avoir besoin d'accéder aux applications qui sont exécutées sur les serveurs internes. Les utilisateurs externes peuvent se connecter aux applications à partir d'ordinateurs qui ne font pas partie du domaine interne.

Remarque : L'implémentation d'AD FS ne signifie pas nécessairement que les utilisateurs ne sont pas invités à s'authentifier lorsqu'ils accèdent aux applications. Selon le scénario, les utilisateurs peuvent être invités à indiquer leurs informations d'identification. Cependant, les utilisateurs s'authentifient toujours à l'aide de leurs informations d'identification internes dans le domaine de compte approuvé et n'ont jamais besoin de se souvenir d'autres informations d'identification pour l'application. En outre, les informations d'identification internes ne sont jamais présentées à l'application ou au serveur AD FS du partenaire.

Les organismes peuvent utiliser AD FS pour activer l'authentification unique (SSO) dans ces scénarios. Puisque tous les utilisateurs et l'application sont dans la même forêt AD DS, l'organisation n'a plus qu'à déployer un serveur de fédération unique. Ce serveur peut fonctionner comme fournisseur de revendications pour authentifier les demandes de l'utilisateur et émettre les revendications. Ce même serveur est également la partie de confiance ou le consommateur des revendications pour fournir l'autorisation d'accès aux applications.

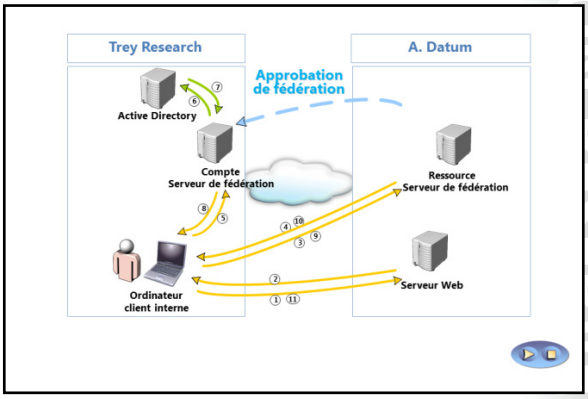
Remarque : La diapositive et la description suivante utilisent les termes service de fédération et proxy du service de fédération pour décrire les services de rôle AD FS. Le *serveur de fédération* est responsable de l'émission des revendications et, dans ce scénario, est également responsable de la consommation des revendications. Le *proxy du service de fédération* est un composant proxy recommandé pour les déploiements où les utilisateurs en dehors du réseau doivent accéder à l'environnement AD FS. Ces composants sont examinés plus en détail dans la leçon suivante.

Les étapes suivantes décrivent le flux de communication dans ce scénario.

1. L'ordinateur client, situé en dehors du réseau, doit accéder à une application Web sur le serveur Web. L'ordinateur client envoie une demande HTTPS au serveur Web.
2. Le serveur Web reçoit la demande et identifie que l'ordinateur client n'a pas de revendication. Le serveur Web redirige l'ordinateur client vers le proxy du service de fédération.
3. L'ordinateur client envoie une demande HTTPS au proxy du service de fédération. Selon le scénario, le proxy du service de fédération peut inviter l'utilisateur à s'authentifier, ou utiliser l'authentification Windows intégrée pour recueillir les informations d'identification de l'utilisateur.
4. Le proxy du service de fédération transmet la demande et les informations d'identification au serveur de fédération.
5. Le serveur de fédération utilise AD DS pour authentifier l'utilisateur.
6. Si l'authentification est réussie, le serveur de fédération collecte les informations AD DS sur l'utilisateur, qui sont ensuite utilisées pour générer les revendications de l'utilisateur.
7. Si l'authentification est réussie, les informations d'authentification et les autres informations sont recueillies dans un jeton de sécurité et retransmises à l'ordinateur client via le proxy du service de fédération.
8. Le client présente ensuite le jeton au serveur Web. La ressource Web reçoit la demande, valide les jetons signés et utilise les revendications dans le jeton de l'utilisateur pour fournir l'accès à l'application.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Activation par AD FS de l'authentification unique (SSO) dans une fédération B2B



Un des scénarios les plus classiques pour déployer AD FS consiste à permettre l'authentification unique (SSO) dans une fédération B2B. Dans le scénario, l'organisation qui a besoin d'accéder à une application ou à un service d'une autre organisation peut gérer ses propres comptes utilisateurs et définir ses propres mécanismes d'authentification. L'autre organisation peut alors définir les applications et les services qu'elle expose aux utilisateurs en dehors de l'organisation et les revendications qu'elle accepte pour fournir l'accès à ces applications et ces services. Pour activer le partage de l'application ou du service dans ce scénario, les organisations doivent établir une approbation de fédération, puis définir les règles pour échanger les revendications entre les deux organisations.

La diapositive de cette rubrique montre le flux du trafic dans un scénario B2B fédéré à l'aide d'une application Web prenant en charge les revendications. Dans ce scénario, les utilisateurs de Trey Research doivent accéder à une application Web de la société A. Datum. Le processus d'authentification AD FS pour ce scénario est le suivant :

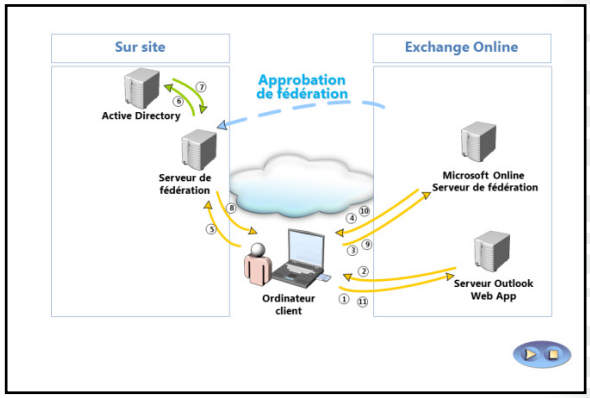
1. Un utilisateur de Trey Research utilise un navigateur Web pour établir une connexion HTTPS au serveur Web de la société A. Datum.
2. L'application Web reçoit la demande et vérifie que l'utilisateur n'a pas de jeton valide enregistré dans un cookie par le navigateur Web. Puisque l'utilisateur n'est pas authentifié, l'application Web redirige le client vers le serveur de fédération d'A. Datum (à l'aide d'un message de redirection HTTP 302).
3. L'ordinateur client envoie une demande HTTPS au serveur de fédération de la société A. Datum. Le serveur de fédération détermine le domaine d'accueil pour l'utilisateur. Dans ce cas, le domaine d'accueil est Trey Research.
4. L'ordinateur client est redirigé à nouveau vers le serveur de fédération dans le domaine d'accueil, Trey Research.
5. L'ordinateur client envoie une demande HTTPS au serveur de fédération Trey Research.
6. Si l'utilisateur est déjà connecté au domaine, le serveur de fédération peut utiliser le ticket d'authentification Kerberos de l'utilisateur pour demander l'authentification à partir d'AD DS pour le compte de l'utilisateur, à l'aide de l'authentification intégrée Windows. Si l'utilisateur n'est pas connecté au domaine, il est invité à indiquer ses informations d'identification.
7. Le contrôleur de domaine AD DS authentifie l'utilisateur et renvoie le message de réussite au serveur de fédération, avec d'autres informations relatives à l'utilisateur qui peuvent être utilisées pour générer les revendications de l'utilisateur.
8. Le serveur de fédération crée la revendication pour l'utilisateur selon les règles définies pour le partenaire de fédération. Les données de revendications sont placées dans un jeton de sécurité signé numériquement, puis envoyées vers l'ordinateur client, qui le renvoie au serveur de fédération de la société A. Datum.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Le serveur de fédération de la société A. Datum valide que le jeton de sécurité provient d'un partenaire de fédération de confiance.
10. Le serveur de fédération de la société A. Datum crée et signe un nouveau jeton, qu'il envoie ensuite à l'ordinateur client, qui l'envoie alors à son tour à l'URL d'origine demandée.
11. L'application sur le serveur Web reçoit la demande et valide les jetons signés. Le serveur Web délivre au client un cookie de session indiquant qu'il a été authentifié avec succès et un cookie persistant basé sur un fichier est délivré par le serveur de fédération (validité par défaut 30 jours) pour supprimer l'étape de découverte du domaine d'accueil pendant la durée de vie du cookie. Le serveur fournit ensuite l'accès à l'application selon les revendications fournies par l'utilisateur.

Activation par AD FS de l'authentification unique (SSO) avec les services en ligne

Comme les organisations déplacent les services et les applications vers les services basés sur le cloud, il est de plus en plus important que ces organisations puissent simplifier l'expérience d'authentification et d'autorisation pour leurs utilisateurs, car ils consomment les services basés sur le cloud. Les services basés sur le cloud ajoutent un autre degré de complexité à l'environnement informatique, puisqu'ils sont situés en dehors du contrôle administratif direct des administrateurs informatiques, et peuvent être exécutés sur de nombreuses plateformes différentes.



Vous pouvez utiliser AD FS pour fournir aux utilisateurs une expérience d'authentification unique (SSO) sur les diverses plateformes disponibles basées sur le cloud. Par exemple, une fois que les utilisateurs sont authentifiés avec les informations d'identification AD DS, ils peuvent alors accéder aux services en ligne Microsoft, tels que les solutions hébergées Microsoft Exchange Online ou SharePoint® Online, à l'aide de ces informations d'identification de domaine.

AD FS peut également fournir l'authentification unique (SSO) aux fournisseurs de cloud non Microsoft. Puisqu'AD FS est basé sur des normes ouvertes, il peut interagir avec tout système de revendications conforme.

Le processus d'accès à une application basée sur le cloud est assez semblable au scénario B2B. Un déploiement hybride Exchange Online est un exemple de service basé sur le cloud qui utilise AD FS pour l'authentification. Dans ce type de déploiement, une organisation déploie certaines de ses boîtes aux lettres dans un environnement Microsoft Office 365™ et Exchange Online. Cependant, l'organisation gère tous ses comptes utilisateurs dans son environnement AD DS sur site. Le déploiement utilise l'outil de synchronisation d'annuaires Microsoft Online Services pour synchroniser les informations des comptes d'utilisateurs à partir du déploiement sur site vers le déploiement Exchange Online.

Lorsque l'utilisateur tente de se connecter à sa boîte aux lettres Exchange Online, il doit être authentifié à l'aide de ses informations d'identification AD DS internes. Si les utilisateurs tentent de se connecter directement à l'environnement Exchange Online, ils sont redirigés de nouveau au déploiement interne d'AD FS pour l'authentification avant d'avoir l'accès.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les étapes suivantes décrivent ce qui se produit quand un utilisateur tente d'accéder à sa boîte aux lettres en ligne à l'aide d'un navigateur Web :

1. L'utilisateur ouvre un navigateur Web et envoie une demande HTTPS au serveur Exchange Online Microsoft Outlook® Web App.
2. Le serveur Outlook Web App reçoit la demande et vérifie si l'utilisateur fait partie d'un déploiement hybride d'Exchange Server. Si tel est le cas, le serveur redirige l'ordinateur client vers le serveur de fédération Microsoft Online Services.
3. L'ordinateur client envoie une demande HTTPS au serveur de fédération Microsoft Online Services.
4. L'ordinateur client est de nouveau redirigé vers le serveur de fédération sur site. La redirection vers le domaine d'accueil de l'utilisateur est basée sur le suffixe UPN de l'utilisateur.
5. L'ordinateur client envoie une demande HTTPS au serveur de fédération sur site.
6. Si l'utilisateur est déjà connecté au domaine, le serveur de fédération sur site peut prendre le ticket d'authentification Kerberos de l'utilisateur et demander l'authentification à partir d'AD DS pour le compte de l'utilisateur, à l'aide de l'authentification Windows intégrée. Si l'utilisateur est connecté en dehors du réseau ou depuis un ordinateur qui n'appartient pas au domaine interne, il est invité à indiquer ses informations d'identification.
7. Le contrôleur de domaine AD DS authentifie l'utilisateur et renvoie le message de réussite au serveur de fédération, avec d'autres informations relatives à l'utilisateur que le serveur de fédération peut utiliser pour générer les revendications de l'utilisateur.
8. Le serveur de fédération crée la revendication pour l'utilisateur selon les règles définies au cours de la configuration du serveur AD FS. Les données de revendications sont placées dans un jeton de sécurité signé numériquement, puis envoyées vers l'ordinateur client, qui les renvoie au serveur de fédération Microsoft Online Services.
9. Le serveur de fédération Microsoft Online Services valide que le jeton de sécurité provient d'un partenaire de fédération de confiance. Cette approbation est configurée lorsque vous configurez l'environnement hybride Exchange Server.
10. Le serveur de fédération Microsoft Online Services crée et signe un nouveau jeton, qu'il envoie à l'ordinateur client, qui l'envoie à son tour au serveur Outlook Web App.
11. Le serveur Outlook Web App reçoit la demande et valide les jetons signés. Le serveur délivre au client un cookie de session indiquant qu'il a été authentifié avec succès. L'utilisateur se voit alors accorder l'accès à sa boîte aux lettres Exchange Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Déploiement d'AD FS

Une fois que vous avez compris comment AD FS fonctionne, la prochaine étape consiste à déployer le service. Avant de procéder au déploiement d'AD FS, vous devez comprendre les composants que vous devrez déployer ainsi que les conditions préalables, notamment en ce qui concerne les certificats. Cette leçon fournit une vue d'ensemble du déploiement du rôle serveur AD FS dans Windows Server 2012.

Objectifs de la leçon

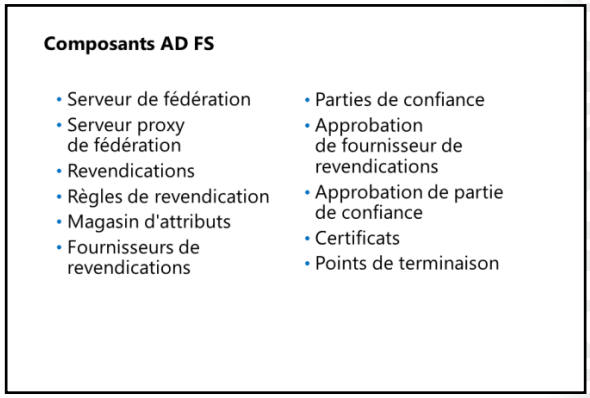
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les composants que vous pouvez inclure dans un déploiement d'AD FS ;
- dresser la liste des conditions préalables au déploiement d'AD FS ;
- décrire l'infrastructure à clé publique (PKI) et les exigences en matière de certificat pour le déploiement d'AD FS ;
- décrire les rôles du serveur de fédération AD FS ;
- installer le rôle serveur AD FS.

Composants AD FS

AD FS est installé en tant que rôle serveur dans Windows Server 2012. Cependant, vous devez installer et configurer plusieurs composants différents dans le cadre d'un déploiement d'AD FS.

Le tableau suivant répertorie les composants AD FS.



Composant	Il exécute les tâches suivantes :
Serveur de fédération	Le serveur de fédération délivre, gère et valide des demandes concernant des revendications d'identité. Toutes les implémentations d'AD FS nécessitent au moins un service de fédération pour chaque forêt participante.
Serveur proxy de fédération	Le serveur proxy de fédération est un composant facultatif que vous déployez généralement dans un réseau de périmètre. Il n'ajoute aucune fonctionnalité au déploiement d'AD FS, mais est déployé uniquement pour fournir une couche de sécurité aux connexions à partir d'Internet vers le serveur de fédération.
Revendications	Une revendication est une déclaration faite par une entité de confiance à propos d'un objet tel qu'un utilisateur. La revendication pourrait inclure le nom d'utilisateur, le titre de la fonction ou tout autre facteur qui pourrait être utilisé dans un scénario d'authentification. Avec Windows Server 2012, l'objet peut être également un périphérique utilisé dans le cadre du déploiement d'un contrôle d'accès dynamique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

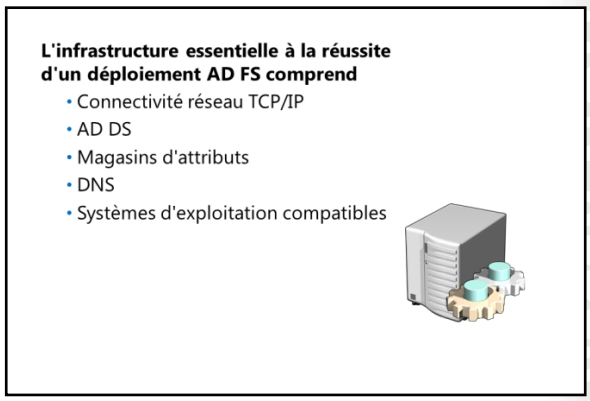
Composant	Il exécute les tâches suivantes :
Règles de revendication	Les règles de revendication déterminent la manière dont les revendications sont traitées par les serveurs de fédération. Par exemple, une règle de revendication peut définir qu'une adresse de messagerie est acceptée en tant que revendication valide, ou qu'un nom de groupe d'une organisation est traduit en un rôle spécifique à une application dans l'autre organisation. Les règles sont généralement traitées en temps réel comme les revendications sont effectuées.
Magasin d'attributs	AD FS utilise un magasin d'attributs pour rechercher les valeurs de revendication. AD DS est un magasin d'attributs commun disponible par défaut, car le rôle du serveur de fédération doit être installé sur un serveur joint au domaine.
Fournisseur de revendications	Le fournisseur de revendications est le serveur qui émet les revendications et authentifie les utilisateurs. Un fournisseur de revendications active un côté du processus d'autorisation et d'authentification AD FS. Le fournisseur de revendications gère l'authentification de l'utilisateur, puis émet les revendications que l'utilisateur présente à une partie de confiance.
Partie de confiance	La partie de confiance est la partie dans laquelle se trouve l'application. Elle active le deuxième côté du processus d'autorisation et d'authentification AD FS. La partie de confiance est un service Web qui consomme les revendications à partir du fournisseur de revendications. Microsoft Windows Identity Foundation doit être installé sur le serveur de la partie de confiance ou doit utiliser l'agent AD FS 1.0 prenant en charge les revendications.
Approbation de fournisseur de revendications	Il s'agit des données de configuration qui définissent les règles selon lesquelles un client peut demander des revendications auprès d'un fournisseur de revendications, puis les soumettre à une partie de confiance. L'approbation est constituée de divers identificateurs tels que les noms, les groupes et différentes règles.
Approbation de partie de confiance	Il s'agit des données de configuration AD FS qui fournissent les revendications à propos d'un utilisateur ou d'un client à une partie de confiance. Elle est constituée de divers identificateurs, tels que les noms, les groupes et différentes règles.
Certificats	AD FS utilise les certificats numériques lors de communications sur SSL ou en tant que partie du processus de délivrance de jetons, du processus de réception de jetons et du processus d'édition des métadonnées. Les certificats numériques sont également utilisés pour la signature de jetons.
Points de terminaison	Les points de terminaison sont des mécanismes WCF (Windows Communication Foundation) qui permettent l'accès aux technologies AD FS, y compris l'émission de jetons et l'édition de métadonnées. AD FS est fourni avec des points de terminaison intégrés qui sont responsables de fonctionnalités spécifiques.

Remarque : Plusieurs de ces composants sont décrits plus en détail dans tout le reste de ce module.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions préalables d'AD FS

Avant de déployer AD FS, vous devez vérifier que votre réseau interne répond à certaines conditions préalables de base. La configuration des services réseau suivants est essentielle à la réussite du déploiement d'AD FS :



- Connectivité du réseau. La connectivité du réseau suivante est requise :
  - L'ordinateur client doit pouvoir communiquer avec l'application Web, le serveur de fédération de ressources ou le serveur proxy de fédération, et le serveur de fédération de comptes ou le proxy de fédération à l'aide de HTTPS.
  - Les serveurs proxy de fédération doivent pouvoir communiquer avec les serveurs de fédération dans la même organisation à l'aide de HTTPS.
  - Les serveurs de fédération et les ordinateurs clients internes doivent pouvoir communiquer avec les contrôleurs de domaine pour l'authentification.
- AD DS. AD DS est une partie essentielle d'AD FS. Les contrôleurs de domaine doivent au minimum exécuter Windows Server 2003 Service Pack 1 (SP1). Les serveurs de fédération doivent être joints à un domaine AD DS. Le proxy du service de fédération ne doit pas être joint au domaine. Même si vous pouvez installer AD FS sur un contrôleur de domaine, nous vous déconseillons de le faire pour des raisons de sécurité.
- Magasins d'attributs. AD FS utilise un magasin d'attributs pour générer les informations relatives aux revendications. Le magasin d'attributs contient les informations relatives aux utilisateurs, qui sont extraites du magasin par le serveur AD FS après l'authentification de l'utilisateur. AD FS prend en charge les magasins d'attributs suivants :
  - Active Directory en mode application (ADAM) dans Windows Server 2003
  - AD LDS (Active Directory Lightweight Directory Services) dans Windows Server 2008, Windows Server 2008 R2 et Windows Server 2012
  - Microsoft SQL Server® 2005 (toutes les éditions)
  - SQL Server 2008 (toutes les éditions)
  - Magasin d'attributs personnalisé

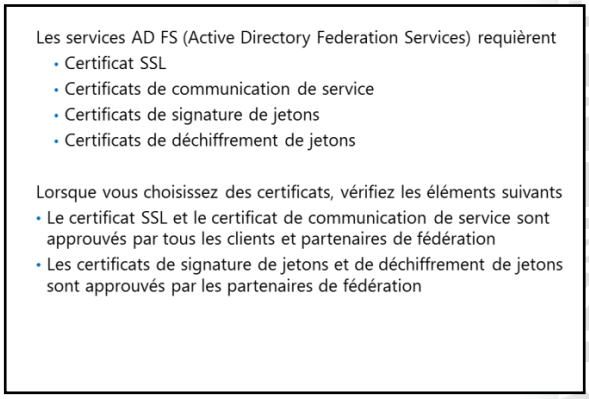
Remarque : AD DS peut être utilisé à la fois comme fournisseur d'authentification et comme magasin d'attributs. AD FS peut également utiliser les services AD LDS comme magasin d'attributs. Dans AD FS 1.x, AD LDS peut être utilisé comme magasin d'authentification, mais dans la version actuelle d'AD FS, AD LDS peut être utilisé uniquement comme magasin d'attributs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- DNS (Domain Name System). La résolution de noms permet aux clients de trouver les serveurs de fédération. Les ordinateurs clients doivent résoudre les noms DNS pour l'ensemble des serveurs de fédération ou des batteries AD FS auxquels ils se connectent et les applications Web que l'ordinateur client tente d'utiliser. Si l'ordinateur client est externe au réseau, l'ordinateur client doit résoudre le nom DNS pour le proxy du service de fédération, et non le serveur de fédération interne ou la batterie AD FS. Le proxy du service de fédération doit résoudre le nom du serveur de fédération interne ou de la batterie. Si les utilisateurs ont directement accès au serveur de fédération interne et si les utilisateurs externes doivent se connecter via le serveur proxy de fédération, vous devrez configurer différents enregistrements DNS dans les zones DNS internes et externes.
- Conditions préalables au système d'exploitation. Vous pouvez déployer uniquement la version d'AD FS pour Windows Server 2012 comme rôle serveur sur un serveur Windows Server 2012.

Exigences en matière de certificat et d'infrastructure à clé publique

Les services AD FS sont conçus pour permettre aux ordinateurs de communiquer en toute sécurité, même s'ils sont situés à des emplacements différents. Dans ce scénario, la plupart des communications entre les ordinateurs transite via Internet. Pour garantir la sécurité du trafic du réseau, toutes les communications sont protégées via SSL (Secure Sockets Layer). Ce facteur signifie qu'il est important de choisir et d'attribuer correctement les certificats SSL aux serveurs AD FS. Pour fournir la sécurité SSL, les serveurs AD FS utilisent les certificats en tant que certificats de communication de service, certificats de signature de jetons et certificats de déchiffrement de jetons.



Certificat SSL

Vous utilisez un certificat SSL pour sécuriser les communications vers les sites Web qui s'exécutent sur les serveurs de fédération et les serveurs proxy de fédération. Ce certificat est lié par défaut au site Internet sur les serveurs de fédération. Le certificat SSL doit être géré à l'aide du Gestionnaire IIS (Internet Information Server).

Certificats de communication de service

Les serveurs de fédération utilisent un certificat d'authentification de serveur pour activer la sécurité des messages WCF. Par défaut, il s'agit du même certificat que celui utilisé par un serveur de fédération comme certificat SSL dans IIS. Vous pouvez choisir le certificat à utiliser lorsque vous configurez le rôle serveur AD FS sur le serveur et vous pouvez modifier le certificat attribué après le déploiement en utilisant la console AD FS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Certificats de signature de jetons

Le certificat de signature de jetons est utilisé pour signer chaque jeton délivré par un serveur de fédération. Ce certificat est essentiel dans un déploiement d'AD FS, car la signature de jetons indique le serveur de fédération qui a délivré le jeton. Ce certificat est utilisé par le fournisseur de revendications pour s'identifier, et est utilisé par la partie de confiance pour vérifier que le jeton provient d'un partenaire de fédération de confiance.

La partie de confiance exige également un certificat de signature de jetons pour signer les jetons qu'elle prépare pour les autres composants AD FS, tels que les applications et les clients Web. Ces jetons doivent être signés par le certificat de signature de jetons de la partie de confiance pour être validés par les applications de destination.

Lorsque vous configurez un serveur de fédération, le serveur attribue un certificat auto-signé en tant que certificat de signature de jetons. Puisqu'aucune autre partie n'approuve le certificat auto-signé, vous pouvez choisir de remplacer le certificat auto-signé par un certificat approuvé. Vous pouvez également configurer tous les serveurs de fédération dans les organisations partenaires pour approuver le certificat auto-signé. Vous pouvez avoir plusieurs certificats de signature de jetons configurés sur le serveur de fédération, mais seul le certificat principal est utilisé pour signer les jetons.

Certificats de déchiffrement de jetons

Les certificats de chiffrement de jetons sont utilisés pour chiffrer le jeton d'utilisateur avant sa transmission à travers le réseau. Pour fournir cette fonctionnalité, la clé publique du certificat du serveur de fédération de la partie de confiance doit être fournie au serveur de fédération du fournisseur de revendications. Le certificat est envoyé sans clé privée. Le serveur du fournisseur de revendications utilise la clé publique à partir du certificat pour chiffrer le jeton d'utilisateur. Lorsque le jeton est renvoyé au serveur de fédération de la partie de confiance, il utilise la clé privée à partir du certificat pour déchiffrer le jeton. Cela fournit une couche de sécurité supplémentaire lors de la transmission du certificat via Internet.

Lorsque vous configurez un serveur de fédération, le serveur attribue un certificat auto-signé comme certificat de déchiffrement de jetons. Puisqu'aucune autre partie n'approuve le certificat auto-signé, vous pouvez choisir de remplacer le certificat auto-signé par un certificat approuvé. Vous pouvez également configurer tous les serveurs de fédération dans les organisations partenaires pour approuver le certificat auto-signé.

 **Remarque :** Les serveurs proxy de fédération exigent uniquement un certificat SSL, qui est utilisé pour activer la communication SSL de toutes les connexions clientes. Étant donné que le serveur proxy de fédération ne délivre pas de jeton, il n'a pas besoin d'autres types de certificats. Pour activer les communications sécurisées avec les ordinateurs clients, les serveurs Web déployés dans le cadre d'un déploiement d'AD FS doivent être configurés avec les certificats de serveur SSL.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sélection d'une autorité de certification

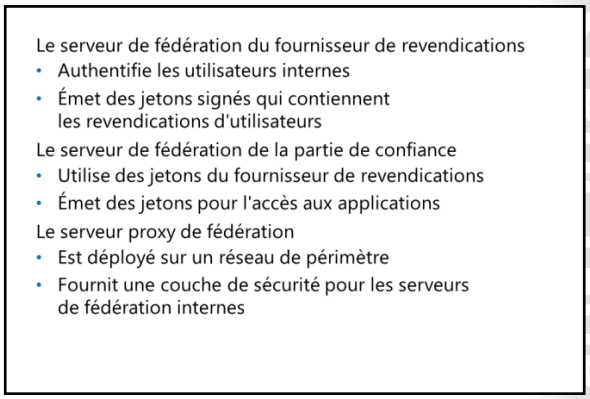
Les serveurs de fédération AD FS peuvent utiliser les certificats auto-signés, les certificats à partir d'une autorité de certification privée ou interne, ou les certificats acquis auprès d'une autorité de certification externe ou publique. Dans la plupart des déploiements d'AD FS, le facteur le plus important lors de la sélection des certificats est l'approbation des certificats par toutes les parties concernées. Cela signifie que si vous configurez un déploiement d'AD FS qui interagit avec d'autres organisations, vous devez certainement utiliser une autorité de certification publique pour le certificat SSL sur le serveur proxy de fédération, car les certificats délivrés par l'autorité de certification publique sont approuvés automatiquement par tous les partenaires.

Si vous déployez AD FS uniquement pour votre organisation et si tous les serveurs et ordinateurs clients sont sous votre contrôle, envisagez d'utiliser un certificat d'une autorité de certification privée et interne. Si vous déployez une autorité de certification d'entreprise interne sur Windows Server 2012, vous pouvez utiliser la stratégie de groupe pour garantir que tous les ordinateurs de l'organisation approuvent automatiquement les certificats délivrés par l'autorité de certification interne. Le recours à une autorité de certification interne peut réduire considérablement le coût des certificats.

Remarque : Le déploiement d'une autorité de certification interne à l'aide des services de certificats Active Directory (AD CS) est un processus simple, mais il est essentiel de le planifier et de l'implémenter avec précaution.

Rôles du serveur de fédération

Lorsque vous installez le rôle serveur AD FS, vous pouvez configurer le serveur comme un serveur de fédération ou comme un serveur proxy de fédération. Après l'installation du rôle du serveur de fédération, vous pouvez configurer le serveur comme fournisseur de revendications, partie de confiance ou les deux à la fois. Ces fonctions de serveur sont les suivantes :



- Fournisseur de revendications. Un fournisseur de revendications est un serveur de fédération qui fournit aux utilisateurs les jetons signés qui contiennent les revendications. Les serveurs de fédération du fournisseur de revendications sont déployés dans les organisations dans lesquelles se trouvent les comptes d'utilisateurs. Lorsqu'un utilisateur demande un jeton, le serveur de fédération du fournisseur de revendications vérifie l'authentification de l'utilisateur à l'aide d'AD DS, puis collecte les informations à partir d'un magasin d'attributs (AD DS ou AD LDS, par exemple) pour remplir la revendication de l'utilisateur avec les attributs requis par l'organisation partenaire. Le serveur délivre les jetons au format SAML. Le serveur de fédération du fournisseur de revendications protège également le contenu des jetons de sécurité en transit en les signant et en les chiffrant, le cas échéant.

- Partie de confiance. Une partie de confiance est un serveur de fédération qui reçoit les jetons de sécurité d'un fournisseur de revendications approuvé. Les serveurs de fédération de la partie de confiance sont déployés dans les organisations qui fournissent l'accès à l'application aux organisations du fournisseur de revendications. La partie de confiance accepte et valide la revendication, puis délivre de nouveaux jetons de sécurité que le serveur Web peut utiliser pour fournir l'accès approprié à l'application.

 **Remarque :** Un seul serveur AD FS peut fonctionner à la fois en tant que fournisseur de revendications et en tant que partie de confiance, même avec les mêmes organisations partenaires. Le serveur AD FS fonctionne en tant que fournisseur de revendications lorsqu'il authentifie les utilisateurs et fournit les jetons pour une autre organisation, mais il accepte également les jetons de la même organisation ou d'une autre organisation dans un rôle de partie de confiance.

- Serveur proxy de fédération. Un serveur proxy de fédération fournit un niveau supplémentaire de sécurité pour le trafic AD FS en provenance d'Internet vers les serveurs de fédération AD FS internes. Des serveurs proxy de fédération peuvent être déployés à la fois dans les organisations du fournisseur de revendications et de la partie de confiance. Du côté du fournisseur de revendications, le proxy collecte les informations d'authentification depuis les ordinateurs clients et les transmet au serveur de fédération du fournisseur de revendications pour être traitées. Le serveur de fédération délivre un jeton de sécurité au proxy, qui l'envoie au proxy de la partie de confiance. Le serveur proxy de fédération de la partie de confiance accepte ces jetons, puis les transmet au serveur de fédération interne. Le serveur de fédération de la partie de confiance délivre ensuite un jeton de sécurité pour l'application Web, puis l'envoie au serveur proxy de fédération qui le transfère à son tour au client. Le serveur proxy de fédération ne fournit pas de jeton, ni ne crée de revendication ; il transfère uniquement les demandes des clients aux serveurs AD FS internes. Toutes les communications entre le serveur proxy de fédération et le serveur de fédération utilise HTTPS.

 **Remarque :** Un serveur proxy de fédération ne peut pas être configuré en tant que fournisseur de revendications ou partie de confiance. Le fournisseur de revendications et la partie de confiance doivent être membres d'un domaine AD DS. Le serveur proxy de fédération peut être configuré en tant que membre d'un groupe de travail ou d'une forêt extranet, puis déployé dans un réseau de périmètre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Installation du rôle serveur AD FS

Au cours de cette démonstration, vous allez découvrir comme installer et effectuer la configuration initiale du rôle serveur AD FS dans Windows Server 2012. L'instructeur installera le rôle serveur, puis exécutera l'Assistant Configuration du serveur de fédération AD FS pour configurer le serveur en tant que serveur de fédération autonome.

Remarque : Les serveurs de fédération autonomes doivent être déployés uniquement dans les petits environnements ou les environnements tests. Le déploiement d'un serveur autonome ne vous permet pas d'ajouter un autre serveur ultérieurement pour permettre l'évolutivité et la redondance. Dans la plupart des environnements de production, vous devez déployer une batterie de serveurs, même si la batterie ne contient qu'un seul nœud.

Procédure de démonstration

Installer le rôle serveur AD FS

- Sur LON-DC1, dans le Gestionnaire de serveur, ajoutez le rôle serveur AD FS (**Active Directory Federation Services**).

Configurer le rôle serveur AD FS

1. Exécutez l'Assistant Configuration du serveur de fédération AD FS à l'aide des paramètres suivants :
    - créer un service de fédération ;
    - créer un déploiement autonome ;
    - utiliser le certificat **LON-DC1.Adatum** ;
    - choisir le nom de service **LON-DC1.Adatum.com**.
2. Ouvrez Windows® Internet Explorer® et connectez-vous à **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.

Leçon 3
Implémentation d'AD FS pour une seule organisation

Le scénario de déploiement le plus simple pour AD FS se situe au sein d'une seule organisation. Dans ce scénario, un seul serveur AD FS peut fonctionner à la fois comme fournisseur de revendications et comme partie de confiance. Tous les utilisateurs de ce scénario sont internes à l'organisation, tout comme l'application à laquelle les utilisateurs accèdent.

Cette leçon fournit des informations détaillées sur les composants requis pour configurer AD FS dans un seul déploiement d'organisation. Ces composants incluent la configuration des revendications, des règles de revendication, des approbations de fournisseur de revendications et des approbations de partie de confiance.

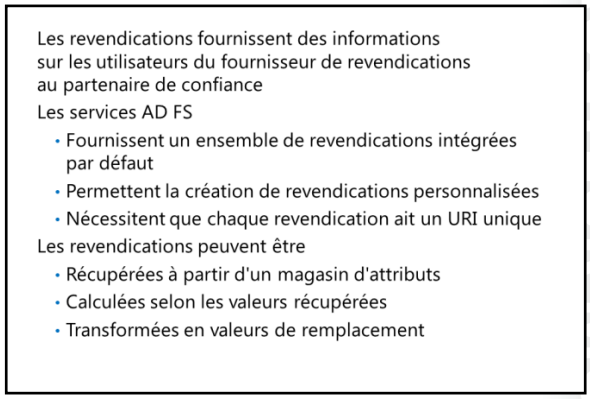
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les revendications AD FS ;
- décrire les règles de revendication AD FS ;
- décrire les approbations de fournisseur de revendications ;
- décrire les approbations de partie de confiance ;
- configurer les approbations de fournisseur de revendications et de partie de confiance.

Que sont les revendications AD FS ?

Les revendications AD FS fournissent le lien entre les rôles de fournisseur de revendications et de partie de confiance dans un déploiement AD FS. Une *revendication AD FS* est une déclaration faite à propos d'un sujet particulier (tel qu'un utilisateur) par une entité approuvée (telle qu'un fournisseur de revendications). Le fournisseur de revendications crée les revendications et la partie de confiance les consomme. Les revendications AD FS fournissent une méthode normalisée et flexible aux organisations du fournisseur de revendications pour apporter des informations spécifiques sur les utilisateurs de leurs organisations. Elles fournissent également une méthode aux parties de confiance pour définir exactement les informations dont elles ont besoin pour autoriser l'accès à l'application. Les informations de revendication fournissent les détails requis par les applications pour permettre l'accès aux applications prenant en charge les revendications.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Types de revendications

Chaque revendication AD FS a un type de revendication, tel que l'adresse de messagerie, le nom d'utilisateur principal (UPN) ou le nom. Des revendications peuvent être émises pour les utilisateurs selon le type de revendication défini. Par conséquent, une revendication avec un type Nom et, par exemple, une valeur Weber peut être émise pour un utilisateur. AD FS fournit plusieurs types de revendications intégrés. Éventuellement, vous pouvez en créer de nouveaux selon les besoins de l'organisation.

 **Remarque :** Dans AD FS 1.0, vous pouvez configurer des revendications en tant que revendications d'identité, revendications de groupe ou revendications personnalisées. Ces types de revendications ne s'appliquent pas à AD FS 2.0 ou à une version plus récente. Globalement, toutes les revendications sont désormais considérées comme des revendications personnalisées.

Chaque type de revendication AD FS est identifié par un URI (Uniform Resource Identifier) qui identifie de manière unique le type de revendication. Ces informations sont fournies dans les métadonnées de serveur AD FS. Par exemple, si l'organisation du fournisseur de revendications et celle de la partie de confiance décident d'utiliser un type de revendication AccountNumber, les deux organisations doivent configurer un type de revendication avec ce nom. Le type de revendication est publié et l'URI du type de revendication doit être identique sur les deux serveurs AD FS.

Méthode de remplissage des valeurs de revendication

Les revendications émises par un fournisseur de revendications contiennent les informations requises par la partie de confiance pour autoriser l'accès à l'application approprié. Une des premières étapes de la planification du déploiement d'AD FS consiste à définir exactement les informations sur chaque utilisateur indispensables aux applications pour autoriser l'accès de cet utilisateur à l'application. Une fois ces informations définies, les revendications sont ensuite définies sur le serveur de fédération du fournisseur de revendications. Les informations requises pour remplir la revendication peuvent être obtenues de plusieurs façons :

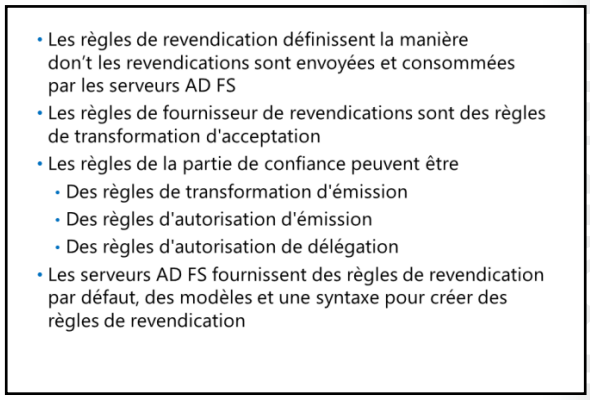
- La revendication peut être récupérée à partir d'un magasin d'attributs. Souvent, les informations requises pour la revendication sont déjà enregistrées dans un magasin d'attributs qui est disponible pour le serveur de fédération. Par exemple, une organisation peut décider que la revendication doit inclure le nom d'utilisateur principal (UPN), l'adresse de messagerie et les appartenances aux groupes spécifiques. Ces informations sont déjà enregistrées dans AD DS, le serveur de fédération peut alors juste récupérer ces informations à partir d'AD DS lors de la création de la revendication. Puisqu'AD FS peut utiliser AD DS, AD LDS, SQL Server, un répertoire LDAP (Lightweight Directory Access Protocol) non Microsoft ou un magasin d'attributs personnalisé pour remplir les revendications, vous pouvez définir pratiquement toute valeur au sein de la revendication.
- La revendication peut être calculée selon les informations collectées. Les serveurs de fédération du fournisseur de revendications peuvent également calculer les informations selon les informations recueillies à partir d'un magasin d'attributs. Par exemple, il est possible de fournir des informations sur le salaire d'une personne dans une revendication. Ces informations sont probablement enregistrées dans une base de données des ressources humaines, mais la valeur réelle peut être considérée comme confidentielle. Vous pouvez définir une revendication qui classe les salaires par catégorie dans une organisation, puis laisser le serveur AD FS calculer la catégorie à laquelle un utilisateur spécifique appartient. De cette façon, la revendication comprend uniquement les informations sur la catégorie de salaire, et non le salaire réel de l'utilisateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- La revendication peut être transformée d'une valeur à une autre. Dans certains cas, les informations enregistrées dans un magasin d'attributs ne correspondent pas exactement aux informations requises par l'application lors de la réalisation des informations d'autorisation. Par exemple, l'application peut avoir différents rôles d'utilisateur définis qui ne correspondent pas directement aux attributs enregistrés les magasins d'attributs. Cependant, le rôle d'application peut être mis en corrélation avec l'appartenance au groupe AD DS. Par exemple, les utilisateurs du groupe Ventes peuvent être mis en corrélation avec un rôle d'application, tandis que les utilisateurs du groupe Gestion des ventes peuvent être mis en corrélation avec un rôle d'application différent. Pour établir la corrélation dans AD FS, vous pouvez configurer une transformation de revendications qui prend la valeur fournie par le fournisseur de revendications et traduit la valeur en une revendication utile pour l'application dans la partie de confiance.
- Si vous avez déployé un contrôle d'accès dynamique, une revendication de périphérique de contrôle d'accès dynamique peut être transformée en une revendication AD FS. Celle-ci peut être utilisée pour permettre aux utilisateurs d'accéder à des sites Web AD FS uniquement à partir des stations de travail approuvées qui ont émis une revendication de périphérique valide.

Que sont les règles de revendication AD FS ?

Les règles de revendication définissent la manière dont les revendications sont envoyées et consommées par les serveurs AD FS. Elles définissent la logique métier qui est appliquée aux revendications fournies par des fournisseurs de revendications et celles acceptées par les parties de confiance. Vous pouvez utiliser les règles de revendication pour :



- définir les revendications entrantes acceptées d'un ou plusieurs fournisseurs de revendications ;
- définir les revendications sortantes fournies à une ou plusieurs parties de confiance ;
- appliquer les règles d'autorisation pour permettre l'accès à une partie de confiance spécifique pour un ou plusieurs utilisateurs ou groupes d'utilisateurs.

Vous pouvez configurer deux types de règles de revendication :

- Règles de revendication pour l'approbation d'un fournisseur de revendications. Une approbation de fournisseur de revendications est la relation d'approbation AD FS qui est configurée entre un serveur AD FS et un fournisseur de revendications. Vous pouvez configurer les règles de revendication pour définir la manière dont le fournisseur de revendications traite et émet les revendications.
- Règles de revendication pour l'approbation d'une partie de confiance. Une approbation de partie de confiance est la relation d'approbation AD FS qui est configurée entre un serveur AD FS et une partie de confiance. Vous pouvez configurer les règles de revendication qui définissent la façon dont la partie de confiance accepte les revendications du fournisseur de revendications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les règles de revendication sur un fournisseur de revendications AD FS sont toutes considérées comme des règles de transformation d'acceptation. Ces règles déterminent les types de revendications qui sont acceptés par le fournisseur de revendications, puis envoyés à une approbation de partie de confiance. Lors de la configuration d'AD FS dans une seule organisation, une approbation de fournisseur de revendications par défaut est configurée avec le domaine AD DS local. Cet ensemble de règles définit les revendications qui sont acceptées à partir d'AD DS.

Il existe trois types de règles de revendication pour une approbation de partie de confiance :

- Règles de transformation d'émission. Ces règles définissent les revendications qui sont envoyées à la partie de confiance définie dans l'approbation de partie de confiance.
- Règles d'autorisation d'émission. Ces règles définissent les utilisateurs qui ont le droit d'accès ou non à la partie de confiance définie dans l'approbation de partie de confiance. Cet ensemble de règles peut comprendre les règles qui donnent explicitement accès à une partie de confiance, et/ou les règles qui refusent explicitement l'accès à une partie de confiance.
- Règles d'autorisation de délégation. Ces règles définissent les revendications qui spécifient les utilisateurs qui peuvent agir pour le compte d'autres utilisateurs lors de l'accès à la partie de confiance. Cet ensemble de règles peut comprendre les règles qui autorisent explicitement les délégués à une partie de confiance ou les règles qui refusent explicitement les délégués à une partie de confiance.

Remarque : Une seule règle de revendication peut être associée à une seule relation d'approbation fédérée. Autrement dit, il est impossible de créer un ensemble de règles pour une approbation, puis de réutiliser ces règles pour d'autres approbations que vous configurez sur votre serveur de fédération.

Les serveurs AD FS sont préconfigurés avec un ensemble de règles par défaut et plusieurs modèles par défaut que vous pouvez utiliser pour créer les règles de revendication les plus courantes. Vous pouvez également créer des règles de revendication personnalisées en utilisant le langage des règles de revendication AD FS.

Qu'est-ce qu'une approbation de fournisseur de revendications ?

Une approbation de fournisseur de revendications est configurée sur le serveur de fédération de la partie de confiance. L'approbation de fournisseur de revendications identifie le fournisseur de revendications et décrit la façon dont la partie de confiance consomme les revendications émises par le fournisseur de revendications. Vous devez configurer une approbation de fournisseur de revendications pour chaque fournisseur de revendications.

- Les approbations de fournisseur de revendications
  - Sont configurées sur le serveur de fédération de la partie de confiance
  - Identifient le fournisseur de revendications
  - Configurent les règles de revendication pour le fournisseur de revendications
- Dans un scénario d'organisation simple, une approbation de fournisseur de revendications nommée Active Directory définit comment les informations d'identification de l'utilisateur AD DS sont traitées
- Des approbations de fournisseur de revendications supplémentaires peuvent être configurées
  - En important les métadonnées de fédération
  - En important un fichier de configuration
  - En configurant l'approbation manuellement

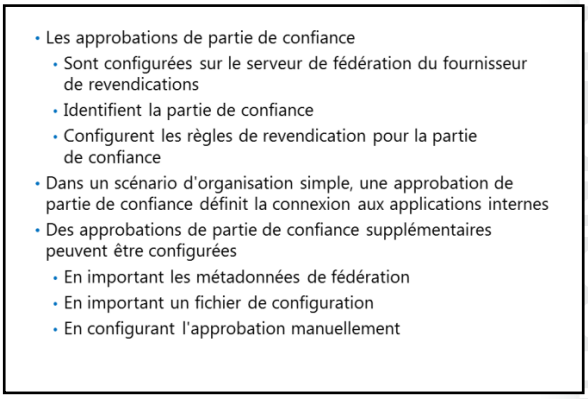
Par défaut, un serveur AD FS est configuré avec une approbation de fournisseur de revendications nommée Active Directory. Cette approbation définit les règles de revendication, qui sont toutes des règles de transformation d'acceptation qui définissent comment le serveur AD FS accepte les informations d'identification AD DS. Par exemple, les règles de revendication par défaut sur l'approbation de fournisseur de revendications comprennent les règles qui transmettent les noms d'utilisateur, les identificateurs de sécurité (SID) et les SID de groupe à la partie de confiance. Dans un déploiement d'AD FS au sein d'une seule organisation dans lequel AD DS authentifie tous les utilisateurs, l'approbation de fournisseur de revendications par défaut peut être l'unique approbation de fournisseur de revendications requise.

Lorsque vous développez le déploiement d'AD FS pour inclure d'autres organisations, vous devez créer des approbations de fournisseur de revendications supplémentaires pour chaque organisation fédérée de fournisseur d'identité. Lors de la configuration d'une approbation de fournisseur de revendications, trois options s'offrent à vous :

- Importer les données relatives au fournisseur de revendications via les métadonnées de fédération. Si le serveur de fédération AD FS ou le serveur proxy de fédération est accessible via le réseau à partir de votre serveur de fédération AD FS, vous pouvez entrer le nom d'hôte ou l'URL du serveur de fédération partenaire. Votre serveur de fédération AD FS se connecte au serveur partenaire, puis télécharge les métadonnées de fédération à partir du serveur. Les métadonnées de fédération comprennent toutes les informations requises pour configurer l'approbation de fournisseur de revendications. Dans le cadre du téléchargement des métadonnées de fédération, votre serveur de fédération télécharge également le certificat SSL utilisé par le serveur de fédération partenaire.
- Importer les données relatives au fournisseur de revendications à partir d'un fichier. Utilisez cette option si le serveur de fédération partenaire n'est pas directement accessible à partir de votre serveur de fédération, mais que l'organisation partenaire a exporté sa configuration et vous a fourni les informations dans un fichier. Le fichier de configuration doit inclure les informations de configuration de l'organisation partenaire et le certificat SSL utilisé par le serveur de fédération partenaire.
- Configurer manuellement l'approbation de fournisseur de revendications. Utilisez cette option si vous souhaitez configurer directement tous les paramètres de l'approbation de fournisseur de revendications. Lorsque vous sélectionnez cette option, vous devez fournir les fonctionnalités que le fournisseur de revendications prend en charge et l'URL utilisée pour accéder aux serveurs AD FS du fournisseur de revendications, puis ajouter le certificat SSL utilisé par l'organisation partenaire.

Qu'est-ce qu'une approbation de partie de confiance ?

Une approbation de partie de confiance est définie sur le serveur de fédération de fournisseur de revendications. L'approbation de partie de confiance identifie la partie de confiance et définit également les règles de revendication qui définissent la façon dont la partie de confiance accepte et traite les revendications du fournisseur de revendications.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans un seul scénario d'organisation, l'approbation de partie de confiance définit comment le serveur AD FS interagit avec les applications déployées dans l'application. Lorsque vous configurez l'approbation de partie de confiance dans une seule organisation, vous fournissez l'URL de l'application interne et configurez les paramètres, par exemple si l'application prend en charge SAML 2.0 ou si elle requiert les jetons AD FS 1.0, l'URL utilisée par le serveur Web et les règles d'autorisation d'émission de l'application.

Le processus de configuration de l'approbation de la partie de confiance est semblable à celui de l'approbation de fournisseur de revendications. Lorsque vous développez le déploiement d'AD FS pour inclure d'autres organisations, vous devez créer des approbations de partie de confiance supplémentaires pour chaque organisation fédérée. Lors de la configuration d'une approbation de partie de confiance, trois options s'offrent à vous :

- Importer les données relatives à la partie de confiance via les métadonnées de fédération. Si le serveur de fédération AD FS ou le serveur proxy de fédération est accessible via le réseau à partir de votre serveur de fédération AD FS, vous pouvez entrer le nom d'hôte ou l'URL du serveur de fédération partenaire. Votre serveur de fédération AD FS se connecte au serveur partenaire, puis télécharge les métadonnées de fédération à partir du serveur. Les métadonnées de fédération comprennent toutes les informations requises pour configurer l'approbation de partie de confiance. Dans le cadre du téléchargement des métadonnées de fédération, votre serveur de fédération télécharge également le certificat SSL utilisé par le serveur de fédération partenaire.
- Importer les données relatives à la partie de confiance à partir d'un fichier. Utilisez cette option si le serveur de fédération partenaire n'est pas accessible directement à partir de votre serveur de fédération. Dans ce cas, l'organisation partenaire peut exporter ses informations de configuration vers un fichier, qu'elle vous fait suivre. Le fichier de configuration doit inclure les informations de configuration de l'organisation partenaire et le certificat SSL utilisé par le serveur de fédération partenaire.

Configurer manuellement l'approbation de fournisseur de revendications. Utilisez cette option si vous souhaitez configurer directement tous les paramètres de l'approbation de fournisseur de revendications.

Démonstration : Configuration des approbations de fournisseur de revendications et de partie de confiance

Dans cette démonstration, vous allez apprendre à configurer les approbations de fournisseur de revendications et de partie de confiance. L'instructeur montrera comment modifier l'approbation de fournisseur de revendications Active Directory par défaut. Il créera également une approbation de partie de confiance et montrera comment configurer l'approbation.

Procédure de démonstration

Configurer une approbation de fournisseur de revendications

1. Dans la console AD FS, ouvrez **Approbations de fournisseur de revendications**, mettez en surbrillance le magasin **Active Directory**, puis cliquez sur **Modifier les règles de revendication**.
2. Dans la boîte de dialogue **Modifier les règles de revendication pour Active Directory**, sur l'onglet **Règles de transformation d'acceptation**, démarrez l'Assistant **Ajouter une règle de revendication de transformation**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Exécutez l'Assistant Ajouter une règle de revendication de transformation avec les paramètres suivants :
   - Sous Modèle de règle de revendication, cliquez sur **Envoyer les attributs LDAP en tant que revendications**.
   - Nommez la règle de revendication **Règle d'attributs LDAP sortants**.
   - Choisissez Active Directory en tant que magasin d'attributs.
   - Dans **Mappage des attributs LDAP aux types de revendications sortantes**, sélectionnez les valeurs suivantes :
     - Adresses de messagerie = **Adresse de messagerie**
     - Nom d'utilisateur principal = **UPN**

Configurer une application Windows Identity Foundation pour AD FS

1. Sur LON-SVR1, à partir de l'écran d'accueil, démarrez l'**Utilitaire de fédération Windows Identity Foundation**.
2. Exécutez l'Assistant Utilitaire de fédération avec les paramètres suivants :
   - Pointez sur l'exemple d'application du fichier web.config en accédant à **C:\Inetpub\wwwroot\AdatumTestApp\web.config**.
   - Spécifiez une zone **URI d'application** en saisissant **https://lon-svr1.adatum.com/AdatumTestApp/.**
   - Sélectionnez l'option **Utiliser un STS existant**, puis saisissez le chemin d'accès **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.
   - Désactivez la validation de la chaîne de certificats.
   - Sélectionnez l'option **Aucun chiffrement**.

Configurer une approbation de partie de confiance

1. Dans la console AD FS, dans le volet central, cliquez sur **Requis : Ajouter une approbation de partie de confiance**.
2. Exécutez l'Assistant Ajouter une approbation de partie de confiance avec les paramètres suivants :
   - Sélectionnez l'option **Importer les données relatives à la partie de confiance publiée en ligne ou sur un réseau local** et saisissez **https://lon-svr1.adatum.com/adatumtestapp**.
   - Spécifiez le Nom complet **ADatum Test App**.
   - Sélectionnez l'option **Autoriser tous les utilisateurs à accéder à cette partie de confiance**.
   - Vérifiez que la case à cocher **Modifier les règles de revendication pour ADatum Test App** est activée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Déploiement d'AD FS dans un scénario de fédération B2B

Un deuxième scénario classique d'implémentation d'AD FS se trouve dans un scénario de fédération B2B. Dans ce scénario, les utilisateurs d'une organisation ont besoin d'accéder à une application d'une autre organisation. Dans ce scénario, AD FS active l'authentification unique (SSO). De cette façon, les utilisateurs se connectent toujours dans leur environnement AD DS personnel, mais se voient accorder l'accès à l'application partenaire selon les revendications acquises à partir de leur serveur AD FS local.

La configuration d'AD FS d'un scénario de fédération B2B est assez semblable à la configuration d'AD FS d'un seul scénario d'organisation. La principale différence réside dans le fait que les approbations de partie de confiance et les approbations de fournisseur de revendications font désormais référence aux organisations externes plutôt qu'à l'AD DS ou l'application internes.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- configurer le partenaire de compte dans un scénario de fédération B2B ;
- configurer le partenaire de ressource dans un scénario de fédération B2B ;
- expliquer comment configurer les règles de revendication pour un scénario de fédération B2B ;
- expliquer le fonctionnement de la découverte du domaine d'accueil ;
- configurer les règles de revendication.

Configuration d'un partenaire de compte

Dans un scénario AD FS B2B, la terminologie que vous utilisez pour décrire les deux partenaires concernés par le déploiement d'AD FS varie légèrement. Dans ce scénario, l'organisation du fournisseur de revendications est également appelée organisation partenaire de compte. Une *organisation partenaire de compte* est l'organisation dans laquelle les comptes d'utilisateurs sont enregistrés dans un magasin d'attributs. Un partenaire de compte gère les tâches suivantes :

Un partenaire de compte est un fournisseur de revendications dans un scénario de fédération B2B

Pour configurer un partenaire de compte

1. Implémenter la topologie physique
2. Ajouter un magasin d'attributs
3. Configurer une approbation de partie de confiance
4. Ajouter une description de revendication
5. Préparer les ordinateurs clients pour la fédération

- recueillir les informations d'identification des utilisateurs qui utilisent un service Web, puis authentifier ces informations d'identification ;
- accumuler les revendications pour les utilisateurs, puis les empaqueter dans des jetons de sécurité. Les jetons peuvent ensuite être présentés par le biais d'une approbation de fédération pour accéder aux ressources de fédération situées dans l'organisation partenaire de ressource.

Configuration de l'organisation partenaire de compte

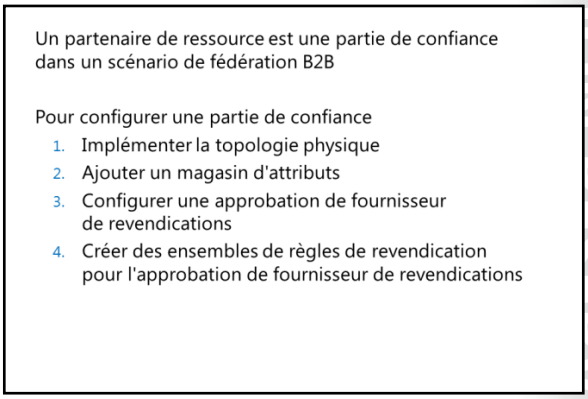
La configuration de l'organisation partenaire de compte pour se préparer à la fédération implique les étapes suivantes :

1. Implémenter la topologie physique pour le déploiement de partenaire de compte. Cette étape peut inclure le choix du nombre de serveurs de fédération et de proxys du service de fédération à déployer, ainsi que la configuration des enregistrements et des certificats DNS requis.
2. Ajouter un magasin d'attributs. Utilisez la console AD FS pour ajouter le magasin d'attributs. Dans la plupart des cas, vous utilisez le magasin d'attributs Active Directory par défaut (qui doit être utilisé pour authentification), mais vous pouvez également ajouter d'autres magasins d'attributs pour établir les revendications d'utilisateur si nécessaire.
3. Se connecter à une organisation partenaire de ressource en créant une approbation de partie de confiance. La meilleure façon de procéder consiste à utiliser l'URL de métadonnées de fédération qui est fournie par l'organisation partenaire de ressource. Avec cette option, votre serveur AD FS collecte automatiquement les informations requises pour l'approbation de partie de confiance.
4. Ajouter une description de revendication. La description de revendication répertorie les revendications que votre organisation fournit au partenaire de confiance. Ces informations peuvent comprendre les noms d'utilisateur, les adresses de messagerie, les informations d'appartenance à un groupe ou toute autre information d'identification d'un utilisateur.
5. Préparer les ordinateurs clients pour la fédération. Cette opération peut se faire en deux étapes :
    a. Ajouter le serveur de fédération du partenaire de compte. Dans le navigateur des ordinateurs clients, ajoutez le serveur de fédération du partenaire de compte à la liste Intranet locale. En ajoutant le serveur de fédération du partenaire de compte à la liste Intranet locale sur les ordinateurs clients, vous activez l'authentification Windows intégrée ; autrement dit, les utilisateurs ne sont pas invités à s'authentifier s'ils sont déjà connectés au domaine. Vous pouvez utiliser les objets de stratégie de groupe (GPO) pour attribuer l'URL à la liste locale du site Intranet.
    b. Configurer les approbations de certificat. Il s'agit d'une étape facultative nécessaire uniquement si un ou plusieurs serveurs auxquels les clients accèdent ne disposent pas de certificats approuvés. L'ordinateur client devra probablement se connecter aux serveurs de fédération de compte, aux serveurs de fédération de ressource ou aux serveurs proxy de fédération, ainsi qu'aux serveurs Web de destination. Si aucun de ces certificats ne provient d'une autorité de certification publique de confiance, vous devrez probablement ajouter le certificat approprié ou le certificat racine au magasin de certificats sur les clients. Pour ce faire, vous pouvez utiliser les objets de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration d'un partenaire de ressource

L'organisation partenaire de ressource est la partie de confiance dans un scénario de fédération B2B. L'organisation partenaire de ressource se trouve à l'endroit où les ressources existent et où elles sont accessibles aux organisations partenaires de compte. Le partenaire de ressource gère les tâches suivantes :



- accepter les jetons de sécurité que le serveur de fédération du partenaire de compte produit et valide ;
- consommer les revendications à partir des jetons de sécurité, puis fournir les nouvelles revendications à ses serveurs Web après avoir pris une décision d'autorisation.

Les serveurs Web doivent être dotés de Windows Identity Foundation ou des services de rôle de l'agent Web AD FS 1.x prenant en charge les revendications pour externaliser la logique d'identité et accepter les revendications.

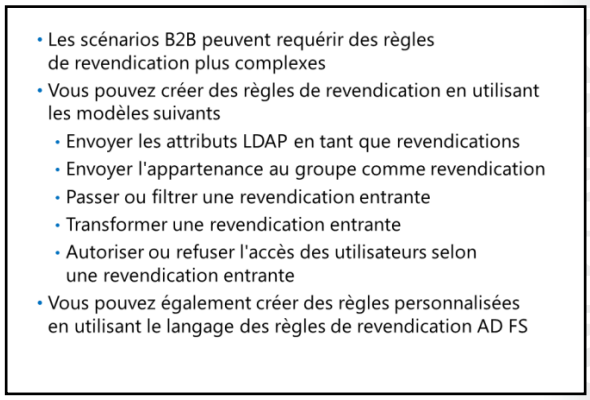
Remarque : Windows Identity Foundation fournit un ensemble d'outils de développement cohérents qui permettent aux développeurs d'intégrer dans leurs applications l'authentification et l'autorisation basées sur les revendications. Windows Identity Foundation comprend également un Kit de développement logiciel (SDK) et des exemples d'applications. Vous utilisez un exemple d'application Windows Identity Foundation dans l'atelier pratique de ce module.

La configuration de l'organisation partenaire de ressource est semblable à la configuration de l'organisation partenaire de compte et comprend les étapes suivantes :

1. Implémenter la topologie physique pour le déploiement du partenaire de ressource. Les étapes de planification et d'implémentation sont les mêmes que celles du partenaire de compte, avec l'ajout de la planification de l'emplacement et de la configuration du serveur Web.
2. Ajouter un magasin d'attributs. Sur le partenaire de ressource, le magasin d'attributs est utilisé pour remplir les revendications qui sont offertes au client pour être présentées sur le serveur Web.
3. Se connecter à une organisation partenaire de compte en créant une approbation de fournisseur de revendications.
4. Créer des ensembles de règles de revendication pour l'approbation de fournisseur de revendications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des règles de revendication pour les scénarios B2B



Dans un seul déploiement d'organisation d'AD FS, il peut être assez simple de concevoir et d'implémenter les règles de revendication. Dans de nombreux cas, vous devrez peut-être fournir uniquement le nom d'utilisateur ou le nom de groupe qui est recueilli à partir de la revendication et présenté au serveur Web. Dans un scénario B2B, vous devrez probablement configurer des règles de revendication plus compliquées pour définir l'accès de l'utilisateur entre des systèmes très différents.

Les règles de revendication définissent la façon dont les partenaires de compte (fournisseurs de revendications) créent les revendications et la façon dont les partenaires de ressource (parties de confiance) consomment les revendications. AD FS fournit plusieurs modèles que vous pouvez utiliser lors de la configuration des règles de revendication :

- Modèle de règle Envoyer les attributs LDAP en tant que revendications**.** Utilisez ce modèle quand vous sélectionnez des attributs spécifiques dans un magasin d'attributs LDAP pour remplir les revendications. Vous pouvez configurer plusieurs attributs LDAP en tant que revendications individuelles dans une seule règle de revendication que vous créez à partir de ce modèle. Par exemple, vous pouvez créer une règle qui extrait les attributs AD DS **sn** (nom de famille) et **givenName** à partir de tous les utilisateurs authentifiés, puis envoyer ces valeurs comme revendications sortantes à envoyer à une partie de confiance.
- Modèle de règle Envoyer l'appartenance à un groupe en tant que revendication**.** Utilisez ce modèle pour envoyer un type de revendication particulier et une valeur de revendication associée qui est basée sur l'appartenance au groupe de sécurité AD DS. Par exemple, vous pouvez utiliser ce modèle pour créer une règle qui envoie un type de revendication de groupe avec la valeur SalesAdmin, si l'utilisateur est un membre du groupe de sécurité de responsables des ventes dans son domaine AD DS. Cette règle n'émet qu'une seule revendication basée sur le groupe AD DS que vous sélectionnez comme faisant partie du modèle.
- Modèle de règle Passer ou filtrer une revendication entrante. Utilisez ce modèle pour définir les restrictions supplémentaires relatives aux revendications qui sont soumises aux parties de confiance. Par exemple, vous pouvez utiliser une adresse de messagerie d'utilisateur en tant que revendication, mais n'envoyer que l'adresse de messagerie si le suffixe de domaine sur l'adresse de messagerie est adatum.com. Lorsque vous utilisez ce modèle, vous pouvez passer toute revendication extraite à partir du magasin d'attributs ou configurer les règles qui filtrent si la revendication est transmise selon différents critères.

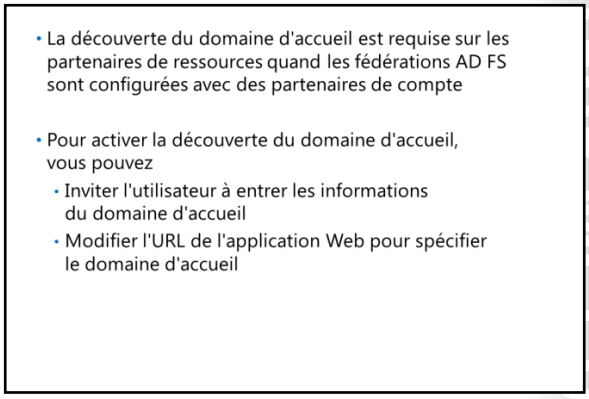
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Modèle de règle Transformer une revendication entrante. Utilisez ce modèle pour mapper la valeur d'un attribut du magasin d'attributs du fournisseur de revendications à une valeur différente du magasin d'attributs de partie de confiance. Par exemple, il est possible de fournir à tous les membres du département Marketing de la société A. Datum un accès limité à une application d'achat au sein de Trey Research. Chez Trey Research, l'attribut utilisé pour définir le niveau d'accès limité peut être défini par **LimitedPurchaser**. Pour aborder ce scénario, vous pouvez configurer une règle de revendication qui transforme une revendication sortante, dans laquelle la valeur Département est Marketing, en une revendication entrante dans laquelle l'attribut **ApplicationAccess** est **LimitedPurchaser**. Les règles créées à partir de ce modèle doivent avoir une relation un-à-un entre la revendication au fournisseur de revendications et la revendication au partenaire de confiance.
- Modèle de règle Autoriser ou refuser l'accès des utilisateurs selon une revendication entrante. Ce modèle est disponible uniquement lorsque vous configurez des règles d'autorisation d'émission ou des règles d'autorisation de délégation sur une approbation de partie de confiance. Utilisez ce modèle pour créer les règles qui autorisent ou refusent l'accès aux utilisateurs à une partie de confiance, selon le type et la valeur d'une revendication entrante. Ce modèle de règle de revendication vous permet d'exécuter un contrôle d'autorisation sur le fournisseur de revendications avant l'envoi des revendications à une partie de confiance. Par exemple, vous pouvez utiliser ce modèle de règle pour créer une règle qui autorise uniquement les utilisateurs du groupe Ventes à accéder à une partie de confiance, puisque que les demandes d'authentification des membres des autres groupes ne sont pas envoyées à la partie de confiance.

Si aucun des modèles de règles de revendication intégrés n'offre la fonctionnalité dont vous avez besoin, vous pouvez créer des règles plus complexes à l'aide du langage des règles de revendication AD FS. En créant une règle personnalisée, vous pouvez extraire les informations sur les revendications à partir de plusieurs magasins d'attributs et associer également les types de revendications à une seule règle de revendication.

Fonctionnement de la découverte du domaine d'accueil

Certaines organisations partenaires de ressource qui hébergent des applications prenant en charge les revendications peuvent autoriser l'accès à leurs applications à plusieurs partenaires de compte. Dans ce scénario, lorsque les utilisateurs se connectent à l'application Web, un mécanisme doit diriger les utilisateurs vers le serveur de fédération AD FS de leur domaine d'accueil, plutôt que vers le serveur de fédération d'une autre organisation. Le processus pour diriger les clients vers le partenaire de compte approprié est appelé *découverte du domaine d'accueil*.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La découverte du domaine d'accueil se produit après la connexion du client au site Web de la partie de confiance et la redirection du client vers le serveur de fédération de la partie de confiance. À ce stade, le serveur de fédération de la partie de confiance doit rediriger le client vers le serveur de fédération du domaine d'accueil du client pour que l'utilisateur puisse être authentifié. Si plusieurs fournisseurs de revendications ont été configurés sur le serveur de fédération de la partie de confiance, il est indispensable de savoir vers quel serveur de fédération rediriger le client.

Globalement, il existe trois façons d'implémenter la découverte du domaine d'accueil :

1. Demander aux utilisateurs de sélectionner leur domaine d'accueil. Avec cette option, lorsque l'utilisateur est redirigé vers le serveur de fédération de la partie de confiance, le serveur de fédération peut afficher une page Web demandant à l'utilisateur d'identifier la société pour laquelle il travaille. Une fois que l'utilisateur sélectionne la société appropriée, le serveur de fédération peut utiliser ces informations pour rediriger l'ordinateur client vers le serveur de fédération d'accueil approprié pour l'authentification.
2. Modifier le lien de l'application Web pour inclure une chaîne WHR qui spécifie le domaine d'accueil de l'utilisateur. Le serveur de fédération de la partie de confiance utilise cette chaîne pour rediriger l'utilisateur automatiquement vers le domaine d'accueil approprié. Autrement dit, l'utilisateur ne doit pas être invité à sélectionner le domaine d'accueil, car la chaîne WHR de l'URL sur laquelle l'utilisateur clique transmet les informations nécessaires vers le serveur de fédération de la partie de confiance. Le lien modifié ressemble probablement au lien suivant : https://www.adatum.com/OrderApp/?whr=urn:federation:TreyResearch.

 **Remarque :** Le profil SAML appelé authentification unique (SSO) initiée par le fournisseur d'identité représente l'une des options disponibles pour la découverte du domaine d'accueil avec des applications compatibles avec SAML 2.0. Ce profil SAML configure les utilisateurs pour qu'ils puissent accéder en premier à leur fournisseur de revendications local, qui peut préparer le jeton de l'utilisateur avec les revendications requises pour accéder à l'application Web du partenaire. La version des services AD FS pour Windows Server 2012 n'implémente pas complètement le profil d'authentification unique (SSO) initiée par le fournisseur d'identité, mais fournit certaines des ces fonctionnalités en implémentant une fonctionnalité nommée RelayState.

 **Documentation supplémentaire :** Pour en savoir plus sur RelayState, reportez-vous au site Web Supporting Identity Provider Initiated RelayState (en anglais) à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=270036.

 **Remarque :** Le processus de découverte du domaine d'accueil se produit la première fois que l'utilisateur tente d'accéder à une application Web. Une fois que l'utilisateur s'est authentifié avec succès, un cookie de découverte du domaine d'accueil est délivré au client pour que l'utilisateur n'ait pas à suivre l'ensemble du processus la prochaine fois. Ce cookie de découverte du domaine d'accueil expire après un mois, sauf si le cache de cookie est supprimé avant l'expiration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration des règles de revendication

Dans cette démonstration, vous apprendrez à configurer les règles de revendication sur une approbation de partie de confiance qui transfère un nom de groupe en tant que partie de la revendication. Vous découvrirez également comment configurer une règle de revendications qui limite l'accès à l'application uniquement aux membres d'un groupe particulier.

Procédure de démonstration

Configurer les règles de revendication

1. Sur LON-DC1, modifiez l'approbation de partie de confiance **ADatum Test App** en créant une nouvelle règle de transformation d'émission qui passe ou filtre une revendication entrante.
   - Nommez la règle **Envoyer la règle du nom de groupe**.
   - Configurez la règle pour utiliser un type de revendication entrante de groupe.
2. Supprimez la **règle d'autorisation d'émission** qui accorde l'accès à tous les utilisateurs.
3. Créez une règle d'autorisation d'émission qui autorise ou refuse l'accès aux utilisateurs selon la revendication entrante. Configurez cette règle avec les paramètres suivants :
   - Nom : **Autoriser la règle du groupe Production** ;
   - Type de revendication entrante : **Groupe**
   - Valeur de revendication entrante : **Production**
   - **Autoriser l'accès aux utilisateurs avec cette revendication entrante**.
4. Créez une règle d'autorisation d'émission qui autorise ou refuse l'accès aux utilisateurs selon la revendication entrante. Configurez cette règle avec les paramètres suivants, puis cliquez sur **Terminer** :
   - Nom : **Autoriser les utilisateurs A. Datum** ;
   - Type de revendication entrante : **UPN** ;
   - Valeur de revendication entrante : **@adatum.com** ;
   - **Autoriser l'accès aux utilisateurs avec cette revendication entrante**.
5. Ouvrez les propriétés de la règle **Autoriser les utilisateurs A. Datum** et examinez le langage des règles de revendications.

Atelier pratique : Implémentation des services AD FS (Active Directory Federation Services)

Scénario

La société A. Datum a mis en place un grand choix de relations commerciales avec d'autres sociétés et clients. Certaines de ces sociétés partenaires et de ces clients doivent accéder aux applications métier qui s'exécutent sur le réseau A. Datum. Les groupes d'entreprise chez A. Datum souhaitent fournir un niveau maximal de fonctionnalités et d'accès à ces sociétés. Les départements Sécurité et Opérations souhaitent vérifier que les partenaires et les clients peuvent accéder uniquement aux ressources auxquelles ils ont besoin d'accéder et que l'implémentation de la solution n'augmente pas considérablement la charge de travail de l'équipe chargée des opérations. A. Datum travaille également sur la migration de certaines parties de son infrastructure réseau vers des services en ligne, notamment Windows Azure et Office 365.

Pour répondre aux besoins de l'entreprise, A. Datum envisage d'implémenter AD FS. Dans le cadre du déploiement initial, la société envisage d'utiliser AD FS pour implémenter l'authentification unique (SSO) des utilisateurs internes qui accèdent à une application sur un serveur Web. A. Datum a également conclu un partenariat avec une autre société, la société Trey Research. Les utilisateurs de Trey Research doivent pouvoir accéder à la même application.

En tant que l'un des administrateurs réseau seniors chez A. Datum, vous êtes chargé de l'implémentation de la solution AD FS. Comme preuve de concept, vous envisagez de déployer un exemple d'application prenant en charge les revendications et de configurer AD FS pour permettre aux utilisateurs internes et aux utilisateurs de Trey Research d'accéder à la même application.

Objectifs

- Configurer les conditions préalables d'AD FS.
- Installer et configurer AD FS.
- Configurer AD FS pour une seule organisation.
- Configurer AD FS pour des partenaires commerciaux fédérés.

Configuration de l'atelier pratique

Durée approximative : 90 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-CL1** **22412B-MUN-DC1**
Nom d'utilisateur	Adatum\Administrator
Mot de passe	Pa$$w0rd.

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Ouvrez une session en utilisant les informations d'authentification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 3 pour **22412B-LON-SVR1**, **22412B-LON-CL1**et **22412B-MUN-DC1**.
   a. Connectez-vous à 22412B-LON-SVR1 en tant que **ADATUM\Administrateur**.
   b. Ne vous connectez pas à 22412B-LON-CL1 à ce stade.
   c. Sur 22412B-MUN-DC1, connectez-vous en tant que **TREYRESEARCH\Administrateur** avec le mot de passe **Pa$$w0rd**.

Exercice 1 : Configuration des conditions préalables des services AD FS (Active Directory Federation Services)

Scénario

Pour déployer AD FS au sein de la société A. Datum, vous devez vérifier que tous les composants requis sont configurés. Vous envisagez de vérifier qu'AD CS est déployé dans l'organisation, puis de configurer les certificats requis pour AD FS sur le serveur AD FS et les serveurs Web. Vous envisagez également de configurer les redirecteurs DNS pour activer la communication entre Adatum.com et TreyResearch.net.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les redirecteurs DNS (Domain Name System)
2. Échanger les certificats racines pour activer des approbations de certificat
3. Demander et installer un certificat pour le serveur Web
4. Lier le certificat à l'application prenant en charge les revendications sur le serveur Web et vérifier l'accès à l'application

▶ Tâche 1 : Configurer les redirecteurs DNS (Domain Name System)

1. Sur LON-DC1, créez un redirecteur conditionnel pour le domaine TreyResearch.net à l'aide de l'adresse IP **172.16.10.10**du serveur DNS.
2. Sur MUN-DC1, créez un redirecteur conditionnel pour le domaine Adatum.com à l'aide de l'adresse IP **172.16.0.10** du serveur DNS.

▶ Tâche 2 : Échanger les certificats racines pour activer des approbations de certificat

1. Sur LON-DC1, copiez **MUN-DC1.TreyResearch.net_TreyResearch-MUN-DC1-CA.crt** de **\\MUN-DC1.treyresearch.net\certenroll** vers le dossier **Documents.**
2. Créez une console MMC (Microsoft Management Console) et ajoutez l'**Éditeur de gestion des stratégies de groupe**.
3. Modifiez l'objet de stratégie de groupe de la stratégie de domaine par défaut et importez le certificat racine copié dans le dossier Autorités de certification racines de confiance.
4. Sur MUN-DC1, copiez **LON-DC1.Adatum.com_Adatum-LON-DC1-CA.crt** de **\\LON-DC1.Adatum.com\certenroll** dans le dossier **Documents**.
5. Créez une console MMC et ajoutez le composant logiciel enfichable **Certificats** destiné à l'ordinateur local.
6. Importez le certificat racine copié dans le dossier Autorités de certification racines de confiance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Demander et installer un certificat pour le serveur Web

1. Sur LON-SVR1, ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Demandez un nouveau certificat de domaine pour le serveur à l'aide des paramètres suivants :
   - Nom commun : **LON-SVR1.adatum.com**
   - Organisation : **A. Datum**
   - Unité d'organisation : **Informatique**
   - Ville : **London**
   - Department/région : **Angleterre**
   - Pays/région : **GB**
3. Demandez le certificat à partir de **Adatum-LON-DC1-CA**.

▶ Tâche 4 : Lier le certificat à l'application prenant en charge les revendications sur le serveur Web et vérifier l'accès à l'application

1. Sur LON-SVR1, dans IIS, créez une liaison de site HTTPS, puis sélectionnez le certificat qui vient d'être créé.
2. Sur LON-DC1, ouvrez Internet Explorer et connectez-vous à **https://lon-svr1.adatum.com/adatumtestapp**.
3. Vérifiez que vous pouvez vous connecter au site, mais que vous recevez une erreur d'accès refusé 401. Cela est normal, car vous n'avez pas encore configuré AD FS pour l'authentification.
4. Fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous devez avoir configuré le transfert DNS pour activer la résolution de noms entre A. Datum et Trey Research et échangé des certificats racines entre les deux organisations. Vous devez avoir également installé et configuré un certificat Web sur le serveur d'applications.

Exercice 2 : Installation et configuration d'AD FS

Scénario

Pour commencer l'implémentation d'AD FS, vous envisagez d'installer AD FS sur le contrôleur de domaine de la société A. Datum et de configurer le serveur en tant que serveur de fédération autonome. Vous envisagez également de configurer le serveur pour utiliser un certificat de signature de jetons signé par une autorité de certification.

Les tâches principales de cet exercice sont les suivantes :

1. Installer et configurer AD FS
2. Créer un serveur de fédération autonome à l'aide de l'Assistant Configuration du serveur de fédération AD FS
3. Vérifier que le fichier FederationMetaData.xml est présent et contient des données valides

▶ Tâche 1 : Installer et configurer AD FS

- Sur LON-DC1, dans le Gestionnaire de serveur, ajoutez le rôle serveur AD FS (**Active Directory Federation Services**).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer un serveur de fédération autonome à l'aide de l'Assistant Configuration du serveur de fédération AD FS

- Sur LON-DC1, exécutez l'**Assistant Configuration du serveur de fédération AD FS** à l'aide des paramètres suivants :
  - créer un service de fédération ;
  - créer un déploiement autonome ;
  - utiliser le certificat **LON-DC1.Adatum.com** ;
  - choisir un nom de service **LON-DC1.Adatum.com**.

▶ Tâche 3 : Vérifier que le fichier FederationMetaData.xml est présent et contient des données valides

1. Sur LON-CL1, connectez-vous en tant que **Adatum\Brad** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez **Internet Explorer**.
3. Dans les options Internet, ajoutez **https://LON-DC1.Adatum.com** et **https://LON-SVR1.adatum.com** à la zone Intranet local.
4. Connectez-vous à **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.
5. Vérifiez que le fichier xml s'ouvre avec succès, puis parcourez son contenu.
6. Fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous aurez installé et configuré le rôle serveur AD FS et vérifié la réussite de l'installation en affichant le contenu du fichier FederationMetaData.xml.

Exercice 3 : Configuration d'AD FS pour une seule organisation

Scénario

Le premier scénario d'implémentation de l'application AD FS de mise à l'épreuve vise à garantir que les utilisateurs internes peuvent utiliser l'authentification unique (SSO) pour accéder à l'application Web. Vous envisagez de configurer le serveur AD FS et une application Web pour permettre ce scénario. Vous souhaitez également vérifier que les utilisateurs internes peuvent accéder à l'application.

1. Les tâches principales de cet exercice sont les suivantes :
2. Configurer un certificat de signature de jetons pour LON-DC1.Adatum.com
3. Configurer l'approbation de fournisseur de revendications Active Directory
4. Configurer l'application de revendications pour approuver les revendications entrantes en exécutant l'Utilitaire de fédération Windows Identity Foundation
5. Configurer une approbation de partie de confiance pour l'application prenant en charge les revendications
6. Configurer les règles de revendication pour l'approbation de partie de confiance
7. Tester l'accès à l'application prenant en charge les revendications

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer un certificat de signature de jetons pour LON-DC1.Adatum.com

1. Sur LON-DC1, à l'invite Windows PowerShell, utilisez la commande **set-ADFSProperties– AutoCertificateRollover $False** pour activer la modification des certificats attribués.
2. Dans la console AD FS, ajoutez le certificat de **LON-DC1.Adatum.com** comme nouveau certificat de signature de jetons. Vérifiez que le certificat a le sujet suivant **CN=LON-DC1.Adatum.com** et des rôles **Garantit votre identité auprès d'un ordinateur distant** et **Garantit l'identité d'un ordinateur distant**.
3. Faites du nouveau certificat le certificat principal et supprimez l'ancien certificat.

▶ Tâche 2 : Configurer l'approbation de fournisseur de revendications Active Directory

1. Sur LON-DC1, dans la console AD FS, accédez à **Approbations de fournisseur de revendications**, mettez en surbrillance le magasin **Active Directory** et accédez à **Modifier les règles de revendication**.
2. Dans la boîte de dialogue **Modifier les règles de revendication pour Active Directory**, sur l'onglet **Règles de transformation d'acceptation**, démarrez l'Assistant Ajouter une règle de revendication de transformation et exécutez l'Assistant avec les paramètres suivants :
   - Modèle de règle de revendication : **Envoyer les attributs LDAP en tant que revendications**
   - Nom : **Règle d'attributs LDAP sortants**
   - Magasin d'attributs : **Active Directory**
3. Dans **Mappage des attributs LDAP aux types de revendications sortantes**, sélectionnez les valeurs suivantes :
   - Adresses de messagerie = **E-Mail-Addresses**
   - User-Principal-Name = **UPN**
   - Display-Name = **Nom**

▶ Tâche 3 : Configurer l'application de revendications pour approuver les revendications entrantes en exécutant l'Utilitaire de fédération Windows Identity Foundation

1. Sur LON-SVR1, à partir de l'écran d'accueil, démarrez l'**Utilitaire de fédération Windows Identity Foundation**.
2. Exécutez l'Assistant avec les paramètres suivants :
   - Pointez sur le fichier web.config de l'exemple d'application Windows Identity Foundation en accédant à **C:\Inetpub\wwwroot\ AdatumTestApp \web.config**.
   - Spécifiez une zone URI d'application en saisissant **https://lon-svr1.adatum.com/AdatumTestApp/**.
   - Sélectionner l'option **Utiliser un STS** existant et saisissez le chemin d'accès **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.
   - Sélectionnez l'option **Aucun chiffrement**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer une approbation de partie de confiance pour l'application prenant en charge les revendications

1. Sur LON-DC1, dans la console AD FS, dans le volet central, cliquez sur **Requis : ajouter une partie de confiance approuvée**.
2. Exécutez l'Assistant Ajouter une approbation de partie de confiance avec les paramètres suivants :
   - Sélectionnez l'option **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confience**, puis saisissez **https://lon-svr1.adatum.com/adatumtestapp**.
   - Spécifiez le **Nom complet ADatum Test App**.
   - Sélectionnez l'option **Authoriser l'accés de tous les utilisateurs à cette partie de confiance**.
   - À la fin de l'exécution de l'Assistant, acceptez l'option pour ouvrir **Modifier les règles de revendication pour ADatum Test App**.

▶ Tâche 5 : Configurer les règles de revendication pour l'approbation de partie de confiance

1. Dans la boîte de dialogue **Modifier les règles de revendication pour Adatum Test App,** sur l'onglet **Règles de transformation d'émission,** choisissez d'ajouter une règle.
2. Exécutez l'Assistant Ajouter une règle de revendication de transformation avec les paramètres suivants :
   - Dans la liste déroulante **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**.
   - Nommez la règle de revendication **Passer la règle du nom de compte Windows**.
   - Dans la liste déroulante **Type de revendication entrante**, cliquez sur **Nom de compte Windows**.
3. Créez trois règles supplémentaires pour passer par **Adresse de messagerie**, **UPN** et **Revendication par type de nom**.

▶ Tâche 6 : Tester l'accès à l'application prenant en charge les revendications

1. Sur LON-CL1, ouvrez Internet Explorer, et connectez-vous à **https://lon-svr1.adatum.com/AdatumTestApp/**.
2. Vérifiez que vous avez accès à l'application.

Résultats : À la fin de cet exercice, vous aurez configuré les services AD FS pour une seule organisation. Pour ce faire, vous devez avoir configuré un certificat de signature de jetons ainsi qu'une approbation de fournisseur de revendications pour Adatum.com. Vous devez également avoir configuré l'exemple d'application pour approuver les revendications entrantes et configuré une approbation de partie de confiance et les règles de revendication associées. Vous devez également avoir testé l'accès à l'exemple d'application Windows Identity Foundation dans un seul scénario d'organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT - - -

Exercice 4 : Configuration d'AD FS pour des partenaires commerciaux fédérés

Scénario

Le deuxième scénario de déploiement consiste à permettre aux utilisateurs de Trey Research d'accéder à l'application Web. Vous envisagez de configurer l'intégration d'AD FS au sein de Trey Research avec AD FS au sein de la société A. Datum, puis de vérifier que les utilisateurs de Trey Research peuvent accéder à l'application. Vous souhaitez également confirmer que vous pouvez configurer l'accès basé sur les groupes d'utilisateurs. Vous devez vous vérifiez que tous les utilisateurs au sein d'A. Datum, et seulement les utilisateurs membres du groupe Production au sein de Trey Research, peuvent accéder à l'application.

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter une approbation de fournisseur de revendications pour le serveur AD FS de TreyResearch.net
2. Configurer une approbation de partie de confiance sur MUN-DC1 pour l'application prenant en charge les revendications A. Datum
3. Vérifier l'accès à l'application de test A. Datum pour les utilisateurs de Trey Research
4. Configurer les règles de revendication pour que l'approbation de fournisseur de revendications et l'approbation de partie de confiance autorisent l'accès à un seul groupe
5. Vérifier les restrictions et l'accessibilité à l'application prenant en charge les revendications

▶ Tâche 1 : Ajouter une approbation de fournisseur de revendications pour le serveur AD FS de TreyResearch.net

1. Sur LON-DC1, dans la console AD FS, développez **Relations d'approbation**, cliquez sur **Approbations de fournisseur de revendications**, puis sur **Ajouter une approbation de fournisseur de revendications**.
2. Exécutez l'Assistant Ajouter une approbation de fournisseur de revendications avec les paramètres suivants :
   - Sélectionnez **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confience** et saisissez **https://mun-dc1.treyresearch.net** en tant que source des données.
   - Dans **Nom complet**, saisissez **mun-dc1.treyresearch.net**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Modifier les règles de revendication pour mun-dc1.treyresearch.net Propriétés** utilisez les valeurs suivantes :
   - Ajoutez une **règle** aux règles de transformation d'acceptation.
   - Cliquez sur **Passer ou filtrer une revendication entrante** dans la liste **Modèle de règle de revendication**.
   - Utilisez **Passer la règle du nom de compte Windows** en tant que nom de la règle de revendication.
   - Choisissez **Nom de compte Windows** en tant que type de revendication entrante, puis choisissez de **Passer toutes les valeurs de revendication**.
   - Terminez la règle.
4. Sur LON-DC1, exécutez la commande suivante dans Windows PowerShell.

```
Set-ADFSClaimsProviderTrust –TargetName “mun-dc1.treyresearch.net” –
SigningCertificateRevocationCheck None
```

Remarque : Vous devez désactiver la vérification de la révocation des certificats uniquement dans les environnements de test. Dans un environnement de production, la vérification de la révocation des certificats doit être activée.

▶ Tâche 2 : Configurer une approbation de partie de confiance sur MUN-DC1 pour l'application prenant en charge les revendications A. Datum

1. Sur MUN-DC1, dans la console AD FS, ouvrez l'**Assistant Ajouter une approbation de partie de confiance** et exécutez-le avec les paramètres suivants :
   - Sélectionnez l'option **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confience** et saisissez **https:// lon-dc1.adatum.com**.
   - Spécifiez le **Nom complet Adatum TestApp**.
   - Sélectionnez l'option **Autoriser l'accès de tous les utilisateurs à cette partie de confiance**.
   - Acceptez l'option pour ouvrir **Modifier les règles de revendication pour Adatum Test App** à la fin de l'exécution de l'Assistant.
2. Dans la boîte de dialogue de propriétés **Modifier les règles de revendication pour Adatum TestApp**, sur l'onglet **Règles de transformation d'émission**, cliquez pour ajouter une règle avec les paramètres suivants :
   - Dans la liste Modèle de règle de revendication, cliquez sur **Passer ou filtrer une revendication entrante**.
   - Dans la zone Nom de la règle de revendication, saisissez **Passer la règle du nom de compte Windows**.
   - Choisissez **Nom de compte Windows** dans **Type de revendication entrante**.
   - Choisissez de **Passer toutes les valeurs de revendication**.
   - Terminez l'Assistant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérifier l'accès à l'application de test A. Datum pour les utilisateurs de Trey Research

1. Sur MUN-DC1, ouvrez Internet Explorer et connectez-vous à **https://lon-svr1.adatum.com/adatumtestapp/**.
2. Sélectionnez **mun-dc1.treyresearch.net** en tant que domaine d'accueil et connectez-vous en tant que **TreyResearch\April** avec le mot de passe **Pa$$w0rd**.
3. Vérifiez que vous avez accès à l'application.
4. Fermez Internet Explorer et connectez-vous au même site Web. Vérifiez que cette fois vous n'êtes pas invité à sélectionner un domaine d'accueil.

Remarque : À nouveau, vous n'êtes pas invité à sélectionner un domaine d'accueil. Une fois que les utilisateurs ont sélectionné un domaine d'accueil et ont été authentifiés par une autorité du domaine, ils reçoivent un cookie _LSRealm du serveur de fédération de la partie de confiance. La durée de vie par défaut pour le cookie est de 30 jours. Par conséquent, pour se connecter à plusieurs reprises, vous devez supprimer ce cookie après chaque tentative de connexion pour revenir un état propre.

▶ Tâche 4 : Configurer les règles de revendication pour que l'approbation de fournisseur de revendications et l'approbation de partie de confiance autorisent l'accès à un seul groupe

1. Sur MUN-DC1, ouvrez la console **AD FS** et accédez à l'approbation de partie de confiance d'**Adatum TestApp**.
2. Ajoutez une nouvelle règle de transformation d'émission qui envoie l'appartenance à un groupe en tant que revendication. Nommez la règle **Autoriser la règle du groupe Production**, configurez le groupe d'utilisateurs comme **Production**, configurez le type de revendication sortante comme **Groupe** et la valeur de revendication sortante comme **Production**.
3. Sur LON-DC1, dans la console AD FS, modifiez la **règle de fournisseur de revendications mun-dc1.treyresearch.net** pour créer une règle qui passe ou filtre une revendication entrante avec le nom de la règle **Envoyer la règle du groupe Production**. Configurez la règle avec le type de revendication entrante **Groupe**.
4. Modifiez l'approbation de partie de confiance d'**Adatum Test App** en créant une règle de transformation d'émission qui passe ou filtre une revendication entrante. Nommez la règle **Envoyer la règle du nom de groupe TreyResearch** et configurez la règle pour utiliser le type de revendication entrante **Groupe**.
5. Supprimez la règle d'autorisation d'émission qui accorde l'accès à tous les utilisateurs.
6. Créez une règle d'autorisation d'émission qui autorise ou refuse l'accès aux utilisateurs selon la revendication entrante. Configurez la règle avec le nom **Autoriser la règle du groupe Production TreyResearch**, le **Type de revendication entrante Groupe**, la **Valeur de revendication entrante Production** et sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**.
7. Créez une règle d'autorisation d'émission qui autorise ou refuse l'accès aux utilisateurs selon la revendication entrante. Configurez cette règle avec le nom **Temp**, le **Type de revendication entrante UPN**, la **Valeur de revendication entrante @adatum.com**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Modifiez la règle Temp et copiez le langage des règles de revendication dans le presse-papiers.
9. Supprimez la règle Temp.
10. Créez une règle qui envoie les revendications à l'aide d'une règle personnalisée nommée **Règle d'accès utilisateur ADatum**.
11. Cliquez dans la zone **Règle personnalisée** et appuyez sur les touches Crtl + V pour coller le contenu du presse-papiers dans la zone. Modifiez la première URL afin qu'elle corresponde au texte suivant, puis cliquez sur **Terminer**.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", Value =~
"^(?i).+@adatum\.com$"]=> issue(Type =
“http://schemas.microsoft.com/authorization/claims/permit”, Value =
“PermitUsersWithClaim”);
```

▶ Tâche 5 : Vérifier les restrictions et l'accessibilité à l'application prenant en charge les revendications

1. Sur MUN-DC1, ouvrez Internet Explorer et connectez-vous à **https://lon-svr1.adatum.com/adatumtestapp/**.
2. Vérifiez que **TreyResearch\April** n'a plus accès à A. Datum test app.
3. Effacez l'historique de navigation dans Internet Explorer.
4. Connectez-vous à **https://lon-svr1.adatum.com/adatumtestapp/**.
5. Vérifiez que **TreyResearch\Morgan** a accès à A. Datum test app. Morgan est membre du groupe Production.

Résultats : À la fin de cet exercice, vous aurez configuré une approbation de fournisseur de revendications pour Trey Research sur Adatum.com et une approbation de partie de confiance pour Adatum sur TreyResearch.net. Vous avez vérifié l'accès à l'application A. Datum prenant en charge les revendications. Vous avez configuré ensuite l'application pour limiter l'accès à partir de TreyResearch aux groupes spécifiques et vous avez vérifié l'accès approprié.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-MUN-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-CL1**, **22412B-LON-SVR1** et **22412B-LON-DC1**.

UTILISATION PRÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quels sont les avantages du déploiement d'AD FS avec une application ou un service de basés sur le cloud ?

Question : Dans quelles circonstances choisiriez-vous de déployer un serveur proxy de fédération ? Dans quelles circonstances n'avez-vous pas besoin de déployer un serveur proxy de fédération ?

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Erreurs de certificat sur le serveur de fédération	
Erreurs de certificat sur le client	
Échec de l'authentification avec AD FS de l'application cliente	

Problèmes réels et scénarios

Question : Tailspin Toys déploie une nouvelle application Web prenant en charge les revendications, qui doit être accessible à la fois aux utilisateurs de Tailspin Toys et aux utilisateurs de Trey Research. Quels composants AD FS devez-vous déployer au sein de Tailspin Toys pour permettre ce niveau d'accès ?

Question : Fabrikam, Inc. examine les configurations requises pour AD FS. La société souhaite utiliser un serveur proxy de fédération pour garantir une sécurité maximale. Fabrikam bénéficie actuellement d'un réseau interne avec des serveurs DNS internes et son DNS Internet est hébergé par une société d'hébergement. Le réseau de périmètre utilise les serveurs DNS de la société d'hébergement pour la résolution DNS. Que doit faire la société pour préparer le déploiement ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9

Implémentation de l'équilibrage de la charge réseau

Table des matières :

Vue d'ensemble du module **9-1**

Leçon 1 : Vue d'ensemble de NLB **9-2**

Leçon 2 : Configuration d'un cluster NLB **9-6**

Leçon 3 : Planification d'une implémentation NLB **9-13**

Atelier pratique : Implémentation de l'équilibrage de la charge réseau **9-19**

Contrôle des acquis et éléments à retenir **9-24**

Vue d'ensemble du module

L'Équilibrage de la charge réseau (NLB) est un composant réseau de Windows Server®. NLB utilise un algorithme distribué pour équilibrer la charge du trafic IP sur plusieurs hôtes. L'équilibrage de la charge réseau aide à améliorer l'extensibilité et la disponibilité des services IP critiques pour l'entreprise. La technologie NLB offre également une disponibilité de haut niveau car elle détecte les défaillances d'hôtes et redistribue automatiquement le trafic aux hôtes survivants.

Pour déployer NLB effectivement, vous devez comprendre sa fonctionnalité et les scénarios où son déploiement est approprié. La principale mise à jour dans NLB pour Windows Server 2012 est l'inclusion d'un ensemble complet d'applets de commande Windows PowerShell®. Ces applets de commande améliorent votre capacité d'automatiser la gestion des clusters NLB dans Windows Server 2012. La console de l'équilibrage de la charge réseau, qui est également disponible dans Windows Server 2008 et Windows Server 2008 R2, est également présente dans Windows Server 2012

Ce module vous présente NLB et vous montre comment déployer cette technologie. Ce module présente également les situations pour lesquelles NLB est approprié, comment configurer et gérer des clusters NLB et comment effectuer des tâches de maintenance sur des clusters NLB.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire NLB ;
- expliquer comment configurer un cluster NLB ;
- expliquer comment planifier une implémentation NLB.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble de NLB

Avant que vous déployiez NLB, vous devez avoir une bonne compréhension des types de charges de travail de serveur pour lesquelles cette technologie de haute disponibilité est appropriée. Si vous ne comprenez pas la fonctionnalité de NLB, il est possible que vous le déployiez d'une manière qui ne permette pas d'atteindre vos objectifs globaux. Par exemple, vous devez comprendre pourquoi NLB est approprié pour des applications Web, mais pas pour les bases de données Microsoft® SQL Server®.

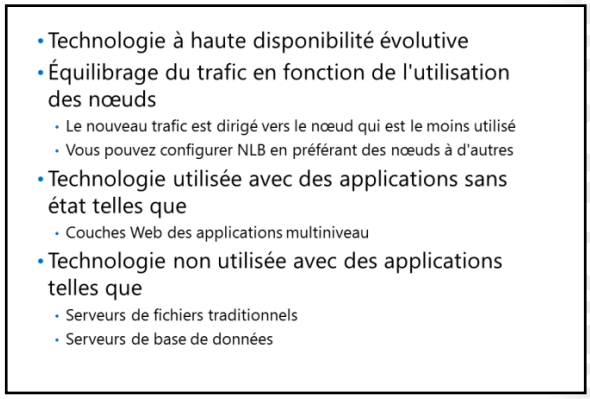
Cette leçon fournit une vue d'ensemble de NLB, ainsi que les nouvelles fonctionnalités de NLB dans Windows Server 2012. Elle décrit également comment NLB fonctionne normalement, et comment la technologie fonctionne pendant la défaillance de serveur et la récupération de serveur.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire la technologie NLB ;
- décrire le fonctionnement du service NLB ;
- expliquer comment NLB traite les défaillances et la récupération de serveur ;
- décrire les nouvelles fonctionnalités NLB dans Windows Server 2012.

Qu'est-ce que NLB ?



NLB est une fonctionnalité évolutive et de haute disponibilité que vous pouvez installer sur toutes les éditions de Windows Server 2012. Une *technologie évolutive* permet d'ajouter des composants supplémentaires (dans ce cas, des nœuds de cluster supplémentaires) pour satisfaire une demande croissante. Un *nœud* dans un cluster NLB de Windows Server 2012 est un ordinateur, physique ou virtuel, qui exécute le système d'exploitation Windows Server 2012.

Les clusters NLB dans Windows Server 2012 peuvent avoir entre 2 et 32 nœuds. Lorsque vous créez un cluster NLB, il crée une adresse et une carte réseau virtuelle. La carte réseau virtuelle a une adresse IP et une adresse MAC (Media Access Control). Le trafic réseau vers cette adresse est distribué équitablement entre les nœuds du cluster. Dans une configuration NLB de base, chaque nœud d'un cluster NLB traitera des demandes à une cadence qui est approximativement égale à celle de tous les autres nœuds du cluster. Lorsqu'un cluster NLB reçoit une demande, il la fera suivre au nœud qui est le moins utilisé. Vous pouvez configurer NLB en préférant des nœuds à d'autres.

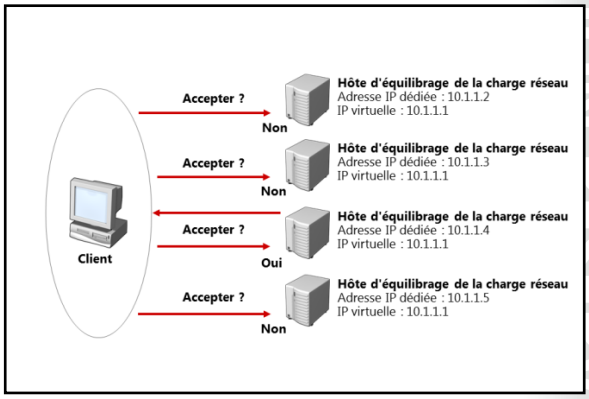
NLB tient compte des défaillances. Ceci signifie que si un des nœuds du cluster NLB est hors connexion, les demandes ne seront plus transférées à ce nœud, mais aux autres nœuds du cluster qui continueront à accepter les demandes. Si le nœud défectueux refonctionne, les demandes entrantes seront redirigées jusqu'à ce que le trafic soit équilibré entre tous les nœuds du cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement de la virtualisation des postes de travail (NLB)

Lorsque vous configurez une application en vue d'utiliser NLB, les clients adressent l'application utilisant l'adresse de cluster NLB plutôt que l'adresse des nœuds faisant partie du cluster NLB. L'*adresse de cluster NLB* est une adresse virtuelle qui est partagée entre les hôtes dans le cluster NLB.



NLB dirige le trafic de la façon suivante : Tous les hôtes dans le cluster NLB reçoivent le trafic entrant, mais seul un nœud du cluster, qui est déterminé par le processus NLB, acceptera ce trafic. Tous autres nœuds du cluster NLB abandonneront le trafic.

Le nœud du cluster NLB qui accepte le trafic dépend de la configuration des règles de port et des paramètres d'affinité. Par ces paramètres, vous pouvez déterminer si le trafic qui utilise un port particulier et un protocole seront acceptés par un nœud particulier, ou si n'importe quel nœud du cluster peut accepter et répondre.

NLB envoie également le trafic aux nœuds selon l'utilisation actuelle de nœud. Le nouveau trafic est dirigé vers les nœuds qui sont les moins utilisés. Par exemple, si vous avez un cluster de quatre nœuds où trois des nœuds répondent aux demandes de 10 clients et un nœud répond aux demandes de 5 clients, le nœud qui a le moins de clients recevra plus de trafic entrant jusqu'à ce que l'utilisation soit équitablement répartie entre les nœuds.

Comment NLB traite les défaillances et la récupération de serveur ?

NLB peut détecter la défaillance des nœuds de cluster. Lorsqu'un nœud de cluster est dans un état défaillant, il est supprimé du cluster, et ce dernier ne dirige pas le nouveau trafic vers le nœud. La défaillance est détectée à l'aide des pulsations. Des pulsations de cluster NLB sont transmises chaque seconde entre les nœuds d'un cluster. Un nœud est automatiquement supprimé d'un cluster NLB s'il manque cinq pulsations consécutives. Les pulsations sont transmises sur un réseau qui est habituellement différent du réseau que le client utilise pour accéder au cluster.

Des pulsations de cluster NLB sont transmises chaque seconde entre les nœuds d'un cluster

La convergence se produit si

- Un nœud manque cinq pulsations consécutives, auquel cas il est automatiquement supprimé d'un cluster NLB
- Un nœud qui était membre d'un cluster est remis en service
- Un administrateur ajoute ou supprime un nœud manuellement

Lorsqu'un nœud est ajouté ou supprimé d'un cluster, un processus appelé la convergence se produit. La convergence permet au cluster de déterminer sa configuration actuelle. La convergence peut seulement se produire si chaque nœud est configuré avec les mêmes règles de port.

Les nœuds peuvent être configurés pour rejoindre un cluster automatiquement en définissant le paramètre d'état d'hôte initial dans les propriétés du nœud à l'aide du Gestionnaire d'équilibrage de la charge réseau. Par défaut, un hôte qui est membre d'un cluster tentera de rejoindre ce cluster automatiquement. Par exemple, après application d'une mise à jour logicielle, si vous redémarrez un serveur qui est membre d'un cluster NLB, le serveur rejoindra le cluster automatiquement à la fin du processus de redémarrage.

Les administrateurs peuvent ajouter ou supprimer manuellement des nœuds des clusters NLB. Lorsqu'un administrateur supprime un nœud, il peut choisir d'exécuter une action Arrêter ou Drainer et arrêter. L'action Arrêter termine toutes les connexions existantes du nœud de cluster et arrête le service NLB. L'action Drainer et arrêter bloque toutes les nouvelles connexions sans terminer les sessions existantes. Une fois que toutes les sessions actives sont terminées, le service NLB est arrêté.

NLB peut seulement détecter une défaillance de serveur ; il ne peut pas détecter une défaillance d'application. Cela signifie que si une application Web échoue mais que le serveur reste opérationnel, le cluster NLB continuera à transférer le trafic vers le nœud de cluster qui héberge l'application défaillante. Une méthode de gestion de ce problème consiste à implémenter une solution de surveillance telle que Microsoft System Center 2012 - Operations Manager. Grâce à Operations Manager, vous pouvez surveiller la fonctionnalité des applications. Vous pouvez également configurer Operations Manager pour générer une alerte au cas où une application sur un nœud de cluster échouerait. Une alerte à son tour peut configurer une action de mise à jour, telle que le redémarrage des services, le redémarrage du serveur ou le retrait du nœud du cluster NLB de sorte qu'il ne reçoive pas davantage de trafic entrant.

Fonctionnalités NLB de Windows Server 2012

Le changement majeur apporté aux fonctionnalités d'équilibrage de la charge réseau dans Windows Server 2012 est l'inclusion de la prise en charge de Windows PowerShell. Le module de NetworkLoadBalancingClusters contient 35 applets de commande NLB. Ce module devient disponible sur un serveur lorsque les Outils d'administration de serveur distant NLB sont installés. Les applets de commande Windows PowerShell ont les noms suivants :

Utiliser 35 nouvelles applets de commande Windows PowerShell NLB pour gérer tous les aspects de configuration NLB

- Utiliser le nom NlbCluster pour gérer le cluster
- Utiliser le nom NlbClusterNode pour gérer différents nœuds

- **NlbClusterNode**. Permet de gérer un nœud de cluster. Comprend les verbes **Add**, **Get**, **Remove**, **Resume**, **Set**, **Start**, **Stop** et **Suspend**.
- **NlbClusterNodeDip**. Permet de configurer l'IP de gestion consacré au nœud de cluster. Comprend les verbes **Add**, **Get**, **Remove** et **Set**.
- **NlbClusterPortRule**. Permet de gérer les règles de port. Comprend les verbes **Add**, **Disable**, **Enable**, **Get**, **Remove** et **Set**.
- **NlbClusterVip**. Permet de gérer l'IP virtuel du cluster NLB. Comprend les verbes **Add**, **Get**, **Remove** et **Set**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- **NlbCluster**. Permet de gérer le cluster NLB. Comprend les verbes **Get**, **New**, **Remove**, **Resume**, **Set**, **Start**, **Stop** et **Suspend**.
- **NlbClusterDriverInfo**. Fournit des informations sur le pilote de cluster NLB. Comprend le verbe **Get**.
- **NlbClusterNodeNetworkInterface**. Permet de récupérer des informations sur le pilote de l'interface réseau d'un nœud de cluster. Comprend le verbe **Get**.
- **NlbClusterIpv6Address**. Permet de configurer l'adresse IPv6 du cluster. Comprend le verbe **New**.
- **NlbClusterPortRuleNodeHandlingPriority**. Permet de définir la priorité sur une base de règles par port. Prend en charge le verbe **Set**.
- **NlbClusterPortRuleNodeWeight**. Permet de définir le poids du nœud sur une base de règles par port. Prend en charge le verbe **Set**.

 **Remarque :** Pour afficher la liste des applets de commande Windows PowerShell pour NLB, vous pouvez utiliser la commande **get-command –module NetworkLoadBalancingClusters**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration d'un cluster NLB

Pour déployer NLB avec succès, vous devez d'abord avoir une bonne compréhension de ses configurations de déploiement requises. Vous devez également avoir organisé la façon dont vous allez utiliser les règles de port et les paramètres d'affinité pour garantir que ce trafic vers l'application qui est hébergée sur le cluster NLB est géré convenablement.

Cette leçon vous fournit des informations sur les configurations d'infrastructure requises que vous devez prendre en considération avant de déployer NLB. Elle vous fournit également des informations importantes sur la façon de configurer les clusters et les nœuds NLB afin de répondre au mieux à vos objectifs.

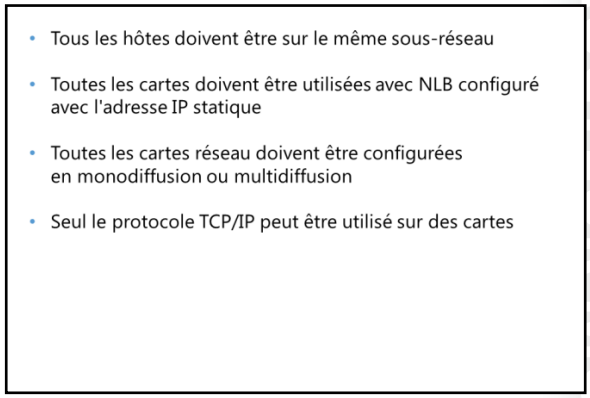
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les conditions requises pour le déploiement NLB ;
- décrire comment implémenter NLB ;
- expliquer les options de configuration de NLB ;
- expliquer comment configurer l'affinité et les règles de port NLB ;
- décrire les éléments réseau à prendre en compte pour NLB.

Conditions requises pour le déploiement NLB

NLB requiert que tous les hôtes du cluster NLB résident sur le même sous-réseau TCP/IP. Bien que les sous-réseaux TCP/IP puissent être configurés pour couvrir plusieurs situations géographiques, les clusters NLB sont peu susceptibles d'accomplir la convergence avec succès si la latence entre les nœuds dépasse 250 millisecondes (ms). Si vous concevez des clusters NLB dispersés géographiquement, vous devez plutôt choisir de déployer un cluster NLB au niveau de chaque site, puis d'utiliser le tourniquet DNS pour distribuer le trafic entre les sites.



Toutes les cartes réseau d'un cluster NLB doivent être configurées en monodiffusion ou multidiffusion. Vous ne pouvez pas configurer un cluster NLB dans le cas d'une association de cartes monodiffusion et multidiffusion. En utilisant le mode monodiffusion, la carte réseau doit prendre en charge la modification de son adresse MAC.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez uniquement utiliser le protocole TCP/IP avec les cartes réseau qui font partie des clusters NLB. NLB prend en charge IPv4 et IPv6. Les adresses IP des serveurs qui font partie du cluster NLB doivent être statiques et ne doivent pas être allouées dynamiquement. Lorsque vous installez NLB, le protocole DHCP (Dynamic Host Configuration Protocol) est désactivé sur chaque interface que vous configurez pour faire partie du cluster.

Toutes les éditions de Windows Server 2012 prennent en charge NLB. Microsoft prend en charge les clusters NLB avec les nœuds qui exécutent différentes éditions de Windows Server 2012. Cependant, pour de meilleurs résultats, les nœuds de cluster NLB doivent être des ordinateurs avec les mêmes spécifications matérielles et qui exécutent la même édition du système d'exploitation de Windows Server 2012.

Démonstration : Déploiement NLB

Cette démonstration montre comment créer un cluster NLB dans Windows Server 2012.

Procédure de démonstration

Créer un cluster NLB dans Windows Server 2012

1. Connectez-vous à **LON-SVR1** à l'aide du compte **ADATUM\Administrateur.**
2. Dans le menu Outils, ouvrez l'environnement d'écriture de scripts intégré (**ISE, Integrated Scripting Environment**) de **Windows PowerShell**.
3. Saisissez les commandes suivantes, en appuyant sur Entrée après chaque commande :

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-
WindowsFeature NLB,RSAT-NLB}
New-NlbCluster -InterfaceName "Connexion au réseau local" -OperationMode Multicast -
ClusterPrimaryIP 172.16.0.42 -ClusterName LON-NLB
Add-NlbClusterNode -InterfaceName "Connexion au réseau local" -NewNodeName "LON-SVR2"
-NewNodeInterface "Connexion au réseau local"
```

4. Ouvrez le **Gestionnaire d'équilibrage de la charge de réseau** à partir du menu **Outils** et affichez le cluster.

Options de configuration pour NLB

La configuration des clusters NLB implique la spécification du mode de réponse des hôtes du cluster dans le trafic réseau entrant. Comment NLB dirige le trafic dépend du port et du protocole qu'il utilise, et si le client a une session réseau existante avec un hôte dans le cluster. Vous pouvez configurer ces paramètres à l'aide des règles de port et des paramètres d'affinité.

Les règles de port déterminent comment le trafic est routé vers les nœuds de cluster en fonction du port TCP ou UDP

- Hôte multiple
- Hôte unique
- Désactiver l'étendue de port

Les paramètres d'affinité déterminent comment la reconnexion se produit

- Aucun
- Unique
- Classe C

Règles de port

Les règles de port permettent de configurer la manière dont le cluster NLB dirige les demandes vers des adresses et ports IP spécifiques. Vous pouvez équilibrer la charge du trafic du port TCP 80 entre tous les nœuds d'un cluster NLB, tout en dirigeant toutes les demandes du port TCP 25 vers un hôte spécifique.

Pour spécifier comment vous souhaitez distribuer les demandes entre les nœuds du cluster, vous devez configurer un mode de filtrage lors de la création d'une règle de port. Vous pouvez effectuer l'opération dans la boîte de dialogue **Ajouter/Modifier une règle de port** permettant de configurer l'un des modes de filtrage suivants :

- **Hôte multiple**. Lorsque vous configurez ce mode, tous les nœuds NLB répondent selon le poids attribué à chaque nœud. Le poids de nœud est calculé automatiquement, selon les caractéristiques du fonctionnement de l'hôte. Si un nœud échoue, d'autres nœuds du cluster continuent à répondre aux demandes entrantes. Le filtrage de l'hôte multiple accroît la disponibilité et l'extensibilité, comme vous pouvez augmenter la capacité en ajoutant des nœuds, et le cluster continue à fonctionner en cas de défaillance de nœud.
- **Hôte unique**. Lorsque vous configurez ce mode, le cluster NLB dirige le trafic vers le nœud qui se voit attribuer la priorité la plus élevée. Dans le cas où le nœud avec la priorité la plus élevée serait indisponible, l'hôte suivant avec la priorité la plus élevée gèrerait le trafic entrant. Les règles de l'hôte unique augmentent la disponibilité, mais n'augmentent pas l'extensibilité.

 **Remarque :** La priorité la plus élevée correspond au numéro le plus faible, avec la priorité 1 qui est la plus élevée et la priorité 10, la moins élevée.

- **Désactiver cette étendue de port**. Lorsque vous configurez cette option, tous les paquets de cette étendue de port sont abandonnés, sans être transférés à tous les nœuds de cluster. Si vous ne désactivez pas une étendue de port et il n'y a aucune règle de port existante, le trafic est transféré vers l'hôte avec le numéro de priorité le plus bas.

Vous pouvez utiliser les applets de commande Windows PowerShell suivants pour gérer les règles de port :

- **Add-NlbClusterPortRule**. Utilisez cette applet de commande pour ajouter une nouvelle règle de port.
- **Disable-NlbClusterPortRule**. Utilisez cette applet de commande pour désactiver une règle de port existante.
- **Enable-NlbClusterPortRule**. Utilisez cette applet de commande pour activer une règle de port désactivée.
- **Set-NlbClusterPortRule**. Utilisez cette applet de commande pour modifier les propriétés d'une règle de port existante.
- **Remove-NlbClusterPortRule**. Utilisez cette applet de commande pour supprimer une règle de port existante.

 **Remarque :** Chaque nœud d'un cluster doit avoir des règles de port identiques. Il existe une exception qui concerne le poids de charge (en mode de filtrage **hôte multiple**) et la priorité de traitement (en mode de filtrage **hôte unique**). Autrement, si les règles de port ne sont pas identiques, le cluster ne convergera pas.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Affinité

L'affinité détermine comment le cluster NLB distribue les demandes d'un client spécifique. Les paramètres d'affinité ne prennent réellement effet que si vous utilisez le mode de filtrage **hôte multiple**. Vous pouvez sélectionner l'un des modes d'affinité suivants :

- **Aucune**. Dans ce mode, n'importe quel nœud de cluster répond à n'importe quelle demande du client, même si le client se reconnecte après une interruption. Par exemple, la première page Web sur une application Web pourrait être récupérée du troisième nœud, de la deuxième page Web du premier nœud, et de la troisième page Web du deuxième nœud. Ce mode d'affinité convient aux applications sans état.
- **Unique**. Lorsque vous utilisez ce mode d'affinité, un nœud de cluster unique traite toutes les demandes d'un client unique. Par exemple, si le troisième nœud d'un cluster gère la première demande d'un client, alors toutes les demandes suivantes seront également gérées par ce nœud. Ce mode d'affinité convient aux applications avec état.
- **Classe C**. Si vous définissez ce mode, un seul nœud répondra à toutes les demandes d'un réseau de classe C (qui utilise le masque de sous-réseau 255.255.255.0). Ce mode est utile pour des applications avec état où le client accède au cluster NLB par les serveurs proxys à charge équilibrée. Ces serveurs proxys auront différentes adresses IP, mais seront dans le même bloc de sous-réseau de classe C (24 bits).

Paramètres de l'hôte

Configurez les paramètres d'un hôte en cliquant sur l'hôte dans la console **Gestionnaire d'équilibrage de la charge réseau**, puis dans le menu **Hôte**, en cliquant sur **Propriétés**. Vous pouvez configurer les paramètres d'hôte suivants pour chaque nœud NLB :

- **Priorité**. Chaque nœud NLB se voit attribuer une valeur prioritaire unique. Si aucune règle de port existante ne correspond au trafic qui est adressé au cluster, le trafic sera attribué au nœud NLB avec la valeur de la priorité la plus basse.
- **Adresse IP dédiée**. Vous pouvez utiliser ce paramètre pour spécifier l'adresse que l'hôte utilise pour des tâches de gestion à distance. Lorsque vous configurez une adresse IP dédiée, NLB configure des règles de port de sorte qu'elles n'affectent pas le trafic vers cette adresse.
- **Masque de sous-réseau**. Lorsque vous sélectionnez un masque de sous-réseau, assurez-vous qu'il y a suffisamment de bits hôtes pour prendre en charge le nombre de serveurs dans le cluster NLB, ainsi que tous les routeurs qui connectent le cluster NLB au reste du réseau de l'organisation. Par exemple, si vous planifiez d'avoir un cluster comportant 32 nœuds et prenant en charge deux routes vers le cluster NLB, vous devez définir un masque de sous-réseau qui prenne en charge 34 bits hôtes ou plus—comme 255.255.255.192.
- **État d'hôte initial**. Vous pouvez utiliser ce paramètre pour spécifier les actions que l'hôte prendra après un redémarrage. L'état Démarré par défaut indique que l'hôte rejoint le cluster NLB automatiquement. L'état Exécution suspendu interrompt l'hôte, ce qui vous permet d'exécuter les opérations qui requièrent plusieurs redémarrages sans déclencher la convergence de cluster. L'état Arrêté arrête le nœud.

Démonstration : Configuration de l'affinité et des règles de port NLB

Dans cette démonstration, vous allez apprendre à :

- configurer l'affinité pour des nœuds de cluster NLB ;
- configurer des règles de port NLB.

Procédure de démonstration

Configurer l'affinité pour des nœuds de cluster NLB

1. Sur LON-SVR2, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. Dans Windows PowerShell, entrez chacune des commandes suivantes, en appuyant sur Entrée après chaque commande :

```
Cmd.exe
Mkdir c:\porttest
Xcopy /s c:\inetpub\wwwroot c:\porttest
Exit
New-Website –Name PortTest –PhysicalPath “C:\porttest” –Port 5678
New-NetFirewallRule –DisplayName PortTest –Protocol TCP –LocalPort 5678
```

Configurer des règles de port NLB

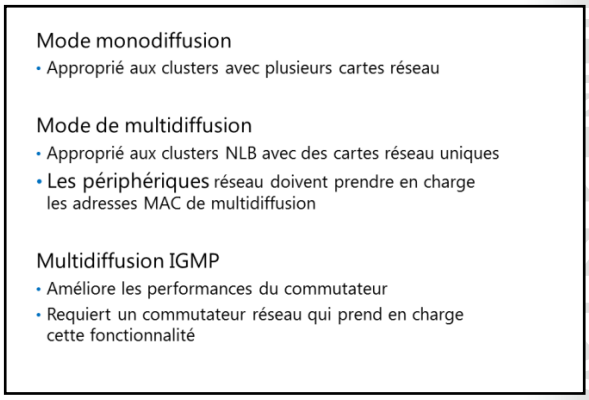
1. Sur LON-SVR1, ouvrez le **Gestionnaire d'équilibrage de la charge réseau**.
2. Supprimez la règle **Tous les ports**.
3. Dans le gestionnaire d'équilibrage de la charge réseau, modifiez les propriétés du cluster **LON-NLB**.
4. Ajoutez une règle de port ayant les propriétés suivantes :
   - Étendue du port : **80 à 80**
   - Protocoles : **Les deux**
   - Mode de filtrage : **Hôte multiple**
   - Affinité : **Aucure**
5. Créez une règle de port ayant les propriétés suivantes :
   - Étendue du port : **5678 à 5678**
   - Protocoles : **Les deux**
   - Mode de filtrage : **Hôte unique**
6. Modifiez les propriétés hôte de **LON-SVR1**.
7. Configurez la règle de port pour le port **5678** et la priorité de traitement définie sur **10**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments réseau à prendre en compte pour NLB

Si vous concevez un réseau pour prendre en charge un cluster NLB, vous devez considérer plusieurs facteurs. La principale décision est si vous souhaitez configurer le cluster NLB pour qu'il utilise le mode d'opération de cluster monodiffusion ou multidiffusion.



Mode monodiffusion

Si vous configurez un cluster NLB pour utiliser le mode monodiffusion, tous les hôtes de cluster utilisent la même adresse MAC de monodiffusion. Le trafic sortant utilise une adresse MAC modifiée qui est déterminée par le paramétrage des priorités de l'hôte de cluster. Ceci empêche le commutateur qui gère le trafic sortant de rencontrer des problèmes avec tous les hôtes de cluster utilisant la même adresse MAC.

Lorsque vous utilisez le mode monodiffusion avec une carte réseau unique sur chaque nœud, seuls les ordinateurs qui utilisent le même sous-réseau peuvent communiquer avec le nœud utilisant l'adresse IP attribuée du nœud. Si vous devez effectuer des tâches de gestion des nœuds, (comme se connecter à l'aide de la fonctionnalité Bureau à distance du système d'exploitation Windows® pour appliquer des mises à jour logicielles), vous devez effectuer ces tâches à partir d'un ordinateur qui est sur le même sous-réseau TCP/IP que le nœud.

Si vous utilisez le mode monodiffusion avec au minimum deux cartes réseau, une carte sera utilisée pour la communication des clusters dédiés, et l'autre carte ou les autres cartes peuvent être utilisées pour les tâches de gestion. En utilisant le mode monodiffusion avec plusieurs cartes réseau, vous pouvez effectuer les tâches de gestion du cluster telles que se connecter à l'aide de PowerShell à distance pour ajouter ou supprimer des rôles et des fonctionnalités.

Le mode monodiffusion peut également réduire les problèmes qui se produisent lorsque les nœuds de cluster hébergent également d'autres rôles ou services non NLB. Par exemple, l'utilisation du mode monodiffusion signifie qu'un serveur faisant partie d'un cluster de serveur Web sur le port 80, peut également héberger un autre service tel que les services DNS ou DHCP. Bien que ce soit possible, nous recommandons que tous les nœuds de cluster aient la même configuration.

Mode de multidiffusion

Lorsque vous configurez un cluster NLB pour utiliser le mode de multidiffusion, chaque hôte de cluster conserve son adresse MAC d'origine, mais se voit également attribuer une adresse MAC de multidiffusion supplémentaire. Chaque nœud du cluster se voit attribuer la même adresse de multidiffusion MAC supplémentaire. Le mode de multidiffusion requiert les commutateurs réseau et les routeurs qui prennent en charge des adresses MAC de multidiffusion.

Protocole de multidiffusion IGMP (Internet Group Management Protocol Multicast)

Le mode de multidiffusion IGMP (Internet Group Management Protocol) est une forme spéciale du mode de multidiffusion qui empêche le commutateur réseau d'être submergé par le trafic. Lorsque vous déployez le mode de multidiffusion IGMP, le trafic est transféré uniquement par les ports de commutateur faisant partie du cluster NLB. Le mode de multidiffusion IGMP requiert le matériel de commutateur qui prend en charge cette fonctionnalité.

Éléments à prendre en compte en matière de réseau

Vous pouvez améliorer les performances de cluster NLB en utilisant le mode monodiffusion à l'aide des réseaux locaux virtuels distincts (VLAN) pour le trafic de cluster et le trafic de gestion. L'utilisation de segments VLAN empêche le trafic de gestion d'affecter le trafic de cluster. Si vous hébergez des nœuds NLB sur des ordinateurs virtuels utilisant Windows Server 2012, vous pouvez également utiliser la virtualisation réseau pour segmenter le trafic de gestion du trafic de cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Planification d'une implémentation NLB

Si vous planifiez une implémentation NLB, vous devez vérifier que les applications que vous déployez sont appropriées pour NLB. Toutes les applications ne sont pas adaptées au déploiement sur des clusters NLB et il est important que vous puissiez identifier lesquelles peuvent profiter de cette technologie. Vous devez également connaître les mesures à prendre pour sécuriser NLB et vous familiariser avec les options permettant de mettre NLB à l'échelle, si l'application hébergée sur le cluster NLB requiert une plus grande capacité.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment concevoir la prise en charge des applications et du stockage NLB ;
- décrire les considérations spéciales du déploiement de clusters NLB sur les ordinateurs virtuels ;
- décrire les options que vous pouvez implémenter pour sécuriser NLB ;
- décrire les options pour la mise à l'échelle de NLB ;

décrire la méthode que vous pouvez utiliser pour mettre un cluster NLB à niveau vers Windows Server 2012.

Conception de la prise en charge des applications et du stockage NLB

Puisque les clients peuvent être redirigés vers n'importe quel nœud dans un cluster NLB, chaque nœud du cluster doit pouvoir fournir une expérience cohérente. Par conséquent, lorsque vous concevez la prise en charge des applications et du stockage pour les applications NLB, vous devez veiller à configurer chaque nœud de la même manière et que chaque nœud ait accès aux mêmes données.

- Chaque nœud d'un cluster NLB doit avoir la même configuration
- Chaque nœud a besoin d'accéder aux mêmes données d'applications cohérentes
- Utiliser la configuration partagée IIS pour avoir l'assurance que la configuration d'application Web est cohérente entre les nœuds NLB
- Utiliser les CSV pour héberger des données d'application et de configuration partagées pour les applications NLB

Si une application hautement disponible est dotée de plusieurs niveaux (comme une application Web qui comprend un niveau de base de données SQL Server), l'application Web est hébergée sur un cluster NLB. SQL Server, comme une application avec état, n'est pas rendu hautement disponible avec NLB. Au lieu de cela, vous utilisez des technologies telles que le clustering avec basculement, la mise en miroir ou les Groupes de disponibilité AlwaysOn, pour rendre la couche de la base de données SQL Server hautement disponible.

Tous les hôtes d'un cluster NLB devraient exécuter les mêmes applications et être configurés de la même manière. Lorsque vous utilisez des applications Web, vous pouvez utiliser la fonctionnalité de configuration partagée IIS 8.0 (Internet Information Services) pour vérifier que tous les nœuds du cluster NLB sont configurés de la même manière.

Vous pouvez également utiliser des technologies telles que les partages de fichiers qui sont hébergés sur des volumes partagés de cluster (CSV) pour héberger les informations de configuration d'application. Les partages de fichiers qui sont hébergés sur les CSV permettent à plusieurs hôtes d'avoir accès aux données des applications et aux données de configuration. Les partages de fichiers qui sont hébergés sur les CSV sont une fonctionnalité de Windows Server 2012.

Éléments à prendre en compte pour le déploiement d'un cluster NLB sur des ordinateurs virtuels

Comme les organisations passent d'un déploiement physique à un déploiement virtuel, les administrateurs doivent considérer plusieurs facteurs en déterminant le placement des nœuds de cluster NLB sur les hôtes Hyper-V®. Ceci comprend la configuration réseau des ordinateurs virtuels, la configuration des hôtes Hyper-V et les avantages d'utiliser la haute disponibilité Hyper-V en même temps que NLB.

- Configurer les ordinateurs virtuels avec plusieurs cartes réseau
- Configurer une carte réseau sur chaque membre de nœud pour utiliser un commutateur de réseau privé partagé
- Configurer le cluster NLB pour utiliser le mode monodiffusion
- Utiliser le commutateur de réseau privé partagé pour la communication des clusters
- Lorsque les nœuds NLB couvrent plusieurs sites, utiliser la virtualisation de réseau pour séparer le réseau de clusters

Placement d'un ordinateur virtuel

Vous devriez placer des nœuds de cluster NLB sur les disques durs distincts sur l'hôte Hyper-V. De cette façon, si un disque ou une baie de disques, même si un nœud devient indisponible, d'autres nœuds de cluster NLB qui sont hébergés sur le même hôte Hyper-V resteront en ligne. Comme recommandation, vous devriez configurer l'hôte Hyper-V avec le matériel redondant, notamment les disques redondants, les cartes réseau et les alimentations. Cela permet d'éviter qu'une défaillance matérielle sur l'hôte Hyper-V rende tous les nœuds d'un cluster NLB indisponible. Lorsque vous utilisez plusieurs cartes réseau, configurez la mise en équipe des cartes réseau pour vous assurer que les ordinateurs virtuels peuvent maintenir l'accès au réseau même si chaque carte réseau présente une défaillance.

Dans la mesure du possible, déployez les nœuds d'ordinateur virtuel NLB sur les hôtes hyper-V distincts. Si vous planifiez ce type de configuration, assurez-vous que les ordinateurs virtuels qui font partie du cluster NLB sont situés sur le même sous-réseau TCP/IP. Ceci protège le cluster NLB d'autres types de défaillance serveur, tels que la défaillance d'une carte mère ou tout autre point de défaillance unique.

Configuration réseau des ordinateurs virtuels

Puisque l'ajout de cartes réseau virtuelles supplémentaires est un processus simple, vous pouvez configurer le cluster NLB pour utiliser le mode monodiffusion, puis déployer chaque ordinateur virtuel avec plusieurs cartes réseau. Vous devez créer des commutateurs virtuels distincts pour le trafic de cluster et le trafic de gestion des nœuds, parce que la segmentation du trafic peut améliorer les performances. Vous pouvez également utiliser la virtualisation de réseau pour partitionner le trafic de cluster à partir du trafic de gestion des nœuds. Vous pouvez utiliser des balises VLAN en guise de méthode de partitionnement du trafic de cluster à partir du trafic de gestion des nœuds.

Lorsque vous utilisez le mode monodiffusion, assurez-vous que vous activez l'usurpation d'adresse MAC pour la carte réseau virtuelle de l'hôte Hyper-V. Pour cela, modifiez les paramètres de la carte réseau virtuelle dans la boîte de dialogue **Paramètres de l'ordinateur virtuel**, qui est disponible via le Gestionnaire Hyper-V. L'activation de l'usurpation d'adresse MAC permet au mode monodiffusion de configurer l'attribution d'adresse MAC sur la carte réseau virtuelle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comparaison entre le cluster NLB et la haute disponibilité d'ordinateur virtuel

La haute disponibilité d'ordinateur virtuel est le processus qui consiste à placer des ordinateurs virtuels sur des clusters de basculement. Lorsqu'un nœud de cluster de basculement échoue, l'ordinateur virtuel bascule de sorte qu'il soit hébergé sur un autre nœud. Bien que le clustering avec basculement et NLB soient tous deux des technologies de disponibilité, ils servent des objectifs différents. Le clustering avec basculement prend en charge des applications avec état telles que SQL Server, tandis que NLB est adapté aux applications sans état telles que les sites Web. Les ordinateurs virtuels hautement disponibles ne permettent pas de mettre à l'échelle une application, parce que vous ne pouvez pas ajouter des nœuds à la capacité d'augmentation. Cependant, il est possible de déployer des nœuds de cluster NLB en tant qu'ordinateurs virtuels hautement disponibles. Dans ce scénario, les nœuds de cluster NLB basculent vers un nouvel hôte Hyper-V en cas d'échec de l'hôte Hyper-V d'origine.

Le degré de disponibilité et de redondance requis fluctue en fonction de l'application. Une application vitale pour l'entreprise qui coûte à une organisation des millions de dollars en cas de défaillance requiert une disponibilité qui diffère de celle d'une application qui provoque une gêne minimale hors connexion.

Éléments à prendre en compte pour la sécurisation NLB

Les clusters NLB sont presque toujours utilisés pour héberger les applications Web qui sont importantes pour l'organisation. En raison de cette importance, vous devriez prendre des mesures pour sécuriser NLB, à la fois en restreignant le trafic qui peut s'adresser au cluster et en vérifiant que les autorisations appropriées sont appliquées.

- Utiliser les règles de port de cluster NLB pour ignorer le trafic non lié aux applications de cluster
- Utiliser les règles de pare-feu sur des nœuds de cluster pour abandonner le trafic non lié aux applications de cluster ou à la gestion des nœuds
- Configurer les applications pour répondre uniquement au trafic adressé au cluster
- Utiliser les réseaux de zone de stockage pour créer les certificats qui prennent en charge le nom d'application et les noms de nœuds
- Implémenter le principe des privilèges minimum pour s'assurer que seuls les utilisateurs autorisés disposent des autorisations appropriées sur les nœuds

Configurer les règles de port

En sécurisant les clusters NLB, vous devez d'abord vérifier que vous créez des règles de port pour bloquer le trafic sur tous les ports autres que ceux utilisés par les applications hébergées sur le cluster NLB. En faisant cela, tout le trafic entrant qui n'est pas adressé spécifiquement aux applications s'exécutant sur le cluster NLB sera ignoré. Si vous ne passez pas par cette première étape, tout le trafic entrant qui n'est pas géré par une règle de port sera transféré au nœud de cluster avec la priorité la plus basse du cluster.

Configurer les règles de pare-feu

Vous devriez également vérifier que le pare-feu Windows avec fonctions de sécurité avancées est configuré sur chaque nœud de cluster NLB. Quand vous activez NLB sur un nœud de cluster, les règles suivantes de pare-feu qui permettent à NLB de fonctionner et de communiquer avec d'autres nœuds du cluster sont créées et activées automatiquement :

- Équilibrage de la charge réseau (DCOM-In).
- Équilibrage de la charge réseau (ICMP4-ERQ-In)
- Équilibrage de la charge réseau (ICMP6-ERQ-In)
- Équilibrage de la charge réseau (RPCSS)
- Équilibrage de la charge réseau (WinMgmt-In)
- Équilibrage de la charge réseau (ICMP4-DU-In)

- Équilibrage de la charge réseau (ICMP4-ER-In)
- Équilibrage de la charge réseau (ICMP6-DU-In)
- Équilibrage de la charge réseau (ICMP6-EU-In)

Une fois créées, ces règles de pare-feu ne comprennent pas des paramètres de portée. Dans des environnements de sécurité élevée, vous configureriez une adresse IP locale ou une plage d'adresses IP appropriée, ainsi qu'une adresse IP distante pour chacune de ces règles. L'adresse IP distante ou la plage d'adresses devrait comprendre les adresses qui sont utilisées par d'autres hôtes du cluster.

Quand vous configurez des règles de pare-feu supplémentaires, souvenez-vous de ce qui suit :

- Quand vous utilisez plusieurs cartes réseau dans le mode monodiffusion, configurez les différentes règles de pare-feu pour chaque interface réseau. Pour l'interface utilisée pour des tâches de gestion, vous devez configurer les règles de pare-feu pour autoriser le trafic entrant de gestion uniquement, par exemple, en activant l'utilisation de Windows PowerShell à distance, Windows Remote Management (WinRM) et le Bureau à distance pour des tâches de gestion. Vous devez configurer les règles de pare-feu sur l'interface réseau utilisée par le nœud de cluster, pour fournir une application au cluster et pour permettre l'accès à cette application. Par exemple, autorisez le trafic entrant sur les ports TCP 80 et 443 sur une application qui utilise les protocoles HTTP et HTTPS.
- Si vous utilisez plusieurs cartes réseau en mode de multidiffusion, configurez les règles de pare-feu qui permettent l'accès aux applications qui sont hébergées sur le cluster, mais bloquez l'accès aux autres ports.

Configurer les applications pour répondre uniquement au trafic adressé au cluster

Vous devez configurer les applications sur chaque nœud pour répondre uniquement au trafic qui est adressé au cluster et ignorer le trafic d'application qui est adressé à chaque nœud. Par exemple, si vous déployez une application Web qui est conçue pour répondre au trafic adressé à www.adatum.com, il y aura un site Web sur chaque nœud qui acceptera le trafic sur le port 80. Selon la configuration de cluster NLB, il est possible que le trafic qui est adressé au nœud sur le port 80 génère une réponse directe. Par exemple, les utilisateurs peuvent accéder à l'application Web de la société A. Datum en entrant l'adresse http://nlb-node-3.adatum.com dans un navigateur, au lieu d'entrer l'adresse http://www.adatum.com. Vous pouvez sécuriser les applications de ce type de trafic direct en les configurant pour répondre uniquement au trafic qui utilise l'adresse de cluster NLB. Pour les applications Web, vous pouvez le faire en configurant le site Web pour utiliser un en-tête d'hôte. Chaque application qui s'exécute sur un cluster NLB aura sa propre méthode unique vous permettant de configurer l'application en vue de répondre uniquement au trafic dirigé vers le cluster, plutôt que vers chaque nœud de cluster.

Sécurisation du trafic avec SSL

Les sites Web NLB doivent tous utiliser le même nom de site Web. Quand vous sécurisez les sites Web que vous rendez hautement disponibles à l'aide de NLB, vous devez vérifier que chaque site Web a un certificat SSL qui correspond au nom de site Web. Vous pouvez utiliser des en-têtes d'hôte sur chaque nœud. Dans la plupart des cas, vous installerez le même certificat de site Web sur chaque nœud du cluster NLB, parce que cette procédure est plus simple que d'obtenir des certificats distincts pour chaque nœud de cluster. Dans certains cas, vous devrez obtenir les certificats qui prennent en charge d'autres noms de l'objet. Les certificats qui les prennent en charge permettent à plusieurs noms d'identifier un serveur, comme le nom utilisé par l'application en cluster et le nom du nœud de cluster. Par exemple, un certificat avec un autre nom d'objet peut prendre en charge les noms www.adatum.com, node1.adatum.com, node2.adatum.com, node3.adatum.com et node4.adatum.internal.

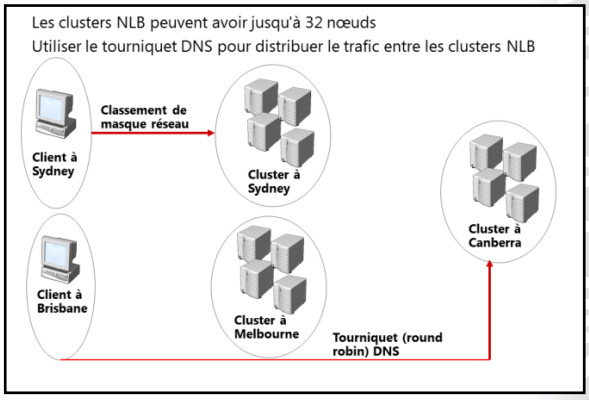
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Principe des privilèges minimum

Assurez-vous que les utilisateurs disposent uniquement des autorisations déléguées pour les tâches qu'ils doivent effectuer sur le nœud NLB. Les membres du cluster d'administrateurs locaux sur n'importe quel nœud unique peuvent ajouter et supprimer des nœuds de cluster, même si ils ne sont pas membres du cluster d'administrateurs locaux sur ces nœuds. Les applications qui s'exécutent sur des clusters NLB doivent être configurées de telle manière qu'elles n'exigent pas des administrateurs d'application l'obtention de privilèges d'administrateur local sur les serveurs qui hébergent l'application. Seuls les utilisateurs dont le rôle de travail exige d'eux de pouvoir établir des rapports de gestion à distance sur les nœuds de cluster NLB, doivent pouvoir établir ces connexions.

Considérations relatives à la mise à l'échelle NLB

La mise à l'échelle est le processus consistant à augmenter la capacité d'un cluster NLB. Par exemple, si vous avez un cluster NLB de quatre nœuds et chaque nœud du cluster est fortement utilisé au point où le cluster ne peut plus gérer le trafic, vous pouvez ajouter des nœuds supplémentaires. L'ajout de nœuds répartira la même charge entre plusieurs ordinateurs, réduisant la charge sur chaque nœud de cluster actuel. La capacité augmente parce qu'un plus grand nombre d'ordinateurs configurés de manière identique peut gérer une charge de travail plus élevée qu'un nombre inférieur d'ordinateurs pareillement configurés.



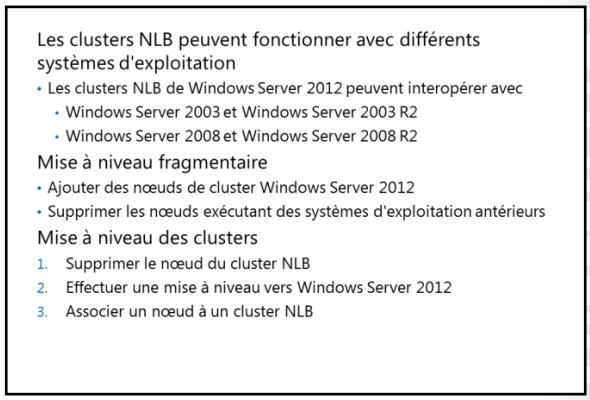
Un cluster NLB peut prendre en charge jusqu'à 32 nœuds. Cela signifie que vous pouvez monter en puissance parallèle un cluster NLB unique de sorte que 32 nœuds distincts fassent partie de ce cluster. Lorsque vous envisagez de mettre une application à l'échelle de sorte qu'elle soit hébergée sur un cluster NLB de 32 nœuds, souvenez-vous que chaque nœud du cluster doit être sur le même sous-réseau TCP/IP.

Une alternative à générer les clusters NLB unique consiste à établir plusieurs clusters NLB, puis à utiliser le tourniquet DNS pour partager le trafic entre eux. Le tourniquet DNS est une technologie qui permet à un serveur DNS de fournir aux clients en faisant la demande différentes adresses IP au même nom d'hôte, dans un ordre séquentiel. Par exemple, s'il existe trois adresses associées à un nom d'hôte, le premier hôte qui en fait la demande reçoit la première adresse, le deuxième reçoit la deuxième adresse et le troisième reçoit la troisième adresse, et ainsi de suite. Lorsque vous utilisez le tourniquet DNS avec NLB, vous associez les adresses IP de chaque cluster avec le nom d'hôte qui est utilisé par l'application.

La distribution du trafic entre les clusters NLB utilisant le tourniquet DNS vous permet également de déployer des clusters NLB entre plusieurs sites. Le tourniquet DNS prend en charge le tri de masques réseau. Cette technologie assure que les clients d'un sous-réseau sont dotés d'une adresse IP d'un hôte sur le même réseau, en cas de disponibilité. Par exemple, vous pouvez déployer trois clusters NLB de quatre nœuds dans les villes de Sydney, Melbourne et Canberra, et utiliser le tourniquet DNS pour distribuer le trafic entre eux. Avec le tri de masques réseau, un client qui accède à l'application depuis Sydney sera dirigé vers le cluster NLB hébergé à Sydney. Un client qui n'est pas sur le même sous-réseau que les nœuds de cluster NLB, comme un client dans la ville de Brisbane, sera dirigé par tourniquet DNS vers le cluster NLB de Sydney, Melbourne ou Canberra.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Remarques relatives à la mise à niveau des clusters NLB



La mise à niveau des clusters NLB implique le déplacement des nœuds de cluster d'un système d'exploitation hôte, par exemple Windows Server 2003 ou Windows Server 2008, vers Windows Server 2012. La mise à niveau du cluster ne peut pas sous-entendre une mise à niveau du système d'exploitation sur chaque nœud, parce que dans certains cas le système d'exploitation hôte d'origine ne peut pas prendre en charge une mise à niveau directe vers Windows Server 2012. Dans les cas où le système d'exploitation hôte d'origine ne prend pas en charge une mise à niveau directe vers Windows Server 2012, vous pourrez exécuter une migration.

Un élément principal à prendre en considération lorsque vous mettez des clusters NLB à niveau est de toujours garder à l'esprit que NLB prend en charge les clusters qui exécutent une association de systèmes d'exploitation. Cela signifie que vous pouvez avoir un cluster exécutant une association de Windows Server 2003, de Windows Server 2008 et de Windows Server 2012. Gardez à l'esprit que, bien que les clusters NLB de systèmes d'exploitation mixtes sont pris en charge, ils ne sont pas recommandés. Vous devriez configurer le cluster NLB de sorte que tous les hôtes exécutent le même système d'exploitation dès que possible.

Remarque : Dans certaines situations, il ne sera pas possible de mettre le système d'exploitation à niveau d'un nœud de cluster.

Lorsque vous effectuez une mise à niveau, vous pouvez utiliser une des stratégies suivantes :

- Mise à niveau fragmentaire. Dans ce type de mise à niveau, vous ajoutez de nouveaux nœuds Windows Server 2012 à un cluster existant, puis supprimez les nœuds qui exécutent des versions antérieures du système d'exploitation Windows Server. Ce type de mise à niveau est approprié si le matériel et le système d'exploitation d'origine ne prennent pas en charge une mise à niveau directe vers Windows Server 2012.
- Mise à niveau propagée. Dans ce type de mise à niveau, vous mettez à niveau chaque nœud du cluster tour à tour. Pour cela, utilisez le nœud hors connexion, effectuez la mise à niveau, puis replacez le nœud dans le cluster.

Liens de référence : Pour plus d'informations sur la mise à niveau des clusters NLB, consultez http://go.microsoft.com/fwlink/?LinkId=270037.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation de l'équilibrage de la charge réseau

Scénario

A. Datum Corporation est une société d'ingénierie et de fabrication. L'organisation est basée à Londres (Angleterre) et s'est rapidement développée en Australie. Comme la société développe, le besoin en applications Web évolutives a augmenté. À cet effet, vous développez un programme pilote pour tester le déploiement de NLB sur les hôtes exécutant le système d'exploitation Windows Server 2012.

Comme vous avez l'intention d'automatiser le processus de déploiement des clusters NLB de Windows, vous utiliserez Windows PowerShell pour effectuer de nombreuses tâches d'installation et de configuration de clusters. Vous configurerez également les règles de port et l'affinité, qui vous permettront de déployer plusieurs applications Web à charge équilibrée sur les mêmes clusters NLB de Windows.

Objectifs

- Implémenter un cluster NLB.
- Configurer et gérer un cluster NLB.
- Valider la haute disponibilité pour le cluster NLB

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-SVR2**
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd.

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**.
5. Répétez les étapes 2 à 4 pour **22412B-LON-SVR1** et **22412B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Implémentation d'un cluster d'équilibrage de la charge réseau

Scénario

Vous souhaitez par la suite automatiser le processus de déploiement des clusters NLB de Windows Server 2012. À cet effet, vous utiliserez Windows PowerShell pour effectuer la majorité des tâches de déploiement de clusters NLB.

Les tâches principales de cet exercice sont les suivantes :

1. Vérifier la fonctionnalité de site Web pour les serveurs autonomes
2. Installer l'équilibrage de la charge réseau (NLB)
3. Créer un nouveau cluster NLB dans Windows Server 2012
4. Ajouter un deuxième hôte au cluster
5. Valider le cluster NLB

▶ Tâche 1 : Vérifier la fonctionnalité de site Web pour les serveurs autonomes

1. Sur LON-SVR1, accédez au dossier **c:\inetpub\wwwroot**.
2. Ouvrez **iis-8** dans Microsoft Paint et utilisez le pinceau de peinture et la couleur rouge pour différencier le logo IIS.
3. Fermez l'Explorateur de fichiers.
4. Basculez vers l'ordinateur **LON-DC1**, puis ouvrez l'**Explorateur de fichiers**.
5. Naviguez vers **http://LON-SVR1** et vérifiez que la page Web est différenciée par la couleur rouge.
6. Naviguez vers **http://LON-SVR2** et vérifiez que le site Web n'est pas différencié par la couleur rouge.
7. Fermez Internet Explorer.

▶ Tâche 2 : Installer l'équilibrage de la charge réseau (NLB)

1. Sur LON-SVR1, ouvrez **Windows PowerShell ISE**.
2. Tapez la commande suivante, puis appuyez sur Entrée :

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-
WindowsFeature NLB,RSAT-NLB}
```

▶ Tâche 3 : Créer un nouveau cluster NLB dans Windows Server 2012

1. Sur LON-SVR1, dans Windows PowerShell ISE, tapez la commande suivante et appuyez sur Entrée :

```
New-NlbCluster -InterfaceName "Connexion au réseau local" -OperationMode Multicast
-ClusterPrimaryIP 172.16.0.42 -ClusterName LON-NLB
```

2. Dans Windows PowerShell ISE, tapez la commande suivante et appuyez sur Entrée :

```
Invoke-Command -Computername LON-DC1 -command {Add-DNSServerResourceRecordA
–zonename adatum.com –name LON-NLB –Ipv4Address 172.16.0.42}
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Ajouter un deuxième hôte au cluster

- Sur LON-SVR1, dans Windows PowerShell ISE, tapez la commande suivante et appuyez sur Entrée :

```
Add-NlbClusterNode -InterfaceName "Connexion au réseau local" -NewNodeName "LON-SVR2"
-NewNodeInterface "Connexion au réseau local"
```

▶ Tâche 5 : Valider le cluster NLB

1. Sur LON-SVR1, ouvrez le Gestionnaire d'équilibrage de la charge réseau et vérifiez que les nœuds LON-SVR1 et LON-SVR2 s'affichent avec l'état **Convergé**.
2. Affichez les propriétés du cluster LON-NLB et vérifiez ce qui suit :
   - Le cluster est défini pour utiliser le mode d'opérations **Multidiffusion**.
   - Il existe une règle de port unique nommée **Tous** qui commence au port **0** et se termine au port **65535** pour les protocoles **TCP** et **UDP**, et qui utilise l'affinité **Unique**.

Résultats : À la fin de cet exercice, vous aurez implémenté un cluster NLB avec succès.

Exercice 2 : Configuration et gestion d'un cluster NLB

Scénario

Vous souhaitez déployer des sites Web distincts sur le cluster NLB, puis différencier ces sites Web selon l'adresse du port. Pour cela, vous souhaitez avoir l'assurance que vous pouvez configurer et valider des règles de port. Vous souhaitez également expérimenter des paramètres d'affinité pour garantir que les demandes sont distribuées de manière équitable entre les hôtes.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les règles et l'affinité de port
2. Valider les règles de port
3. Gérer la disponibilité hôte dans le cluster NLB

▶ Tâche 1 : Configurer les règles et l'affinité de port

1. Sur LON-SVR2, ouvrez **Windows PowerShell**.
2. Dans Windows PowerShell, entrez les commandes suivantes, en appuyant sur Entrée après chaque commande :

```
Cmd.exe
Mkdir c:\porttest
Xcopy /s c:\inetpub\wwwroot c:\porttest
Exit
New-Website -Name PortTest -PhysicalPath "C:\porttest" -Port 5678
New-NetFirewallRule -DisplayName PortTest -Protocol TCP -LocalPort 5678
```

3. Ouvrez l'**Explorateur de fichiers**, puis accédez et ouvrez le fichier **c:\porttest\iis-8.png** dans Microsoft Paint.
4. Utilisez le pinceau **Bleu** pour différencier le logo IIS.
5. Basculez vers **LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Ouvrez Internet Explorer et accédez à **http://LON-SVR2:5678**.
7. Vérifiez que la page de **démarrage** IIS comportant l'image soit identifiée par les marquages bleus.
8. Basculez vers **LON-SVR1**.
9. Sur LON-SVR1, ouvrez le **Gestionnaire d'équilibrage de la charge de réseau** et affichez les propriétés de cluster de LON-NLB.
10. Supprimez la règle **Tous**.
11. Ajoutez une règle de port ayant les propriétés suivantes :
    - Étendue du port : **80 à 80**
    - Protocoles : **Les deux**
    - Mode de filtrage : **Hôte multiple**
    - Affinité : **Aucun**
12. Créez une nouvelle règle de port ayant les propriétés suivantes :
    - Étendue du port : **5678 à 5678**
    - Protocoles : **Les deux**
    - Mode de filtrage : **Hôte unique**
13. Fermez la boîte de dialogue **Propriétés du cluster**.
14. Modifiez les propriétés hôte de LON-SVR1.
15. Configurez la valeur de la **Priorité de traitement** de la règle du port **5678** sur **10**.

▶ Tâche 2 : Valider les règles de port

1. Basculez vers **LON-DC1**.
2. En utilisant Internet Explorer, accédez à **http://lon-nlb**, actualisez la page Web **20** fois et vérifiez que les pages Web avec et sans le marquage rouge de différenciation s'affichent correctement.
3. Sur LON-DC1, naviguez pour adresser **http://LON-NLB:5678**, actualisez la page Web **20** fois et vérifiez que seule la page Web avec le marquage bleu de différenciation s'affiche.

▶ Tâche 3 : Gérer la disponibilité hôte dans le cluster NLB

1. Basculez vers **LON-SVR1**.
2. Sur LON-SVR1, utilisez le Gestionnaire d'équilibrage de la charge réseau pour interrompre LON-SVR1.
3. Vérifiez que le nœud LON-SVR1 s'affiche à l'état **Exécution suspendue** et que le nœud LON-SVR2 s'affiche à l'état **Convergé**.
4. Reprenez, puis démarrez **LON-SVR1**.
5. Vérifiez que les deux nœuds LON-SVR1 et LON-SVR2 s'affichent maintenant à l'état **Convergé**.

Résultats : À la fin de cet exercice, vous aurez configuré et géré un cluster NLB avec succès.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Validation de la haute disponibilité pour le cluster NLB

Scénario

Dans le cadre de la préparation au déploiement de NLB dans l'environnement de votre organisation, vous souhaitez vérifier qu'il est possible d'effectuer des tâches de maintenance (telles que des opérations de redémarrage), sans affecter la disponibilité des sites Web qui sont hébergés sur le cluster. À cet effet, vous vérifierez la disponibilité en redémarrant un des hôtes tout en tentant d'accéder au site Web en cluster. Vous explorerez également la fonctionnalité Drainer et arrêter.

Les tâches principales de cet exercice sont les suivantes :

1. Valider la disponibilité de site Web lorsque l'hôte est indisponible
2. Configurer et valider une action Drainer et arrêter

▶ Tâche 1 : Valider la disponibilité de site Web lorsque l'hôte est indisponible

1. Redémarrez **LON-SVR1**.
2. Basculez vers **LON-DC1**.
3. Sur LON-DC1, ouvrez **Internet Explorer** et accédez à **http://LON-NLB**.
4. Actualisez le site Web **20** fois. Vérifiez que le site Web est disponible, mais qu'il n'affiche pas la marque de différenciation rouge sur le logo IIS jusqu'au redémarrage de LON-SVR1.

▶ Tâche 2 : Configurer et valider une action Drainer et arrêter

1. Sur LON-SVR1, ouvrez le **Gestionnaire d'équilibrage de charge de réseau** et lancez une action Drainer et arrêter sur LON-SVR2.
2. Sur LON-DC1, accédez à **http://lon-nlb** et vérifiez que seule la page d'accueil avec le logo IIS rouge s'affiche.

Résultats : À la fin de cet exercice, vous aurez réussi à valider une haute disponibilité pour le cluster NLB.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste Ordinateurs virtuels, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1** et **22412B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Vous avez créé un cluster NLB de Windows Server 2012 comportant quatre nœuds. Le cluster héberge un site Web qui est hébergé sur IIS. Quels sont les conséquences sur le cluster si vous arrêtez le service de publication World Wide Web sur l'un des nœuds ?

Question : Vous souhaitez héberger les sites Web www.contoso.com, www.adatum.com et www.fabrikam.com sur un cluster NLB de quatre nœuds. L'adresse IP du cluster sera une adresse IP publique et chaque nom de domaine complet est mappé dans le DNS à l'adresse IP publique du cluster. Quelles mesures devez-vous appliquer à chaque nœud pour vérifier que le trafic est dirigé vers le site approprié ?

Question : Vous avez un cluster NLB de Windows de huit nœuds qui héberge une application Web. Vous souhaitez vous assurer que le trafic d'un client qui utilise le cluster demeure dans le même nœud au cours de la session, mais que le trafic des clients distincts est distribué équitablement entre tous les nœuds. Quelle option configurez-vous pour atteindre cet objectif ?

Problèmes réels et scénarios

Pour obtenir une véritable solution de haute disponibilité, utilisez une solution de surveillance avec NLB qui détectera la défaillance d'application. Cela est lié au fait que les clusters NLB continueront à diriger le trafic direct vers les nœuds avec des applications défaillantes si NLB, qui est indépendant de l'application, continue à envoyer le trafic de pulsation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10

Implémentation du clustering avec basculement

Table des matières :

Vue d'ensemble du module **10-1**

Leçon 1 : Vue d'ensemble du clustering avec basculement **10-2**

Leçon 2 : Implémentation d'un cluster de basculement **10-16**

Leçon 3 : Configuration d'applications et de services hautement disponibles sur un cluster de basculement **10-23**

Leçon 4 : Maintenance d'un cluster de basculement **10-29**

Leçon 5 : Implémentation d'un cluster de basculement multisite **10-36**

Atelier pratique : Implémentation du clustering avec basculement **10-42**

Contrôle des acquis et éléments à retenir **10-49**

Vue d'ensemble du module

Toute organisation souhaitant garantir la continuité de ses services auprès de ses utilisateurs doit maintenir une haute disponibilité. La haute disponibilité est un terme qui qualifie la capacité pour un système ou un périphérique à être utilisé dès que nécessaire. Vous pouvez exprimer la haute disponibilité en pourcentage, qui est calculé en divisant le temps de service réel par le temps de service requis. La haute disponibilité ne signifie pas que le système sera exempt de temps d'interruption. Cependant, un réseau qui a un temps de bon fonctionnement de 99,999 % est souvent considéré hautement disponible.

Le clustering avec basculement est l'une des principales technologies de Windows Server® 2012 qui peut garantir la haute disponibilité d'applications et de services divers. Dans ce module, vous allez découvrir ce qu'est le clustering avec basculement, ses composants, ainsi que ses techniques d'implémentation.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire le clustering avec basculement ;
- implémenter un cluster de basculement ;
- configurer des applications et des services à haut niveau de disponibilité ;
- assurer la maintenance d'un cluster de basculement ;
- implémenter un clustering avec basculement multisite.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble du clustering avec basculement

Le clustering avec basculement est un processus de haute disponibilité, où une instance d'un service ou d'une application en cours d'exécution sur un ordinateur peut échouer sur un autre ordinateur dans le cluster de basculement si le premier ordinateur échoue. Dans Windows Server 2012, les clusters de basculement fournissent une solution haute disponibilité pour de nombreux rôles de serveurs et applications. En implémentant des clusters de basculement, vous pouvez maintenir la disponibilité des applications ou des services dans le cas où un ou plusieurs ordinateurs du cluster de basculement venaient à échouer.

Pour implémenter le clustering avec basculement, vous devez bien connaître les principaux concepts relatifs à la haute disponibilité. Vous devez également comprendre la terminologie de clustering et savoir comment fonctionnent les clusters de basculement. Enfin, vous devez vous familiariser avec les nouvelles fonctionnalités de clustering dans Windows Server 2012.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

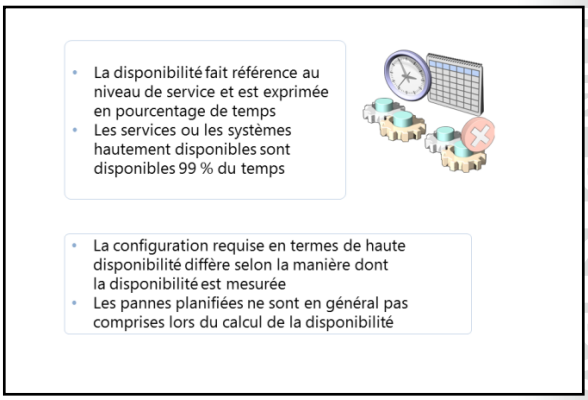
- décrire la haute disponibilité ;
- décrire les améliorations relatives au clustering avec basculement dans Windows Server 2012 ;
- décrire les composants de cluster de basculement ;
- décrire les volumes partagés de cluster (CSV) ;
- définir les principes de basculement et de restauration automatique ;
- décrire un quorum ;
- décrire les modes de quorum dans les clusters de basculement de Windows Server 2012 ;
- décrire les réseaux de cluster de basculement ;
- décrire l'espace du cluster de basculement ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que la haute disponibilité ?

La disponibilité fait référence au niveau de service fourni par les applications, les services ou les systèmes. La disponibilité est exprimée sous forme de pourcentage de la durée de disponibilité d'un service ou système. Les systèmes à haut niveau de disponibilité ont un temps mort minimal (planifié ou non) et sont disponibles plus de 99 % du temps, selon les besoins et le budget de l'organisation. Par exemple, un système qui n'est pas disponible pendant 8,75 heures par an présente un taux de disponibilité de 99,9 %, et serait considéré comme hautement disponible.



Pour améliorer la disponibilité, vous devez implémenter des mécanismes de tolérance de panne visant à masquer ou minimiser l'impact des défaillances sur les composants et les dépendances du service sur le système. La tolérance de panne peut être obtenue en implémentant la redondance des points de défaillance uniques.

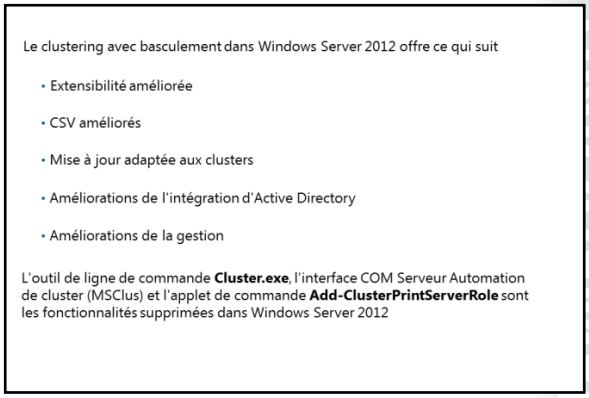
Toute mésentente entre le client et l'organisation informatique concernant les exigences de niveau de service peut être la cause de mauvaises décisions commerciales, ce qui risque d'entraîner des niveaux d'investissement inadéquats et le mécontentement des clients. Veillez à exprimer clairement les exigences de disponibilité afin d'éviter tout malentendu quant aux conséquences.

La période d'évaluation de la disponibilité peut également avoir un impact significatif sur la définition de la disponibilité. Par exemple, une exigence de disponibilité de 99,9 % pour une durée d'un an permet 8,75 heures de temps mort, tandis qu'une exigence de disponibilité de 99,9 % sur une période de quatre semaines consécutives permet uniquement une indisponibilité de 40 minutes pendant chaque période.

Pour la haute disponibilité, vous devriez également identifier et négocier les pannes planifiées, les heures de service et support, les activités de maintenance, les mises à jour de Service Pack et les mises à jour logicielles. Celles-ci sont considérées comme des pannes planifiées et ne sont généralement pas comprises comme des temps d'interruption. Normalement, vous calculez la disponibilité en fonction des pannes non planifiées uniquement. Cependant, vous devez négocier exactement quelles pannes planifiées seront considérées comme un temps mort.

Clustering avec basculement dans Windows Server 2012

La plupart des fonctionnalités du clustering avec basculement et des techniques d'administration de Windows Server 2008 R2 sont présentes dans Windows Server 2012. Cependant, certaines nouvelles fonctionnalités et technologies de Windows Server 2012 augmentent l'extensibilité et la disponibilité de l'espace de stockage en cluster, et fournissent une gestion améliorée et simplifiée, ainsi qu'un basculement plus rapide.



Les nouvelles fonctionnalités importantes du clustering avec basculement dans Windows Server 2012 sont les suivantes :

- Extensibilité améliorée. Dans Windows Server 2012, un cluster de basculement peut avoir 64 nœuds physiques et peut exécuter 4 000 ordinateurs virtuels sur chaque cluster. C'est une amélioration considérable par rapport à Windows Server 2008 R2 qui ne prend en charge que 16 nœuds physiques et 1 000 ordinateurs virtuels par cluster. Chaque cluster que vous créez est maintenant disponible à partir de la console Gestionnaire de serveur. Le Gestionnaire de serveur dans Windows Server 2012 peut découvrir et gérer tous les clusters créés dans un domaine des services de domaine Active Directory® (AD DS). Si vous déployez le cluster dans un scénario multisite, l'administrateur peut désormais contrôler quels nœuds d'un cluster ont des votes pour établir le quorum. L'extensibilité du clustering avec basculement est également améliorée pour les ordinateurs virtuels qui s'exécutent sur des clusters. Il fera l'objet d'une description détaillée plus loin dans ce cours.
- Volumes partagés de cluster (CSV) améliorés. Cette technologie a été introduite dans Windows Server 2008 R2, et est devenue très populaire pour fournir l'espace de stockage de l'ordinateur virtuel. Dans Windows Server 2012, les volumes CSV apparaissent comme des systèmes de fichiers CSV et prennent en charge le stockage SMB (Server Message Block) version 3.0 pour Hyper-V® et d'autres applications. En outre, un volume CSV peut utiliser les fonctionnalités SMB Multichannel et SMB Direct pour permettre au trafic de diffuser en continu sur plusieurs réseaux au sein d'un cluster. Il est également possible d'implémenter le serveur de fichiers sur les volumes CSV, en mode avec montée en puissance parallèle. Pour une sécurité renforcée, vous pouvez utiliser le chiffrement de lecteur Windows® BitLocker® pour des disques CSV, et vous pouvez également rendre le stockage CSV visible uniquement à un sous-ensemble de nœuds d'un cluster. À des fins de fiabilité, vous pouvez analyser et réparer les volumes CSV sans temps hors connexion.
- Mise à jour adaptée aux clusters. Dans les versions antérieures de Windows Server, la mise à jour des nœuds de cluster nécessitait une longue période de préparation et de planification, afin de réduire ou d'éviter le temps mort. En outre, la procédure de mise à jour des nœuds de cluster était une procédure en grande partie manuelle, ce qui entraînait des tâches administratives supplémentaires. Windows Server 2012 présente la mise à jour adaptée aux clusters, une nouvelle technologie à cet effet. Cette technologie met automatiquement à jour les nœuds de cluster avec le correctif logiciel Windows Update, en maintenant le cluster en ligne et en réduisant le temps mort. Cette technologie sera décrite plus en détail dans la « Leçon 4 : Maintenance d'un cluster de basculement. »
- Améliorations de l'intégration d'Active Directory. Dans Windows Server 2008, le clustering avec basculement est intégré dans AD DS. Dans Windows Server 2012, cette intégration a été améliorée. Les administrateurs peuvent maintenant créer des objets ordinateur de cluster dans des unités d'organisation ciblées, ou par défaut dans les mêmes unités d'organisation que les nœuds de cluster. Cette conception fait coïncider les dépendances de cluster de basculement sur AD DS avec le modèle d'administration de domaine délégué qui est utilisé dans de nombreuses organisations informatiques. En outre, vous pouvez à présent déployer les clusters de basculement avec un accès uniquement aux contrôleurs de domaine en lecture seule.
- Améliorations de la gestion. Bien que le clustering avec basculement dans Windows Server 2012 utilise toujours quasiment la même console de gestion et les mêmes techniques administratives, Windows Server 2012 apporte quelques améliorations importantes en matière de gestion. L'Assistant Validation est amélioré, la vitesse de validation pour de grands clusters de basculement est optimisée et de nouveaux tests pour CSV, le rôle Hyper-V et des ordinateurs virtuels ont été ajoutés. De nouveaux applets de commande Windows PowerShell® sont par ailleurs disponibles pour gérer les clusters, surveiller les applications d'ordinateur virtuel en cluster et créer des cibles Internet Small Computer System Interface (iSCSI) à haut niveau de disponibilité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

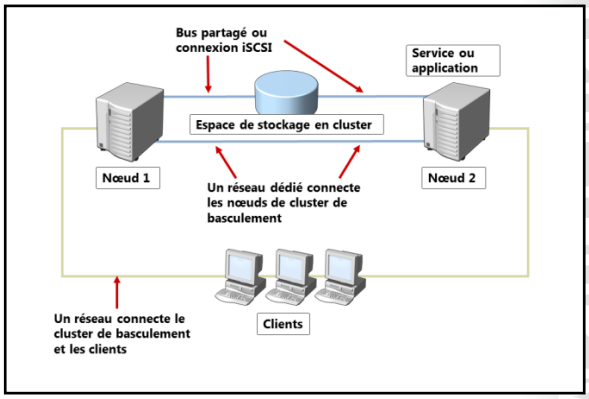
Fonctionnalités supprimées et déconseillées

Dans le clustering Windows Server 2012, certaines des fonctionnalités des versions de clustering avec basculement antérieures sont supprimées ou déconseillées. Si vous effectuez une mise à niveau à partir d'une version antérieure, vous devez être conscient des changements suivants :

- L'outil de ligne de commande Cluster.exe est supprimé. Cependant, vous pouvez éventuellement l'installer avec les outils de clustering avec basculement. Les applets de commande Windows PowerShell de clustering avec basculement fournissent une fonctionnalité généralement identique aux commandes Cluster.exe.
- L'interface Component Object Model (COM) du Serveur Automation de cluster de basculement (MSClus) est supprimée, mais vous pouvez éventuellement l'installer avec les outils de clustering avec basculement.
- La prise en charge des DLL de ressource de cluster 32 bits est déconseillée, mais des DLL 32 bits peuvent éventuellement être installées. Les DLL de ressource de cluster doivent être mises à jour sur 64 bits.
- Le rôle Serveur d'impression a été supprimé de l'Assistant Haute disponibilité, et ne peut pas être configuré dans le Gestionnaire du cluster de basculement.
- L'applet de commande **Add-ClusterPrintServerRole** est supprimée et elle n'est pas prise en charge dans Windows Server 2012.

Composants de cluster de basculement

Un cluster de basculement est un groupe d'ordinateurs indépendants qui fonctionnent ensemble afin d'augmenter la disponibilité des applications et des services. Les câbles physiques et les logiciels connectent les serveurs de cluster. Les serveurs qui font partie du cluster sont également appelés *nœuds*. Si l'un des nœuds de cluster subit une défaillance, un autre nœud commence à assurer les services. Ce processus est appelé *basculement*. Autrement dit, avec les clusters de basculement, les utilisateurs rencontrent un minimum d'interruptions de service, voire même aucune interruption.



Une solution de clustering avec basculement se compose de plusieurs composants qui comprennent :

- *Nœuds*. Il s'agit des ordinateurs membres d'un cluster de basculement. Ces ordinateurs exécutent un service de cluster ainsi que des ressources et applications associées au cluster.
- *Un réseau*. Il s'agit du réseau sur lequel les nœuds de cluster peuvent communiquer entre eux et avec les clients. Il existe trois types de réseaux qui peuvent être utilisés dans un cluster : public, privé et public-et-privé. Ces réseaux sont présentés plus en détail dans la section « Réseaux de cluster de basculement ».
- *Une ressource*. Il s'agit d'une entité qui est hébergée par un nœud. Elle est gérée par le service de cluster, et peut être démarrée, arrêtée et déplacée vers un autre nœud.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Un espace de stockage en cluster.* Il s'agit d'un système de stockage qui est habituellement partagé entre des nœuds de cluster. Dans certains cas, notamment lorsque des clusters de serveurs exécutent Microsoft® Exchange Server, aucun stockage partagé n'est requis.
- *Des clients.* Il s'agit d'ordinateurs (ou utilisateurs) qui utilisent le service de cluster.
- *Un service ou une application.* Entité logicielle présentée aux clients et utilisée par les clients.

Dans un cluster de basculement, chaque nœud du cluster :

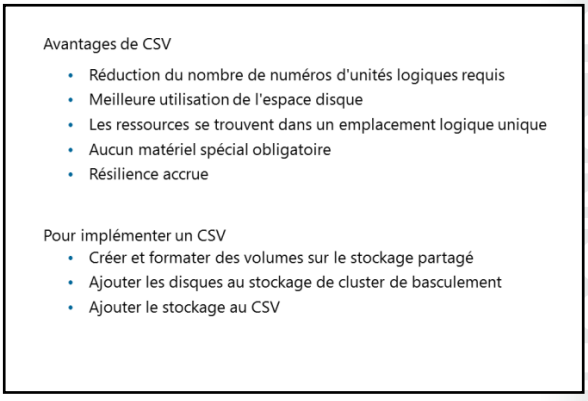
- Dispose d'une connectivité et d'une communication complètes avec les autres nœuds du cluster.
- Est informé lorsqu'un autre nœud rejoint ou quitte le cluster. En outre, chaque nœud tient compte de l'échec d'un nœud ou d'une ressource et a la capacité d'assurer ces services.
- Est connecté à un réseau via lequel les ordinateurs clients peuvent accéder au cluster.
- Est souvent connecté via un bus partagé ou une connexion iSCSI à un stockage partagé.
- Connaît les services ou applications qui s'exécutent localement, et les ressources qui s'exécutent sur tous les autres nœuds du cluster.

L'espace de stockage en cluster fait généralement référence aux unités logiques (disques durs ou numéros d'unités logiques) auxquelles tous les nœuds de cluster sont connectés via un bus partagé. Ce bus est distinct du bus qui contient le système et les disques de démarrage. Les disques partagés stockent des ressources telles que les applications et les partages de fichiers que le cluster gérera.

Un cluster de basculement définit en général au moins deux réseaux de communication de données : le premier réseau permet au cluster de communiquer avec des clients, et l'autre réseau isolé, permet aux membres de nœud de cluster de communiquer directement entre eux. Si aucun stockage partagé directement connecté n'est utilisé, alors un troisième segment réseau (pour iSCSI ou Fibre Channel) peut exister entre les nœuds de cluster et un réseau de stockage des données.

La plupart des applications en cluster et leurs ressources associées sont attribuées à un nœud de cluster à la fois. Le nœud qui fournit l'accès à ces ressources de cluster est le *nœud actif*. Si les nœuds détectent une défaillance sur le nœud actif d'une application en cluster, ou si vous mettez le nœud actif hors connexion pour des raisons de maintenance, l'application en cluster démarre sur un autre nœud du cluster. Pour réduire l'impact de la défaillance, les demandes des clients sont redirigées immédiatement et de façon transparente vers le nouveau nœud de cluster.

Que sont les volumes partagés de cluster (CSV) ?



Dans un déploiement classique de cluster de basculement, un seul nœud à la fois contrôle un numéro d'unité logique sur le stockage partagé. Cela signifie qu'un autre nœud ne peut pas *voir* le stockage partagé, jusqu'à ce qu'il devienne un nœud actif. CSV est une technologie introduite dans Windows Server 2008 R2 qui permet à plusieurs nœuds de partager simultanément un numéro d'unité logique unique. Chaque nœud obtient l'accès exclusif aux fichiers individuels sur le numéro d'unité logique plutôt qu'à l'ensemble du numéro d'unité logique. En d'autres termes, les CSV fournissent une solution distribuée d'accès aux fichiers de sorte que plusieurs nœuds dans le cluster peuvent simultanément accéder au même système de fichiers NTFS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans la première version de Windows Server 2008 R2, le CSV a été conçu uniquement pour héberger des ordinateurs virtuels s'exécutant sur un serveur Hyper-V dans un cluster de basculement. Cette configuration permettait aux administrateurs d'avoir un numéro d'unité logique unique hébergeant plusieurs ordinateurs virtuels dans un cluster de basculement. Plusieurs nœuds de cluster avaient accès au numéro d'unité logique, mais chaque ordinateur virtuel fonctionnait uniquement sur un seul nœud à la fois. Si le nœud sur lequel un ordinateur virtuel s'exécute échouait, le CSV laissait l'ordinateur virtuel redémarrer sur un nœud différent dans le cluster de basculement. En outre, cela simplifiait la gestion des disques pour l'hébergement des ordinateurs virtuels, car chaque ordinateur ne requiert pas de numéro d'unité logique distinct.

Dans Windows Server 2012, le CSV bénéficie d'améliorations supplémentaires. Il est à présent possible d'utiliser un CSV pour d'autres rôles, et pas seulement Hyper-V. Par exemple, dans un scénario de serveur de fichiers avec montée en puissance parallèle, vous pouvez configurer le rôle de serveur de fichiers dans un cluster de basculement. Le serveur de fichiers avec montée en puissance parallèle est conçu pour fournir des partages de fichiers avec montée en puissance parallèle, qui sont disponibles en permanence pour le stockage d'applications serveur basées sur des fichiers. Les partages de fichiers avec montée en puissance parallèle permettent de partager le même dossier sur plusieurs nœuds du même cluster. Dans ce contexte, les CSV dans Windows Server 2012 introduisent la prise en charge d'un cache de lecture, ce qui peut améliorer les performances dans certains scénarios. En outre, un système de fichiers proxy CSV (CSVFS) peut exécuter **Chkdsk** sans affecter les applications possédant des handles ouverts sur le système de fichiers.

Voici d'autres améliorations importantes relatives aux CSV dans Windows Server 2012 :

- CSVFS. Dans la console de gestion des disques, les volumes CSV apparaissent désormais en tant que CSVFS. Toutefois, il ne s'agit pas d'un nouveau système de fichiers. La technologie sous-jacente est toujours le système de fichiers NTFS et des volumes CSVFS sont encore formatés avec NTFS. Cependant, parce que les volumes apparaissent en tant que CSVFS, les applications peuvent découvrir qu'elles s'exécutent sur des CSV, ce qui améliore la compatibilité. De plus, en raison de l'espace de noms de fichier unique, tous les fichiers ont les mêmes nom et chemin d'accès sur tous les nœuds d'un cluster.
- Prise en charge de plusieurs sous-réseaux pour les CSV. Les CSV ont été améliorés pour s'intégrer avec SMB Multichannel afin d'accélérer le débit des volumes CSV.
- Prise en charge du chiffrement de lecteur BitLocker. Windows Server 2012 prend en charge le chiffrement de volume BitLocker pour les disques en cluster traditionnels et les CSV. Chaque nœud exécute le déchiffrement à l'aide du compte d'ordinateur pour le cluster lui-même.
- Prise en charge du stockage SMB 3.0. Le stockage SMB 3.0 est pris en charge pour Hyper-V et des applications telles que Microsoft SQL Server®. Ceci signifie que, par exemple, vous pouvez héberger des fichiers d'ordinateur virtuel Hyper-V sur un dossier partagé.
- Intégration avec SMB Multichannel et SMB Direct. Cette intégration permet au trafic de circuler sur plusieurs réseaux dans le cluster et d'utiliser des cartes réseau qui prennent en charge l'accès direct à la mémoire à distance (RDMA).
- Intégration de la fonctionnalité des espaces de stockage dans Windows Server 2012. Cette intégration peut fournir le stockage virtualisé sur des clusters de disques peu coûteux.
- Réduction des interruptions de service. Les CSV dans Windows Server 2012 permettent d'analyser et de réparer des volumes sans temps hors connexion.

Implémentation de la réplication CSV

Vous pouvez configurer un CSV uniquement au moment de créer un cluster de basculement. Une fois que vous avez créé le cluster de basculement, vous pouvez activer le CSV pour le cluster, puis ajouter le stockage au CSV.

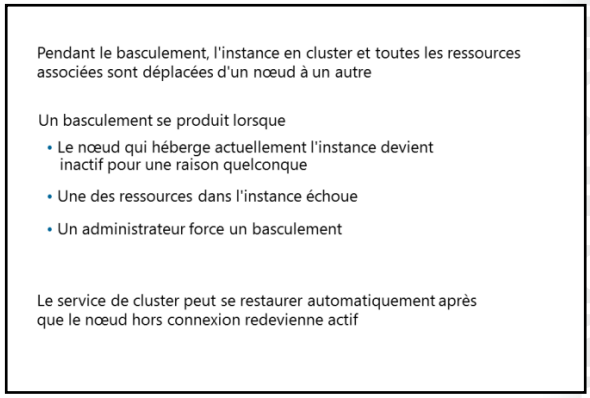
Cependant, avant de pouvoir ajouter le stockage au CSV, le numéro d'unité logique doit être disponible comme stockage partagé pour le cluster. Lorsque vous créez un cluster de basculement, tous les disques partagés configurés dans le Gestionnaire de serveur sont ajoutés au cluster et vous pouvez ensuite les ajouter à un CSV. Si vous ajoutez davantage de numéros d'unité logique au stockage partagé, vous devez d'abord créer des volumes sur le numéro d'unité logique, puis ajouter le stockage au cluster, et enfin ajouter le stockage au CSV.

Il est conseillé de configurer CSV avant de rendre un service hautement disponible. Toutefois, vous pouvez convertir un accès disque standard en CSV après déploiement. Les considérations suivantes s'appliquent :

- La conversion d'un accès disque régulier en CSV supprime la lettre de lecteur ou le point de montage du numéro d'unité logique. Cela signifie que vous devez recréer toutes les ressources qui sont stockées sur le stockage partagé. Vous ne pouvez pas ajouter le stockage partagé à CSV s'il est en cours de utilisation. Si vous disposez d'un service d'ordinateur virtuel en cours d'exécution qui utilise un disque de cluster, vous devez l'arrêter, puis ajouter le disque aux volumes partagés de cluster (CSV).

Que sont le basculement et la restauration automatique ?

Le basculement transfère d'un nœud vers un autre la responsabilité de l'accès aux ressources d'un cluster. Le basculement peut se produire lorsqu'un administrateur déplace intentionnellement des ressources vers un autre nœud à des fins de maintenance, ou lorsqu'un temps mort non planifié se produit sur un nœud à la suite d'une défaillance matérielle ou pour d'autres raisons. En outre, une défaillance de service sur un nœud actif peut déclencher le basculement vers un autre nœud.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

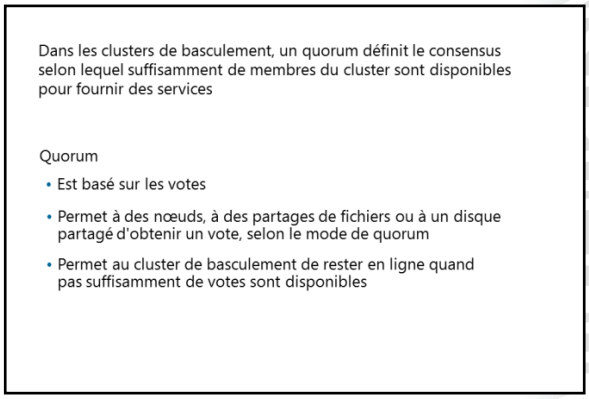
Le processus de basculement se déroule de la manière suivante :

1. Le service de cluster met toutes les ressources de l'instance hors connexion, selon un ordre déterminé par la hiérarchie des dépendances de l'instance. Cela signifie que les ressources dépendantes sont d'abord mises hors connexion, puis les ressources desquelles elles dépendent. Par exemple, si une application dépend d'une ressource de disque physique, le service de cluster met en premier lieu l'application hors connexion, ce qui permet à celle-ci d'écrire des modifications sur le disque avant que ce dernier ne soit également mis hors connexion.
2. Une fois que toutes les ressources ont été mises hors connexion, le service de cluster tente de transférer l'instance vers le nœud suivant dans la liste de propriétaires favoris de l'instance.
3. Si le service de cluster déplace correctement l'instance vers un autre nœud, il tente de remettre toutes les ressources en ligne. Cette fois, il commence par le bas de la hiérarchie des dépendances. Le basculement est terminé lorsque toutes les ressources sont en ligne sur le nouveau nœud.

Une fois que le nœud hors connexion redevient actif, le service de cluster peut restaurer automatiquement des instances qui étaient hébergées sur le nœud hors connexion initialement. Quand le service de cluster restaure automatiquement une instance, il utilise les mêmes procédures que pendant le basculement. Le service de cluster met toutes les ressources de l'instance hors connexion, déplace l'instance, puis remet toutes les ressources de l'instance en ligne.

Qu'est-ce qu'un quorum ?

Un *quorum* est le nombre d'éléments en ligne nécessaires pour qu'un cluster continue de s'exécuter. Chaque nœud de cluster est un élément et en réalité, chaque élément d'un cluster peut voter pour déterminer si le cluster continue de s'exécuter. En présence d'un nombre pair de nœuds, un élément supplémentaire, appelé *témoin*, est attribué au cluster. L'élément témoin peut être un disque ou un partage de fichiers. Chaque élément de vote comprend une copie de la configuration du cluster et le service de cluster veille à maintenir toutes les copies synchronisées à tout moment.



Le cluster cessera d'assurer la protection du basculement si la plupart des nœuds échouent, ou s'il y a un problème de communication entre les nœuds de cluster. Sans mécanisme de quorum, chaque ensemble de nœuds peut continuer à fonctionner en tant que cluster de basculement, ce qui génère une partition du cluster. Le quorum empêche deux ou plusieurs nœuds d'exécuter une ressource du cluster de basculement simultanément. Si une majorité absolue n'est pas atteinte entre les membres de nœud, alors le vote du témoin devient crucial pour maintenir la validité du cluster.

Les opérations simultanées peuvent se produire lorsque des problèmes réseau empêchent un ensemble de nœuds de communiquer avec un autre ensemble de nœuds. Ainsi, une situation peut se produire dans laquelle plusieurs nœuds tentent de contrôler l'accès à une ressource. Si cette ressource est, par exemple, une application de base de données, le dommage tel que l'altération de la base de données pourrait en résulter. Imaginez que deux instances ou plus de la même base de données soient rendues disponibles sur le réseau, ou que des données soient consultées et écrites simultanément sur une cible à partir de plusieurs sources : les conséquences peuvent être graves. Si l'application elle-même n'est pas endommagée, les données peuvent facilement être corrompues.

Étant donné qu'un cluster donné a un ensemble de nœuds et une configuration de quorum spécifiques, le cluster peut calculer le nombre de votes requis pour qu'il puisse continuer à assurer la protection de basculement. Si le nombre de votes baisse en dessous de la majorité, le cluster cesse de s'exécuter, ce qui signifie qu'il n'assurera pas la protection de basculement en cas de défaillance de nœud. Les nœuds écouteront toujours la présence d'autres nœuds, au cas où un autre nœud apparaîtrait de nouveau sur le réseau. Cependant, les nœuds ne fonctionneront pas comme un cluster sauf si un consensus de majorité ou un quorum est obtenu.

Le fonctionnement complet d'un cluster ne dépend pas seulement du quorum, mais également de la capacité de chaque nœud à prendre en charge les services et les applications qui basculent vers ce nœud. Par exemple, un cluster comprenant cinq nœuds peut encore avoir un quorum après la défaillance de deux nœuds, mais chaque nœud de cluster restant continuera à servir des clients uniquement si sa capacité est suffisante (notamment l'espace disque, la puissance de traitement, la bande passante ou la mémoire vive (RAM)) pour prendre en charge les services et applications qui ont basculé dessus. Une partie importante du processus de conception consiste à planifier la capacité de basculement de chaque nœud. Un nœud de basculement doit pouvoir exécuter sa propre charge et la charge des ressources supplémentaires qui pourraient être basculées vers lui.

Processus d'obtention du quorum

Un cluster doit exécuter plusieurs phases pour atteindre un quorum. Lorsqu'un nœud spécifique apparaît en ligne, il détermine s'il existe d'autres membres du cluster avec lesquels il est possible de communiquer. Ce processus peut s'exécuter sur plusieurs nœuds simultanément. Une fois la communication établie avec d'autres membres, les membres comparent l'avis de tous les membres du cluster jusqu'à ce qu'ils se mettent d'accord sur une opinion (en fonction du datage et d'autres informations). Il est décidé si cet ensemble de membres « a le quorum » ou si le total des membres qui le constitue est suffisant pour obtenir suffisamment de votes et éviter ainsi une « division » au sein du cluster.

Un scénario de division signifie qu'un autre ensemble de nœuds qui se trouvent dans le cluster s'exécutent sur une partie du réseau inaccessible par ces nœuds. Par conséquent, plusieurs nœuds peuvent tenter activement d'autoriser l'accès à la même ressource en cluster. Si le nombre de votes est insuffisant pour atteindre le quorum, les électeurs (les membres actuellement identifiés du cluster) attendent que des membres supplémentaires apparaissent. Une fois que le total minimal de votes a été atteint, le service de cluster commence à mettre les ressources et applications de cluster en service. Une fois le quorum atteint, le cluster devient entièrement fonctionnel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Modes de quorum dans le clustering avec basculement de Windows Server 2012

Mode de quorum	Qu'est ce qui obtient un vote ?	Quand le quorum est-il conservé ?
Nœud majoritaire	Seuls les nœuds du cluster ont un vote	Le quorum est conservé lorsque plus de la moitié des nœuds sont en ligne
Nœud et disque majoritaires	Les nœuds du cluster et un témoin de disque ont un vote	Le quorum est conservé lorsque plus de la moitié des votes sont en ligne
Nœud et partage de fichiers majoritaires	Les nœuds du cluster et un témoin de partage de fichiers ont un vote	Le quorum est conservé lorsque plus de la moitié des votes sont en ligne
Pas de majorité : Disque uniquement	Seul le disque quorum partagé a un vote	Le quorum est conservé lorsque le disque partagé est en ligne

Les modes de quorum de Windows Server 2012 sont également présents dans Windows Server 2008. Une majorité de votes continue donc à déterminer si un cluster atteint le quorum. Les nœuds peuvent voter et, dans certains cas, un disque du stockage en cluster (appelé *témoin de disque*) ou un partage de fichiers (appelé *témoin de partage de fichiers*) peut voter. Il existe également un mode de quorum appelé Pas de majorité : Disque uniquement, qui fonctionne comme le quorum à disques dans Windows Server 2003. Différent du mode Aucune majorité : Disque uniquement, dans ce cas, il n'y a aucun point de défaillance avec les modes de quorum, car seul le nombre de votes est important et non si un élément particulier est disponible pour le vote.

Le mode de quorum dans le clustering avec basculement de Windows Server 2012 est flexible. Vous pouvez choisir le mode le mieux adapté à votre cluster. Sachez que dans la plupart des cas, il vaut mieux utiliser le mode de quorum sélectionné par le logiciel de cluster. Si vous exécutez l'Assistant Configuration de quorum, le mode de quorum que l'Assistant répertorie comme « recommandé » est le mode de quorum choisi par le logiciel de cluster. Vous devez modifier la configuration de quorum uniquement si vous estimez que la modification est appropriée pour votre cluster.

Le clustering avec basculement de Windows Server 2012 dispose de quatre modes de quorum :

- Nœud majoritaire. Chaque nœud disponible et en communication avec d'autres nœuds peut voter. Le cluster s'exécute uniquement avec une majorité des votes, autrement dit plus de la moitié. Ce modèle est préféré quand le cluster comporte un nombre impair de nœuds de serveur et qu'aucun témoin n'est requis pour maintenir ou atteindre le quorum.
- Nœud et disque majoritaires. Chaque nœud plus un témoin de disque, qui est un disque désigné dans le stockage en cluster, peuvent voter chaque fois qu'ils sont disponibles et en communication. Le cluster s'exécute uniquement avec une majorité des votes, autrement dit plus de la moitié. Ce modèle est basé sur un nombre pair de nœuds de serveur pouvant communiquer entre eux dans le cluster en plus du témoin de disque.
- Nœud et partage de fichiers majoritaires. Chaque nœud plus le témoin de partage de fichiers, qui est un partage de fichiers désigné créé par l'administrateur, peuvent voter chaque fois qu'ils sont disponibles et en communication. Le cluster s'exécute uniquement avec une majorité des votes, autrement dit plus de la moitié. Ce modèle est basé sur un nombre pair de nœuds de serveur pouvant communiquer entre eux dans le cluster en plus du témoin de partage de fichiers.
- Pas de majorité : Disque uniquement. Le cluster a le quorum si un nœud est disponible et en communication avec un disque spécifique du stockage en cluster. Seuls les nœuds également en communication avec ce disque peuvent joindre le cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

À l'exception du mode Pas de majorité : disque uniquement, tous les modes de quorum dans les clusters de basculement Windows Server 2012 sont basés sur un modèle simple de vote majoritaire. Tant qu'une majorité des votes est disponible, le cluster continue de fonctionner. Par exemple, si un cluster a cinq votes, il continue de fonctionner tant qu'au moins trois votes sont disponibles. Peu importe la source des votes : il peut s'agir d'un nœud, d'un témoin de disque ou d'un témoin de partage de fichiers. Le cluster cessera de fonctionner si une majorité des votes est indisponible.

Dans le mode Pas de majorité : Disque uniquement, le disque quorum partagé peut opposer son véto sur tous les autres votes possibles. Dans ce mode, le cluster continuera de fonctionner tant que le disque quorum partagé et au moins un nœud sont disponibles. Ce type de quorum empêche également que plus d'un nœud n'assume le rôle principal.

 **Remarque :** Si le disque quorum partagé n'est pas disponible, le cluster cessera de fonctionner, même si tous les nœuds sont encore disponibles. Dans le mode Pas de majorité : Disque uniquement, le disque quorum partagé est un point de défaillance unique, c'est pourquoi ce mode n'est pas recommandé.

Lorsque vous configurez un cluster de basculement dans Windows Server 2012, l'Assistant Installation sélectionne automatiquement une des deux configurations par défaut. Par défaut, le clustering avec basculement sélectionne :

- Nœud majoritaire s'il y a un numéro impair de nœuds dans le cluster.
- Nœud et disque majoritaires s'il y a un numéro pair de nœuds dans le cluster.

 **Remarque :** Vous devez modifier ce paramètre uniquement si vous estimez que la modification est appropriée pour votre cluster et que vous comprenez bien les implications de cette modification.

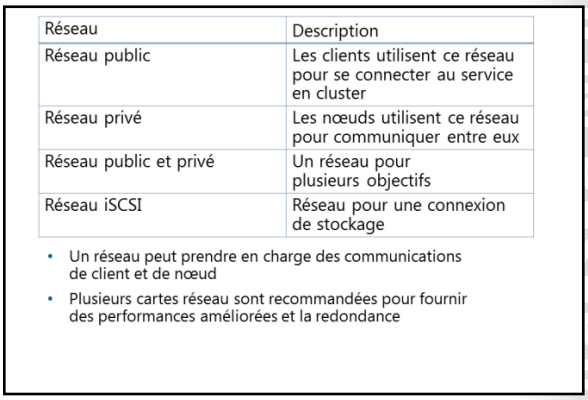
Outre la planification du mode de quorum, vous devez également prendre en compte la capacité des nœuds dans votre cluster et leur capacité à prendre en charge les services et applications qui peuvent basculer vers ce nœud. Par exemple, un cluster comprenant quatre nœuds et un témoin de disque aura toujours le quorum après la défaillance de deux nœuds. Cependant, si plusieurs applications ou services sont déployés sur le cluster, il est possible que chaque nœud de cluster restant n'ait pas la capacité requise pas assurer les services.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Réseaux de cluster de basculement

Les réseaux et les cartes réseau sont des composants importants de l'implémentation de cluster. Vous ne pouvez pas configurer un cluster sans configurer les réseaux que le cluster utilisera. Un réseau peut jouer l'un des rôles suivants dans un cluster :



- *Réseau privé*. Un réseau privé transmet la communication interne des clusters. Les nœuds de cluster utilisent ce réseau pour échanger des pulsations et rechercher d'autres nœuds. Le cluster de basculement authentifie l'ensemble de la communication interne. Cependant, les administrateurs qui sont particulièrement soucieux de la sécurité peuvent souhaiter restreindre la communication interne aux réseaux physiques sécurisés uniquement.
- *Réseau public*. Un réseau public fournit aux systèmes clients l'accès aux services d'application de cluster. Les ressources des adresses IP sont créées sur les réseaux qui permettent aux clients d'accéder au service de cluster.
- *Réseau public et privé*. Un réseau public et privé (également appelé *réseau mixte*) transmet la communication interne des clusters et connecte des clients aux services d'application de cluster.

Lorsque vous configurez des réseaux dans des clusters de basculement, vous devez également déterminer un réseau pour la connexion au stockage partagé. Si vous utilisez iSCSI pour la connexion de stockage partagé, le réseau utilisera un réseau IP de communication Ethernet. Cependant, vous ne devez pas utiliser ce réseau pour la communication de nœud ou de client. Ce type de partage du réseau iSCSI peut provoquer des problèmes de contention et de latence pour les utilisateurs et pour la ressource fournie par le cluster.

Bien qu'il ne s'agisse pas d'une meilleure pratique, vous pouvez utiliser les réseaux privés et publics pour les communications de client et de nœud. Il est préférable de dédier un réseau isolé à la communication privée de nœud. En effet, tout comme lorsque vous utilisez un réseau Ethernet distinct pour iSCSI, vous éviterez ainsi les problèmes de goulot d'étranglement et de contention des ressources. Le réseau public est configuré pour permettre les connexions clientes sur le cluster de basculement. Bien que le réseau public puisse fournir une capacité de sauvegarde du réseau privé, une meilleure pratique en matière de conception consiste à définir des réseaux alternatifs aux principaux réseaux privés et publics, ou au moins d'associer les interfaces réseau utilisées pour ces réseaux.

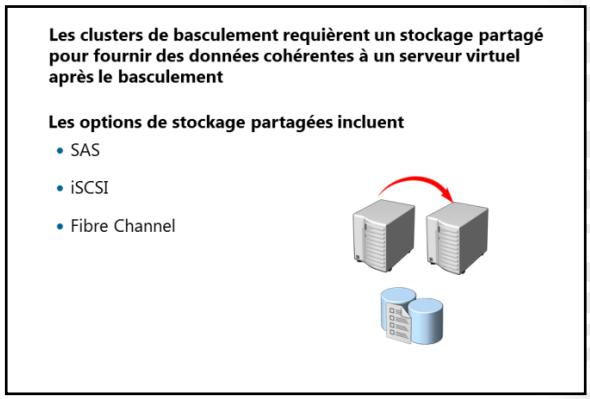
Les fonctionnalités de mise en réseau dans les clusters basés sur Windows Server 2012 sont les suivantes :

- Les nœuds transmettent et reçoivent des pulsations à l'aide de la monodiffusion du protocole UDP (User Datagram Protocol), plutôt que via la diffusion UDP (qui était utilisée dans les clusters hérités). Les messages sont envoyés sur le port 3343.
- Vous pouvez inclure des serveurs en cluster sur différents sous-réseaux IP, ce qui réduit la complexité de la configuration de clusters multisites.

- La *carte virtuelle de cluster de basculement* est un périphérique masqué qui est ajouté à chaque nœud lors de l'installation de la fonctionnalité Clustering avec basculement. Une adresse MAC (Media Access Control) est attribuée à la carte, basée sur l'adresse MAC qui est associée à la première carte réseau physique énumérée dans le nœud.
- Les clusters de basculement prennent entièrement en charge IPv6 pour les communications nœud-à-nœud et nœud-à-client.
- Vous pouvez utiliser le protocole DHCP (Dynamic Host Configuration Protocol) pour attribuer des adresses IP, ou attribuer des adresses IP statiques à tous les nœuds du cluster. Cependant, si certains nœuds possèdent une adresse IP statique alors que vous en configurez d'autres pour qu'ils utilisent le protocole DHCP, l'Assistant Validation d'une configuration émettra une erreur. Les ressources des adresses IP de cluster sont obtenues en fonction de la configuration de l'interface réseau prenant en charge ce réseau de cluster.

Stockage de cluster de basculement

La plupart des scénarios de clustering avec basculement requièrent un stockage partagé pour fournir des données cohérentes à un service ou à une application à haut niveau de disponibilité après le basculement. Les trois options de stockage partagé pour un cluster de basculement sont les suivantes :



- *Interface SAS* (*Serial Attached SCSI*) *partagée*. L'option SAS partagée est l'option la plus peu coûteuse. Cependant, l'option SAS partagée n'est pas très flexible pour le déploiement car les deux nœuds de cluster doivent être physiquement proches l'un de l'autre. En outre, les dispositifs de stockage partagé qui sont des interfaces SAS partagées ont un nombre limité de connexions pour les nœuds de cluster.
- *iSCSI*. *iSCSI* est un type de réseau de zone de stockage (SAN, Storage Area Network) qui transmet des commandes SCSI (Small Computer System Interface) sur les réseaux IP. Les performances sont acceptables dans la plupart des scénarios lorsqu'un réseau Ethernet entre un gigabit par seconde (Gbps) et 10 Gbps est utilisé comme support physique pour la transmission des données. Ce type de réseau SAN est relativement peu coûteux à implémenter car aucun matériel réseau spécialisé n'est requis. Dans Windows Server 2012, vous pouvez implémenter le logiciel cible iSCSI sur n'importe quel serveur, et présenter le stockage local sur l'interface iSCSI aux clients.
- *Fibre Channel*. Les réseaux SAN Fibre Channel présentent en général de meilleures performances que les réseaux SAN iSCSI, mais sont plus onéreux. Des connaissances et du matériel spécialisés sont requis pour implémenter un réseau SAN Fibre Channel.

Remarque : Microsoft iSCSI Software Target est désormais une fonctionnalité intégrée dans Windows Server 2012. Cette fonctionnalité peut fournir le stockage d'un serveur sur un réseau TCP/IP, y compris le stockage partagé pour des applications qui sont hébergées dans un cluster de basculement. En outre, dans Windows Server 2012, vous pouvez configurer un serveur cible iSCSI à haut niveau de disponibilité comme rôle en cluster à l'aide du Gestionnaire du cluster de basculement ou de Windows PowerShell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration requise pour le stockage

Avant de choisir une solution de stockage, vous devez être également informé de la configuration requise pour le stockage :

- Pour bénéficier de la prise en charge native de disque intégrée au clustering avec basculement, utilisez des disques de base et non des disques dynamiques.
- Vous devez formater les partitions avec NTFS. Pour le témoin de disque, la partition doit être NTFS, car le système FAT n'est pas pris en charge.
- Pour le style de partition du disque, vous pouvez utiliser le secteur de démarrage principal (MBR, Master Boot Record) ou la table de partition de l'identificateur unique universel (GUID, Globally Unique IDentifier) (GPT, GUID Partition Table).
- Étant donné que les améliorations apportées au clustering avec basculement nécessitent que le stockage réponde correctement à des commandes SCSI spécifiques, le stockage doit se conformer à la norme appelée SPC-3 (SCSI Primary Commands-3). Le stockage doit notamment prendre en charge les réservations persistantes, tel qu'indiqué dans la norme SPC-3.
- Le pilote miniport utilisé pour le stockage doit être compatible avec le pilote de stockage Storport. Storport offre une architecture plus performante et une meilleure compatibilité Fibre Channel dans des systèmes d'exploitation Windows.
- Vous devez isoler les périphériques de stockage (un cluster par périphérique). Vous ne devriez pas permettre aux serveurs qui appartiennent à différents clusters d'accéder aux mêmes périphériques de stockage. Vous pouvez accomplir ceci à l'aide du numéro d'unité logique masquant ou zone. Ceci empêche les numéros d'unités logiques utilisés sur un cluster d'être vus sur un autre cluster. Utilisez un logiciel MPIO (Multipath I/O). Les nœuds de cluster utilisent généralement plusieurs adaptateurs de bus hôte pour accéder au stockage, ce qui vous permet de bénéficier d'une haute disponibilité supplémentaire. Pour utiliser plusieurs adaptateurs de bus hôte (HBA), vous devez utiliser le logiciel multivoie. Pour Windows Server 2012, votre solution multivoie doit être basée sur Multipath I/O (MPIO) de Microsoft. Votre fabricant de matériel fournit habituellement un module MPIO spécifique au périphérique (DSM) pour votre matériel, bien que Windows Server 2012 comprenne un ou plusieurs DSM dans le cadre du système d'exploitation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Implémentation d'un cluster de basculement

Les clusters de basculement dans Windows Server 2012 présentent des configurations matérielles et logicielles recommandées qui permettent à Microsoft de prendre en charge le cluster. Les clusters de basculement sont destinés à fournir un niveau de service supérieur aux serveurs autonomes. Par conséquent, les configurations matérielles de cluster sont généralement plus strictes que les configurations requises pour les serveurs autonomes.

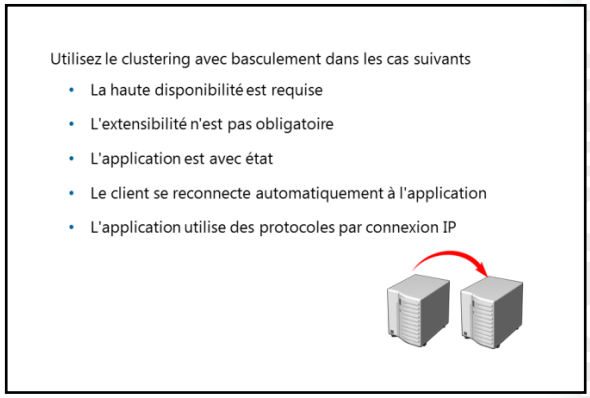
Cette leçon décrit comment se préparer à l'implémentation de cluster. Dans cette leçon, vous allez également présenter les configurations requises en matière de matériel, de réseau, de stockage, d'infrastructure et de logiciels, pour des clusters de basculement Windows Server 2012. Enfin, cette leçon présente les étapes d'utilisation de l'Assistant Validation d'une configuration afin de garantir une configuration correcte du cluster, ainsi que le mode de migration des clusters de basculement.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment se préparer pour l'implémentation du clustering avec basculement ;
- décrire la configuration matérielle requise pour le clustering avec basculement ;
- décrire la configuration de réseau requise pour le clustering avec basculement ;
- décrire la configuration d'infrastructure requise pour le clustering avec basculement ;
- décrire la configuration logicielle requise pour le clustering avec basculement ;
- expliquer comment valider et configurer un cluster de basculement ;
- expliquer comment migrer des clusters de basculement.

Préparation à l'implémentation du cluster de basculement



Avant d'implémenter le clustering avec basculement, vous devez identifier les services et applications que vous souhaitez rendre à haut niveau de disponibilité. Vous ne pouvez pas appliquer le clustering avec basculement à toutes les applications, car elles ont parfois leurs propres mécanismes de redondance. En outre, vous devez garder à l'esprit que le clustering avec basculement n'améliore par l'extensibilité par l'ajout de nœuds. Une extensibilité accrue est obtenue uniquement par une extension verticale et au moyen de matériel puissant pour les différents nœuds. Par conséquent, vous devez utiliser le clustering avec basculement uniquement si votre objectif est la haute disponibilité, et non pas l'extensibilité. Dans Windows Server 2012, il y a une exception à ceci : si vous implémentez des services de fichiers sur les volumes partagés de cluster, vous pouvez également atteindre un niveau d'extensibilité.

Le clustering avec basculement est plus adapté aux applications avec état qui sont limitées à un ensemble unique de données. Une base de données est un exemple d'une telle application. Les données sont enregistrées dans un emplacement unique et peuvent être utilisées uniquement par une instance de base de données. Vous pouvez également utiliser le clustering avec basculement pour des ordinateurs virtuels Hyper-V. Les meilleurs résultats pour le clustering avec basculement sont obtenus lorsque le client peut se reconnecter à l'application automatiquement après le basculement. Si le client ne se reconnecte pas automatiquement, alors l'utilisateur doit redémarrer l'application cliente.

Le clustering avec basculement utilise uniquement des protocoles IP et est donc adapté exclusivement aux applications IP. Désormais, le clustering avec basculement prend en charge IPv4 et IPv6.

Prenez en compte les instructions suivantes au moment de planifier la capacité du nœud dans un cluster de basculement :

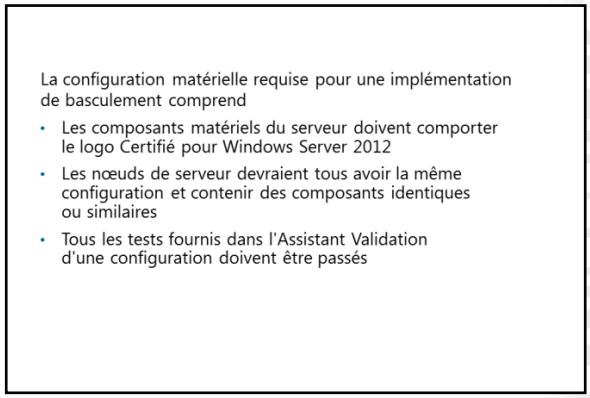
- Répartissez les applications à haut niveau de disponibilité d'un nœud défaillant. Quand tous les nœuds d'un cluster de basculement sont actifs, les services ou applications à haut niveau de disponibilité d'un nœud défaillant doivent être répartis parmi les nœuds restants afin d'empêcher qu'un seul nœud ne soit surchargé.
- Assurez-vous que chaque nœud a la capacité d'inactivité suffisante pour fournir les services ou applications à haut niveau de disponibilité qui lui sont alloués en cas d'échec d'un autre nœud. Cette capacité d'inactivité doit consister en une mémoire tampon suffisante pour éviter que des nœuds s'exécutent à leur capacité maximale après un événement d'échec. L'incapacité à planifier de manière appropriée l'utilisation des ressources peut entraîner une diminution des performances après une défaillance de nœud.
- Utilisez du matériel doté d'une capacité semblable pour tous les nœuds dans un cluster. Cela simplifie le processus de planification pour le basculement, car la charge de basculement sera également distribuée parmi les nœuds restants.
- Utilisez des serveurs de secours pour simplifier la planification de capacité. Quand un nœud passif est inclus dans le cluster, tous les services ou applications à haut niveau de disponibilité d'un nœud défaillant peuvent être basculés vers le mode passif. Cela élimine le besoin d'une planification de capacité complexe. Si cette configuration est sélectionnée, il est important que le serveur de secours ait la capacité suffisante pour exécuter la charge de plus d'une défaillance de nœud.

Vous devez également examiner tous les composants de configuration du cluster pour identifier les points de défaillance uniques. Vous pouvez résoudre de nombreux points de défaillance uniques grâce à des solutions simples, telles que l'ajout de contrôleurs de stockage permettant de séparer des disques et de répartir leurs données, ou l'association de cartes réseau, et l'utilisation de logiciel de gestion multivoie. Ces solutions réduisent le risque que la défaillance d'un périphérique unique n'entraîne un échec dans le cluster. En général, le matériel informatique de classe serveur propose des options en matière d'alimentations multiples pour la redondance d'alimentation et pour créer des ensembles RAID (Redondant Array of Independent Disks) pour la redondance de données du disque.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration matérielle requise pour l'implémentation de cluster de basculement

Il est important que vous preniez les décisions appropriées en sélectionnant le matériel pour vos nœuds de cluster. Les clusters de basculement doivent respecter les critères suivants pour répondre aux exigences en matière de disponibilité et de support :



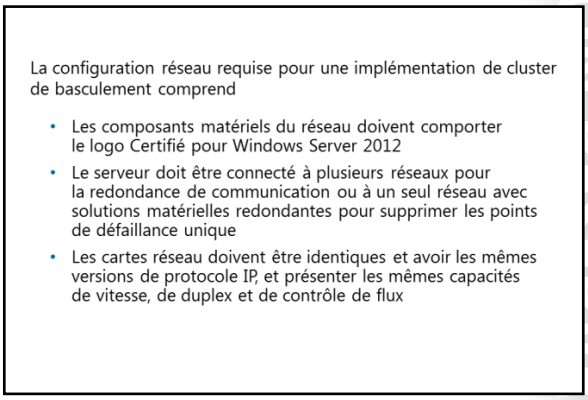
- Tout le matériel que vous sélectionnez pour un cluster de basculement doit répondre aux exigences du logo « Certifié pour Windows Server 2012 ». Le matériel sur lequel ce logo est apposé a été testé de manière indépendante pour répondre aux normes techniques les plus élevées en matière de fiabilité, de disponibilité, de stabilité, de sécurité et de compatibilité de plateforme. Ce logo signifie également que des options de support officiel existent en cas de dysfonctionnements.
- Vous devez installer le même matériel ou du matériel similaire sur chaque nœud de cluster de basculement. Par exemple, si vous choisissez un modèle spécifique de carte réseau, vous devez installer cette carte sur chacun des nœuds de cluster.
- Si vous utilisez une connexion de stockage SAS ou Fiber Channel, les contrôleurs de périphérique de stockage de masse dédiés au stockage en cluster doivent être identiques sur tous les serveurs en cluster. Ils doivent également utiliser la même version du microprogramme.
- si vous utilisez des connexions de stockage iSCSI, chaque serveur en cluster doit être équipé d'une ou de plusieurs cartes réseau ou adaptateurs de bus hôte dédiés au stockage en cluster. Le réseau que vous utilisez pour les connexions de stockage iSCSI ne peut pas être utilisé pour les communications réseau. Sur tous les serveurs en cluster, les cartes réseau qui vous permettent de vous connecter à la cible de stockage iSCSI doivent être identiques (il est recommandé d'utiliser 1 Gbps Ethernet ou plus).
- Une fois que vous avez configuré le matériel sur tous les serveurs, tous les tests fournis dans l'Assistant Validation d'une configuration doivent être passés pour que le cluster soit considéré comme une configuration prise en charge par Microsoft.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de réseau requise pour l'implémentation de cluster de basculement

Une des configurations réseau requises pour l'implémentation de cluster de basculement est que les composants de matériel réseau de cluster de basculement doivent avoir le logo de certification pour Windows Server 2012, et doivent également réussir les tests de l'Assistant Validation d'une configuration. De plus :

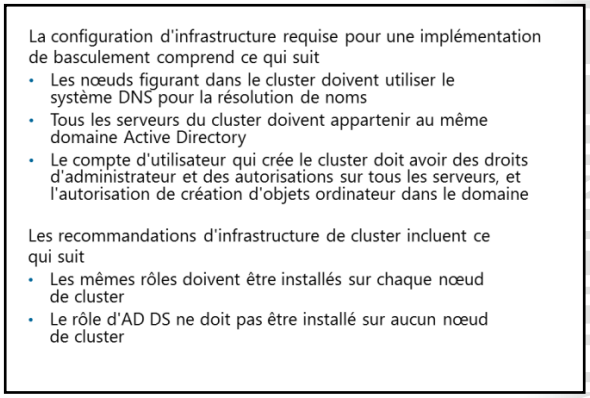


- Les cartes réseau dans chaque nœud doivent être identiques et avoir la même version de protocole IP, et présenter les mêmes capacités de vitesse, de duplex et de contrôle de flux.
- Les réseaux et l'équipement réseau auxquels vous connectez les nœuds doivent être redondants, de sorte que même en cas de défaillance unique, les nœuds continueront de communiquer entre eux. Vous pouvez utiliser l'association de cartes réseau pour fournir une redondance unique de réseau. Nous vous recommandons d'utiliser plusieurs réseaux afin de fournir plusieurs chemins d'accès entre les nœuds pour la communication entre ces derniers. Autrement, un message d'avertissement sera généré pendant le processus de validation.
- Les cartes réseau dans un réseau de clusters doivent utiliser la même méthode d'attribution d'adresses IP, ce qui signifie qu'elles utilisent toutes des adresses IP statiques ou qu'elles utilisent toutes le protocole DHCP.

Remarque : Si vous connectez les nœuds de cluster à un réseau unique, celui-ci passera avec succès le test de redondance de l'Assistant Validation d'une configuration. Toutefois, le rapport émis par l'Assistant inclura un avertissement indiquant que le réseau ne doit pas présenter de point unique de défaillance.

Configuration d'infrastructure requise pour l'implémentation de cluster de basculement

Les clusters de basculement dépendent des services d'infrastructure. Chaque nœud de serveur doit se trouver dans le même domaine Active Directory, et si vous utilisez le système DNS (Domain Name System), les nœuds doivent utiliser les mêmes serveurs DNS pour la résolution de noms.



Il est recommandé d'installer les mêmes fonctionnalités et rôles de Windows Server 2012 sur chaque nœud. Une configuration incohérente sur des nœuds de cluster peut entraîner l'instabilité du système et des problèmes de performances. En outre, vous ne devez pas installer le rôle AD DS sur les nœuds de cluster, car AD DS possède son propre mécanisme de tolérance de panne. Si vous installez le rôle AD DS sur un des nœuds, vous devez l'installer sur tous les nœuds. Cependant, nous le déconseillons.

Vous devez posséder l'infrastructure réseau suivante pour un cluster de basculement :

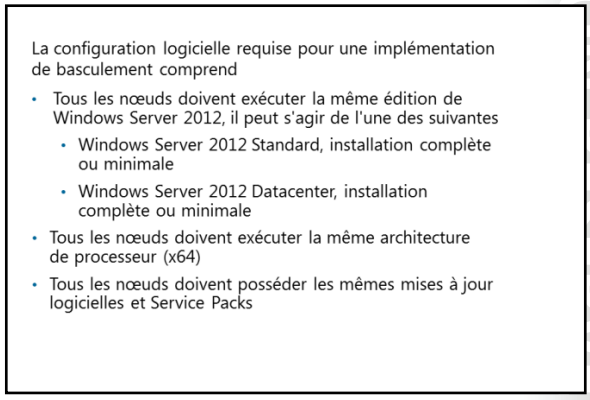
- Paramètres réseau et adresses IP. Lorsque vous utilisez des cartes réseau identiques pour un réseau, utilisez également des paramètres de communication identiques (notamment la vitesse, le mode duplex, le contrôle de flux et le type de média) sur ces cartes. Comparez également les paramètres entre la carte réseau et le commutateur auquel elle se connecte, et assurez-vous qu'aucun paramètre n'est en conflit. Sinon, des problèmes de surcharge du réseau ou de perte d'images peuvent se produire, ce qui risque de compromettre la communication des nœuds entre eux, avec des clients ou avec des systèmes de stockage.
- Sous-réseaux uniques. Si vous utilisez des réseaux privés qui ne sont pas acheminés vers le reste de l'infrastructure réseau pour la communication entre les nœuds de cluster, vérifiez que chacun de ces réseaux privés utilise un sous-réseau unique. Cela est nécessaire même si vous attribuez à chaque carte réseau une adresse IP unique. En outre, ces adresses de réseau privé ne devraient pas être inscrites dans le DNS. Par exemple, si vous avez un nœud de cluster dans un bureau central qui utilise un réseau physique, et un autre nœud dans une filiale qui utilise un réseau physique distinct, ne spécifiez pas 10.0.0.0/24 pour les deux réseaux, même si vous donnez à chaque carte une adresse IP unique. Cela empêche l'apparition de boucles de routage et autres problèmes de communications réseau si, par exemple, les segments sont par erreur configurés dans le même domaine de collision en raison d'attributions incorrectes de réseau local virtuel (VLAN, Virtual Local Area Network).
- DNS. Les serveurs du cluster utilisent généralement le système DNS pour la résolution de noms. Le protocole de mises à jour dynamiques DNS est une configuration prise en charge.
- Rôle de domaine. Tous les serveurs du cluster doivent appartenir au même domaine Active Directory. Il est conseillé d'affecter à tous les serveurs en cluster le même rôle de domaine (serveur membre ou contrôleur de domaine). Le rôle recommandé est serveur membre parce qu'AD DS comprend par définition son propre mécanisme de protection contre le basculement.
- Compte d'administration du cluster. Pour administrer le cluster, vous devez avoir un compte avec des autorisations appropriées. Vous devez avoir des droits d'administrateur local sur tous les nœuds faisant partie du cluster. En outre, lorsque vous créez le cluster, vous devez avoir le droit de créer de nouveaux objets dans les domaines. Vous pouvez y parvenir à l'aide du compte d'administrateur de domaine, ou vous pouvez déléguer ces droits à un autre compte de domaine.

Dans Windows Server 2012, il n'existe pas de compte de service de cluster. À la place, le service de cluster s'exécute automatiquement dans un contexte spécial qui fournit les autorisations et informations d'identification spécifiques qui sont nécessaires pour le service (similaire au contexte système local, mais avec des informations d'identification limitées). Quand un cluster de basculement est créé et qu'un objet ordinateur correspondant est créé dans AD DS, cet objet est configuré afin d'empêcher toute suppression accidentelle. En outre, la ressource de nom de réseau de cluster offre une logique supplémentaire de contrôle de l'intégrité, qui surveille de façon régulière l'intégrité et les propriétés de l'objet ordinateur représentant la ressource de nom de réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration logicielle requise pour l'implémentation de cluster de basculement



Les clusters de basculement requièrent que chaque nœud de cluster exécute la même version de Windows Server 2012. Il peut s'agir de Windows Server 2012 Standard ou Windows Server 2012 Datacenter. Les nœuds doivent également posséder les mêmes mises à jour logicielles et Service Packs. En fonction du rôle qui sera mis en cluster, une installation minimale de Windows Server 2012 peut également répondre à la configuration logicielle requise. Dans Windows Server 2012, Server Core est l'option d'installation par défaut, et donc vous devriez la considérer comme un nœud de cluster. Cependant, vous pouvez également installer le clustering avec basculement sur une version complète d'interface graphique utilisateur.

Il est également primordial que la même version du Service Pack ou toutes les mises à jour du système d'exploitation soient présentes sur tous les nœuds qui constituent le cluster.

Remarque : Windows Server 2012 fournit la technologie Mise à jour adaptée aux clusters qui peut vous aider à maintenir des mises à jour sur des nœuds de cluster. Cette fonctionnalité fera l'objet d'une description détaillée dans la « Leçon 4 : Maintenance d'un cluster de basculement ».

Chaque nœud doit exécuter la même architecture de processeur. Cela signifie que chaque nœud doit avoir la même famille de processeurs, qui peut être, par exemple, la famille de processeurs Intel Xeon avec la technologie de mémoire étendue 64, la famille de processeurs AMD64 d'AMD Opteron ou la famille de processeurs Intel Itanium.

Démonstration : Validation et configuration d'un cluster de basculement

L'Assistant Validation d'une configuration exécute des tests visant à déterminer si le matériel et les paramètres logiciels sont compatibles avec le clustering avec basculement. L'Assistant vous permet d'exécuter l'ensemble ou une partie seulement des tests de configuration. Vous devez exécuter les tests sur des serveurs et périphériques de stockage avant de configurer le cluster de basculement, puis les réexécutez après que des modifications importantes aient été apportées sur le cluster. Vous pouvez accéder aux résultats de test dans le répertoire %windir%\cluster\Reports.

Au cours de cette démonstration, vous allez apprendre à valider et à configurer un cluster.

Procédure de démonstration

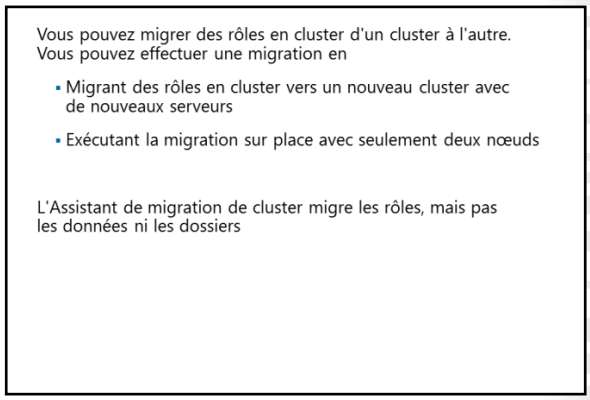
Valider et configurer un cluster

1. Démarrez le Gestionnaire du cluster de basculement sur l'ordinateur LON-SVR3.
2. Démarrez l'Assistant Validation d'une configuration.
3. Examinez le rapport.

4. Créez un cluster. Ajoutez les ordinateurs **LON-SVR3** et **LON-SVR4** en tant que nœuds de cluster.
5. Nommez le cluster **Cluster1**.
6. Utilisez l'**adresse IP 172.16.0.125**.

Migration de clusters de basculement

Dans certains scénarios, comme le remplacement des nœuds de cluster ou la mise à niveau vers une version plus récente d'un système d'exploitation Windows, vous devrez migrer des rôles en cluster ou des services d'un cluster à un autre. Dans Windows Server 2012, il est possible de migrer des rôles en cluster et une configuration de cluster depuis des clusters exécutant Windows Server 2012, Windows Server 2008 R2 ou Windows Server 2008. Vous pouvez migrer ces rôles et configurations de l'une des deux façons suivantes :



- Effectuez une migration à partir d'un cluster existant vers un nouveau cluster qui exécute Windows Server 2012. Dans ce scénario, vous avez deux nouveaux nœuds de cluster exécutant Windows Server 2012, et vous exécutez alors la migration d'un cluster existant avec des nœuds exécutant Windows Server 2008 ou toute version ultérieure.
- Exécutez une migration sur place sur un cluster doté de deux nœuds. Il s'agit d'un scénario plus complexe, où vous souhaitez migrer un cluster vers une version plus récente du système d'exploitation Windows. Dans ce scénario, vous n'avez pas d'ordinateurs supplémentaires pour les nouveaux nœuds de cluster. Par exemple, vous pouvez souhaiter mettre un cluster à niveau qui s'exécute actuellement sur Windows Server 2008 R2 vers un cluster exécutant Windows Server 2012. Pour cela, vous devez d'abord supprimer les ressources d'un nœud, puis expulser ce nœud du cluster. Ensuite, exécutez une nouvelle installation de Windows Server 2012 sur ce serveur. Après l'installation de Windows Server 2012, créez un cluster de basculement à un nœud, migrez les services et les applications en cluster de l'ancien nœud de cluster vers ce cluster de basculement, puis supprimez l'ancien nœud du cluster. La dernière étape est l'installation de Windows Server 2012 sur un autre nœud de cluster, ainsi que la fonctionnalité de cluster de basculement. Ajoutez le serveur au cluster de basculement et exécutez des tests de validation pour confirmer que la configuration globale fonctionne correctement.

L'Assistant de migration de cluster est un outil qui vous permet de migrer des rôles en cluster. Puisque l'Assistant de migration de cluster ne copie pas les données d'un emplacement de stockage à l'autre, vous devez copier ou déplacer les données ou les dossiers (notamment, les paramètres du dossier partagé) pendant une migration. En outre, l'Assistant de migration de cluster ne migre pas les informations de point de montage (informations sur les lecteurs de disque dur qui n'utilisent pas des lettres de lecteur et sont montés dans un dossier sur un autre lecteur de disque dur). Cependant, il peut migrer les paramètres des ressources de disques physiques vers et à partir des disques qui utilisent des points de montage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Configuration d'applications et de services hautement disponibles sur un cluster de basculement

Une fois que vous avez configuré votre infrastructure de clustering, vous devez configurer les rôles ou les services spécifiques pour qu'ils soient à un haut niveau de disponibilité. Tous les rôles ne peuvent pas être mis en cluster. Vous devez par conséquent d'abord identifier la ressource que vous souhaitez mettre dans un cluster, puis vérifier si cette ressource est prise en charge. Dans cette leçon, vous allez apprendre à configurer des rôles et des applications dans des clusters, et à configurer des paramètres de cluster.

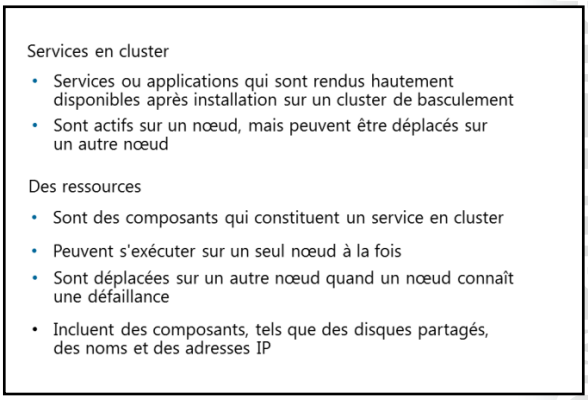
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire et identifier des ressources et des services de cluster ;
- décrire le processus pour les rôles de serveur de clustering ;
- expliquer comment mettre un rôle de serveur de fichiers en cluster ;
- expliquer comment configurer des propriétés de cluster de basculement ;
- expliquer comment gérer des nœuds de cluster ;
- expliquer comment configurer les paramètres de basculement d'application.

Identification des ressources et des services de cluster

Les services en cluster sont des services ou applications qui sont rendus hautement disponibles après installation sur un cluster de basculement. Les services en cluster sont actifs sur un nœud, mais peuvent être déplacés sur un autre nœud. Un service en cluster qui contient une ressource d'adresse IP et une ressource de nom de réseau (ainsi que d'autres ressources) est publié sur un client du réseau sous un nom de serveur unique. Étant donné que le cluster de ressources apparaît en tant que serveur logique unique pour les clients, on l'appelle une *instance de cluster*.



Les utilisateurs accèdent aux applications ou aux services sur une instance de la même manière que si les applications ou les services se trouvaient sur un serveur non-cluster. En général, les applications ou les utilisateurs ne savent pas qu'ils se connectent à un cluster ou ne connaissent pas le nœud auquel ils sont connectés.

Les ressources sont des entités physiques ou logiques, telles qu'un partage de fichiers, un disque ou une adresse IP, gérées par le cluster de basculement. Les ressources sont les unités configurables les plus fondamentales et les plus petites qui peuvent fournir un service aux clients, ou peuvent faire partie des parties importantes du cluster. À tout moment, une ressource peut s'exécuter sur un seul nœud de cluster à la fois et elle est considérée comme en ligne sur un nœud lorsqu'elle fournit son service sur ce nœud spécifique.

Ressources de cluster de serveurs

Une *ressource de cluster* est un composant physique ou logique quelconque qui présente les caractéristiques suivantes :

- Elle peut être mise en ligne et hors connexion.
- Elle peut être gérée dans un cluster de serveurs.
- Elle peut être hébergée par (appartenir à) un seul nœud à la fois.

Pour gérer des ressources, le service de cluster communique avec un DLL de ressource via un moniteur de ressources. Quand le service de cluster fait une demande de ressource, le moniteur de ressources appelle la fonction appropriée de point d'entrée dans le DLL de ressource pour contrôler l'état de la ressource.

Ressources dépendantes

Une *ressource dépendante* nécessite une autre ressource pour fonctionner. Par exemple, parce qu'un nom de réseau doit être associé à une adresse IP, un nom de réseau est considéré comme une ressource dépendante. Par conséquent, une ressource de nom de réseau dépend d'une ressource d'adresse IP. Les ressources dépendantes sont mises hors connexion avant que les ressources dont elles dépendent soient mises hors connexion. De même, elles sont mises en ligne après que les ressources dont elles dépendent soient mises en ligne. Une ressource peut spécifier une ou plusieurs ressources dont elle dépend. Les dépendances de ressources déterminent également des liaisons. Par exemple, des clients seront liés à l'adresse IP spécifique de laquelle dépend une ressource de nom de réseau.

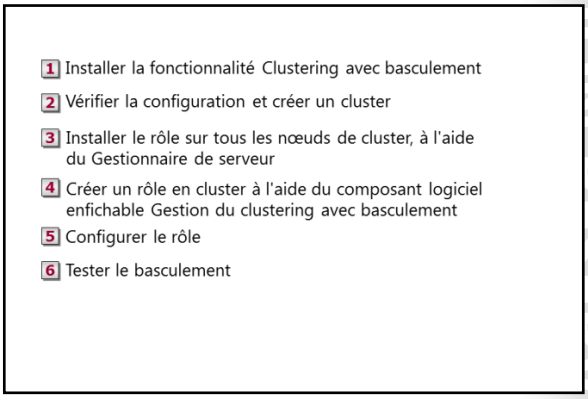
Lorsque vous créez des dépendances de ressources, soyez conscient du fait que bien que certaines dépendances soient strictement requises, d'autres ne sont pas requises mais seulement recommandées. Par exemple, un partage de fichiers qui n'est pas une racine de système de fichiers distribués (DFS) n'a aucune dépendance requise. Cependant, si la ressource de disque qui contient le partage de fichiers échoue, le partage de fichiers sera inaccessible aux utilisateurs. Par conséquent, il est logique de rendre le partage de fichiers dépendant de la ressource de disque.

Une ressource peut également spécifier une liste de nœuds sur lesquels elle peut s'exécuter. Les dépendances et les nœuds possibles sont des éléments importants à prendre en considération lorsque les administrateurs organisent les ressources dans des groupes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Processus de clustering des rôles de serveur



Le clustering avec basculement prend en charge le clustering de plusieurs rôles Windows Server, notamment Services de fichiers, DHCP et Hyper-V. Pour implémenter le clustering pour un rôle de serveur ou pour des applications externes telles que SQL Server ou Exchange Server, exécutez la procédure suivante :

1. Installez la fonctionnalité Clustering avec basculement. Utilisez le Gestionnaire de serveur, le fichier dism.exe ou Windows PowerShell pour installer la fonctionnalité Clustering avec basculement sur tous les ordinateurs qui seront des membres du cluster. Dans Windows Server 2012, vous pouvez installer des rôles et des fonctionnalités sur plusieurs serveurs simultanément à partir d'une seule console de Gestionnaire de serveur.
2. Vérifiez la configuration et créez un cluster avec les nœuds appropriés. Utilisez le composant logiciel enfichable Gestionnaire du cluster de basculement pour en premier lieu valider une configuration, puis créer un cluster avec les nœuds sélectionnés.
3. Installez le rôle sur tous les nœuds de cluster. Utilisez le Gestionnaire de serveurs, le fichier dism.exe ou Windows PowerShell pour installer le rôle de serveur que vous souhaitez utiliser dans le cluster.
4. Créez une application en cluster à l'aide du composant logiciel enfichable Gestionnaire du cluster de basculement.
5. Configurez l'application. Configurez les options sur l'application qui est utilisée dans le cluster.
6. Testez le basculement. Utilisez le composant logiciel enfichable Gestion du cluster de basculement pour tester le basculement en déplaçant intentionnellement le service d'un nœud vers un autre.

Une fois le cluster créé, vous pouvez surveiller son état à l'aide de la console Gestion du cluster de basculement et gérer les options disponibles.

Démonstration : Clustering d'un rôle de serveur de fichiers

Au cours de cette démonstration, vous allez apprendre à mettre en cluster un rôle de serveur de fichiers.

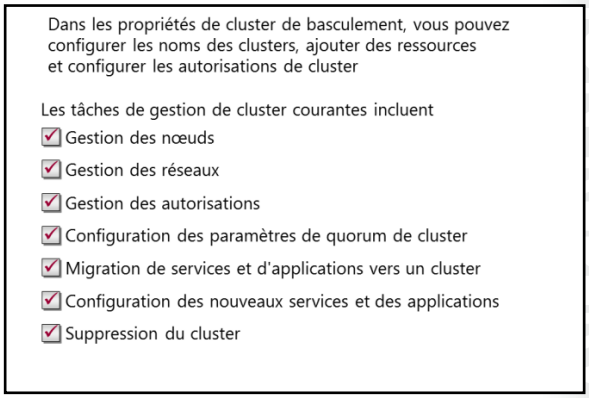
Procédure de démonstration

Mettre en cluster un rôle de serveur de fichiers

1. Sur LON-SVR3, ajoutez **Disque du cluster 2** comme stockage en cluster pour Cluster1.
2. Configurez le **serveur de fichiers** en tant que rôle de cluster.
3. Configurez un **serveur de fichiers à des fins d'indexation**.
4. Pour le nom du **point d'accès client**, tapez **Adatum-FS** et l'adresse **172.16.0.55**.
5. Utilisez **Disque du cluster 2** pour le stockage d'AdatumFS.

Configuration des propriétés de cluster de basculement

Une fois que vous créez un cluster, il offre de nombreuses propriétés que vous pouvez configurer. Lorsque vous ouvrez **Propriétés du cluster**, vous pouvez configurer ou modifier un nom de cluster, vous pouvez ajouter divers types de ressources telles qu'une adresse IP et un nom de réseau au cluster, et vous pouvez également configurer des autorisations de cluster. En configurant des autorisations, vous déterminez qui peut avoir le contrôle total sur ce contrôle spécifique et qui peut juste lire la configuration du cluster.



En outre, vous pouvez effectuer quelques tâches de gestion standard sur chaque cluster périodiquement, ou à la demande. Ces tâches incluent entre autres l'ajout et la suppression de nœuds de cluster, ainsi que la modification des paramètres de quorum. Certaines des tâches de configuration les plus souvent réalisées sont les suivantes :

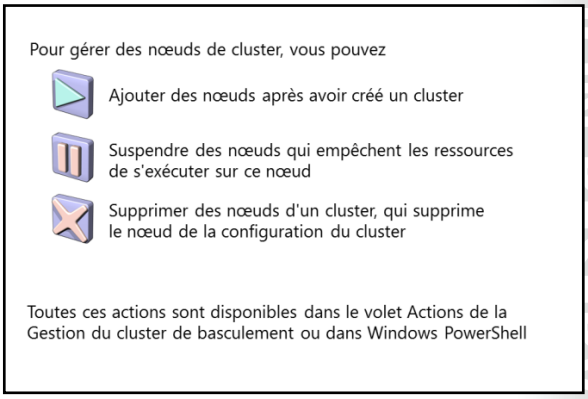
- Gestion des nœuds de cluster. Pour chaque nœud d'un cluster, vous pouvez arrêter temporairement le service de cluster, le suspendre, initialiser le bureau à distance sur le nœud ou exclure un nœud du cluster.
- Gestion des réseaux de cluster. Vous pouvez ajouter ou supprimer des réseaux de cluster, et configurer des réseaux qui seront dédiés à la communication entre les clusters.
- Gestion des autorisations. En gérant les autorisations, vous pouvez déléguer les droits d'administration d'un cluster.
- Configuration des paramètres de quorum de cluster : En configurant des paramètres de quorum, vous déterminez comment le quorum est atteint et dans un cluster peut voter.
- Migration de services et d'applications vers un cluster. Vous pouvez implémenter des services existants sur le cluster et les rendre à haut niveau de disponibilité.
- Configuration de nouveaux services et applications en vue de les utiliser dans un cluster. Vous pouvez implémenter de nouveaux services dans le cluster.
- Suppression d'un cluster. Vous pouvez supprimer un cluster si vous décidez de cesser d'utiliser le clustering, ou si vous souhaitez déplacer le cluster vers un autre ensemble de nœuds.

Vous pouvez effectuer la plupart de ces tâches d'administration à l'aide de la console Gestion du cluster de basculement, ou à l'aide de Windows PowerShell. Cependant, le fichier **Cluster.exe**, qui a été utilisé pour certaines de ces tâches dans les versions précédentes du système d'exploitation Windows Server, n'est plus pris en charge dans Windows Server 2012 et ne fait pas partie de l'installation par défaut.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des nœuds de cluster

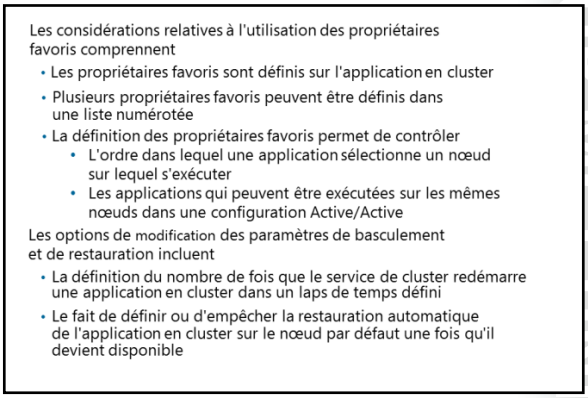
Les nœuds de cluster sont obligatoires pour chaque cluster. Une fois que vous avez créé un cluster et que vous l'avez placé en production, il est possible que vous deviez gérer occasionnellement les nœuds de cluster. Vous pouvez gérer des nœuds de cluster à l'aide de la console Gestion du cluster de basculement ou de Windows PowerShell. La gestion des nœuds de cluster comporte trois parties :



- Vous pouvez ajouter un nœud à un cluster de basculement établi en cliquant sur l'option **Ajouter un nœud** dans le volet Actions de la Gestion du cluster de basculement de la console Gestion du cluster de basculement. L'Assistant Ajout d'un nœud vous invite à fournir des informations sur le nœud supplémentaire.
- Vous pouvez suspendre un nœud pour empêcher que des ressources ne soient basculées ou déplacées vers le nœud. Un nœud est généralement suspendu si des opérations de maintenance ou de dépannage sont effectuées sur celui-ci. Lorsque vous suspendez un nœud, vous pouvez choisir de purger des rôles de ce nœud.
- Vous pouvez supprimer un nœud, processus irréversible pour un nœud de cluster. Une fois le nœud supprimé, il doit être rajouté au cluster. Un nœud est supprimé s'il est endommagé de façon irrémédiable ou s'il n'est plus requis dans le cluster. Si vous supprimez un nœud endommagé, vous pouvez le réparer ou le remplacer, puis le replacer dans le cluster à l'aide de l'Assistant Ajout d'un nœud.

Configuration des paramètres de basculement d'application

Vous pouvez régler les paramètres de basculement, y compris les propriétaires favoris et les paramètres de restauration automatique, afin de contrôler la manière dont le cluster répond en cas d'échec de l'application ou du service. Vous pouvez configurer ces paramètres dans la feuille de propriétés du service ou de l'application en cluster (dans l'onglet **Général** ou dans l'onglet **Basculement**).



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le tableau suivant fournit des exemples illustrant le fonctionnement de ces paramètres.

Paramètre	Result
Exemple 1 : Onglet **Général**, **Propriétaire favori** : **Node1** Onglet **Basculement**, paramètre **Restauration automatique** : **Autoriser la restauration automatique (Immédiatement)**	Si le service ou l'application bascule du Node1 vers le Node2, dès que le Node1 est à nouveau disponible, le service ou l'application rebascule vers le Node1.
Exemple 2 : Onglet **Basculement**, **Nombre maximal d'échecs dans la période spécifiée** : **2** Onglet **Basculement**, **Période (heures)** : **6**	Dans une période de six heures, si l'application ou le service n'échoue pas plus de deux fois, elle ou il sera redémarré ou basculé chaque fois. Si l'application ou le service échoue une troisième fois durant cette période de six heures, elle ou il sera laissé dans un état défaillant. La valeur par défaut pour le nombre maximal de défaillances est n-1, où *n* correspond au nombre de nœuds. Si vous choisissez de modifier la valeur, il est recommandé d'utiliser une valeur relativement basse. En effet, si plusieurs nœuds échouent, l'application ou le service ne sera pas déplacé indéfiniment entre les nœuds.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Maintenance d'un cluster de basculement

Une fois que l'infrastructure de cluster est opérationnelle, vous devez établir une surveillance afin d'empêcher les défaillances possibles. En outre, il est essentiel d'avoir en place des procédures de sauvegarde et de restauration pour la configuration de cluster. Windows Server 2012 offre une nouvelle technologie qui vous permet de mettre à jour les nœuds de cluster sans temps mort. Dans cette leçon, vous découvrirez la surveillance des clusters de basculement, la sauvegarde et la restauration des configurations de cluster et la mise à jour des nœuds de cluster.

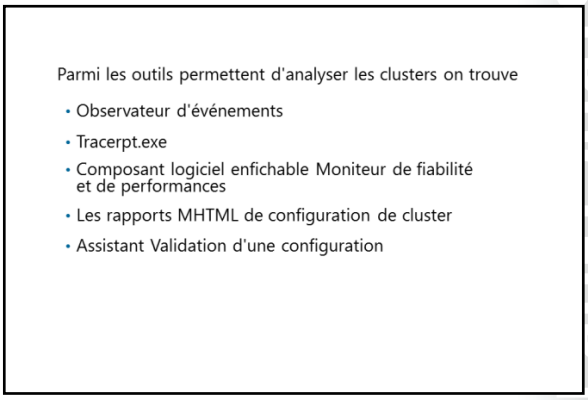
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment surveiller des clusters de basculement ;
- expliquer comment sauvegarder et restaurer une configuration de cluster de basculement ;
- expliquer comment maintenir et dépanner des clusters de basculement ;
- décrire la mise à jour adaptée aux clusters ;
- configurer la mise à jour adaptée aux clusters.

Surveillance de clusters de basculement

Il existe de nombreux outils de surveillance des clusters de basculement dans Windows Server 2012. Vous pouvez utiliser les outils standard de Windows Server, tels que l'observateur d'événements et le composant logiciel enfichable Moniteur de fiabilité et de performances, pour examiner des journaux d'événements de cluster et des mesures de performances. Vous pouvez également utiliser Tracerpt.exe pour exporter des données à des fins d'analyse. En outre, vous pouvez utiliser les rapports de configuration de clusters MHTML (Internet Mail Extension Hypertext Markup Language) et l'Assistant Validation d'une configuration pour résoudre les problèmes liés à la configuration des clusters et les changements matériels. Puisque l'outil en ligne de commande cluster.exe est déconseillé dans Windows Server 2012, vous pouvez utiliser Windows PowerShell à la place pour effectuer des tâches semblables.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Observateur d'événements

En cas de problème dans le cluster, utilisez l'observateur d'événements pour afficher les événements présentant les niveaux de gravité suivants : Critique, Erreur et Avertissement. En outre, des événements à caractère informatif sont enregistrés dans le journal Opérations de clustering avec basculement, qui peut être consulté à partir de l'observateur d'événements, dans le dossier Journaux des applications et des services\Microsoft\Windows. Les événements à caractère informatif sont généralement des opérations de cluster courantes, notamment le départ ou l'arrivée de nœuds dans un cluster, ou la mise hors connexion ou en ligne de ressources.

Dans les versions précédentes de Windows Server, les journaux d'événements étaient répliqués sur chaque nœud du cluster. Cela simplifiait la résolution des problèmes de cluster, car vous pouviez consulter tous les journaux d'événements sur un nœud de cluster unique. Windows Server 2012 ne réplique pas les journaux d'événements entre les nœuds. Cependant, le composant logiciel enfichable Gestion du cluster de basculement propose une option **Événements de cluster** qui vous permet de consulter et de filtrer les événements sur l'ensemble des nœuds de cluster. Cette fonctionnalité est utile pour mettre en corrélation des événements sur plusieurs nœuds de cluster. Le composant logiciel enfichable Gestion du cluster de basculement fournit également une option **Événements de cluster récents** qui interroge tous les événements de type Erreur et Avertissement survenus au cours des 24 heures précédentes. Vous pouvez accéder à des journaux supplémentaires, notamment les journaux d'analyse et de débogage, à partir de l'observateur d'événements. Pour consulter ces journaux, modifiez l'affichage dans le menu principal en sélectionnant l'option **Afficher les journaux d'analyse et de débogage**.

Suivi d'événements pour Windows

Le Suivi d'événement pour Windows est un composant du noyau qui est disponible tôt après le démarrage et tard au moment de l'arrêt. Il est conçu pour permettre un suivi et une remise rapides des événements vers les fichiers de suivi et les consommateurs. Étant donné qu'il est conçu pour être rapide, le Suivi d'événement pour Windows permet uniquement un filtrage in-process de base des événements en fonction d'attributs d'événement.

Le journal de suivi d'événements comprend une journalisation complète des actions de cluster de basculement. Selon la façon dont vous souhaitez afficher les données, utilisez Windows PowerShell ou le fichier Tracerpt.exe pour accéder au journal de suivi d'événements.

Tracerpt.exe analyse les journaux de suivi d'événements uniquement sur le nœud sur lequel il s'exécute. Tous les journaux individuels sont rassemblés dans un emplacement central. Pour transformer le fichier XML en fichier texte ou en fichier HTML pouvant être ouverts dans Windows Internet Explorer®, vous pouvez analyser le fichier XML à l'aide de l'utilitaire d'invite de commandes d'analyse Microsoft XSL msxsl.exe et d'une feuille de style XSL.

Composant logiciel enfichable Moniteur de fiabilité et de performances.

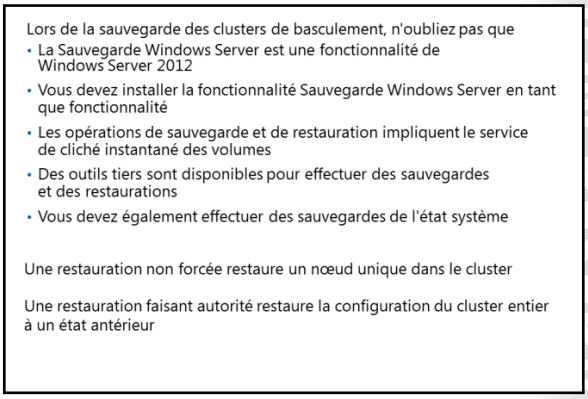
Le composant logiciel enfichable Moniteur de fiabilité et de performances vous permet d'effectuer les tâches suivantes :

- Dégagez des tendances de performances sur chaque nœud. Pour déterminer le niveau de performance d'une application, vous pouvez visualiser des informations spécifiques sur les ressources système utilisées sur chaque nœud, et dégager des tendances.
- Dégagez des tendances en matière de défaillances et de stabilité des applications sur chaque nœud. Vous pouvez indiquer exactement quand les défaillances d'application se produisent et associer les défaillances d'application à d'autres événements sur le nœud.
- Modifiez les paramètres du journal de suivi. Vous pouvez démarrer, arrêter et ajuster les journaux de suivi, y compris leur taille et emplacement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sauvegarde et restauration de la configuration de cluster de basculement

La configuration du cluster peut être un processus long avec beaucoup de détails. Par conséquent, la sauvegarde de votre configuration de cluster est importante. Vous pouvez utiliser la fonctionnalité Sauvegarde Windows Server ou un outil de sauvegarde autre que Microsoft pour effectuer des opérations de sauvegarde et de restauration de la configuration de cluster.



Lorsque vous sauvegardez la configuration de cluster, vous devez prendre en compte les éléments suivants :

- Vous devez tester votre processus de sauvegarde et restauration, avant de placer un cluster en production.
- Vous devez d'abord ajouter la fonctionnalité Sauvegarde Windows Server, si vous décidez de l'utiliser. Vous pouvez y parvenir à l'aide du Gestionnaire de serveur, du fichier dism.exe ou de Windows PowerShell.

La Sauvegarde Windows Server est la fonctionnalité intégrée de sauvegarde et restauration pour Windows Server 2012. Pour garantir l'efficacité de la sauvegarde, tenez compte des éléments suivants :

- Pour qu'une sauvegarde réussisse dans un cluster de basculement, le cluster doit s'exécuter et doit avoir le quorum. En d'autres termes, un nombre suffisant de nœuds doit s'exécuter et indiquer (peut-être avec un disque témoin ou un partage de fichiers témoin, selon la configuration de quorum) que le cluster a atteint le quorum.
- Vous devez sauvegarder toutes les applications en cluster. Si vous mettez en cluster une base de données SQL Server, vous devez avoir un plan de sauvegarde pour les bases de données et la configuration indépendant de la configuration du cluster.
- Si des données d'applications doivent être sauvegardées, les disques sur lesquels vous stockez les données doivent être rendus accessibles par le logiciel de sauvegarde. Pour ce faire, exécutez le logiciel de sauvegarde sur le nœud de cluster qui possède la ressource de disque, ou en exécutant une sauvegarde sur la ressource en cluster sur le réseau. Si vous utilisez des volumes partagés de cluster (CSV), vous pouvez exécuter la sauvegarde de n'importe quel nœud qui est joint au volume CSV.
- Le service de cluster mémorise quelle configuration de cluster est la plus récente et réplique cette configuration sur tous les nœuds de cluster. Si le cluster a un disque témoin, le service de cluster réplique également la configuration sur le disque témoin.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

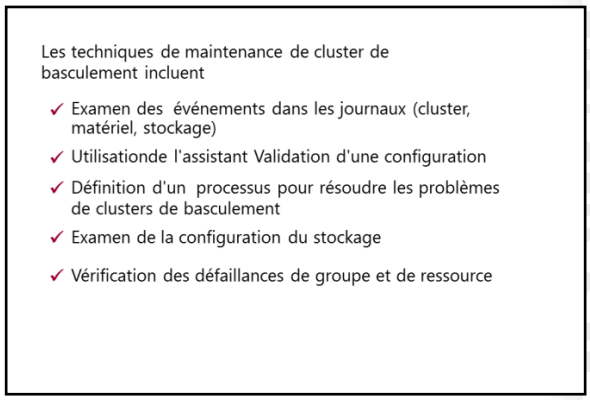
Restauration d'un cluster

Vous pouvez restaurer un cluster de deux façons :

- Restauration ne faisant pas autorité. Utilisez une restauration ne faisant pas autorité quand un seul nœud du cluster est endommagé ou reconstruit, et que le reste du cluster fonctionne correctement. Pour procéder à une restauration ne faisant pas autorité, restaurez les informations de récupération du système (état du système) sur le nœud endommagé. Quand vous redémarrez ce nœud, il intègrera le cluster et recevra automatiquement la dernière configuration de cluster.
- Restauration faisant autorité. Utilisez une restauration faisant autorité quand la configuration de cluster doit être restauré à un point antérieur dans le temps. Par exemple, vous devez utiliser une restauration faisant autorité si un administrateur a par erreur supprimé des ressources en cluster ou modifié d'autres paramètres de cluster. Pour effectuer la restauration faisant autorité, arrêtez la ressource de cluster sur chaque nœud, puis exécutez une récupération du système (état du système) sur un seul nœud en utilisant la fonctionnalité Sauvegarde Windows Server. Une fois que le nœud restauré a redémarré le service de cluster, les nœuds de cluster restants peuvent également démarrer le service de cluster.

Maintenance et résolution des clusters de basculement

La fonctionnalité de validation de cluster dans le clustering avec basculement de Windows Server 2012 empêchent les mauvaises configurations et les clusters non fonctionnels. Cependant, dans certains cas, il peut être encore nécessaire d'exécuter la maintenance ou la résolution des problèmes liés aux clusters.



Voici certaines tâches de maintenance communes qui peuvent empêcher les problèmes de configuration de cluster :

- Utilisez l'Assistant Validation d'une configuration pour identifier les problèmes de configuration qui peuvent être à l'origine des problèmes de cluster.
- Examinez les événements et les journaux de suivi de cluster pour identifier les problèmes d'application ou de matériel qui pourraient provoquer l'instabilité du cluster.
- Examinez les événements et les journaux de matériel pour identifier les composants matériels spécifiques qui pourraient provoquer l'instabilité du cluster.
- Examinez les composants de réseau SAN, les commutateurs, les cartes et les contrôleurs de stockage afin d'identifier les problèmes potentiels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans quels cas résoudre des problèmes de clusters de basculement :

- Identifier le problème perçu en rassemblant et en documentant les symptômes du problème.
- Identifier l'ampleur du problème afin de comprendre quels éléments sont affectés par le problème et l'impact de ce problème sur l'application et les clients.
- Collecter des informations afin de comprendre et d'identifier précisément l'éventuel problème. Après avoir identifié une liste de problèmes possibles, vous pouvez les classer en fonction de leur probabilité ou en fonction de l'impact d'une réparation. Si le problème ne peut pas être précisément identifié, vous devez tenter de reproduire le problème.
- Créer une planification pour réparer le problème. Par exemple, si le problème affecte seulement un groupe limité d'utilisateurs, vous pouvez retarder la réparation pendant les heures creuses afin de planifier le temps mort.
- Compléter et tester chaque réparation individuellement afin d'identifier celle qui a résolu le problème.

Pour résoudre des problèmes de réseau SAN, commencez par vérifier les connexions physiques et chacun journal de composants matériels. En outre, exécutez l'Assistant Validation d'une configuration pour vérifier que la configuration du cluster actuelle peut encore être réparée.

Remarque : Lorsque vous exécutez l'Assistant Validation d'une configuration, vérifiez que les tests de stockage que vous sélectionnez peuvent être exécutés sur un cluster de basculement en ligne. Certains tests de stockage peuvent entraîner la perte de service sur le disque en cluster au moment de leur exécution.

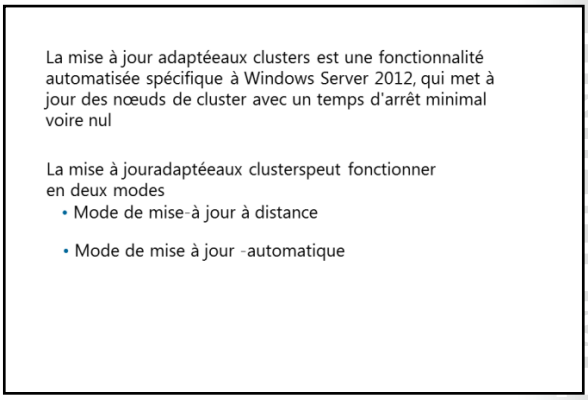
Résolution des défaillances de groupe et de ressource

Pour résoudre les défaillances de groupe et de ressource :

- Utilisez la visionneuse des dépendances dans le composant logiciel enfichable Gestion du cluster de basculement pour identifier les ressources dépendantes.
- Consultez l'observateur d'événements et les journaux de suivi afin de détecter les erreurs sur les ressources dépendantes.
- Déterminez si le problème se produit uniquement sur un nœud spécifique ou sur plusieurs nœuds, en essayant de reproduire le problème sur différents nœuds.

Qu'est-ce que la mise à jour adaptée aux clusters ?

L'application de mises à jour de système d'exploitation Windows sur les nœuds d'un cluster requiert une attention supplémentaire. Si vous souhaitez garantir un temps mort nul pour un rôle en cluster, vous devez manuellement mettre à jour les nœuds de cluster l'un après l'autre, puis déplacer manuellement des ressources du nœud en cours de mise à jour vers un autre nœud. Cette procédure peut être fastidieuse. Dans Windows Server 2012, une nouvelle fonctionnalité met automatiquement des nœuds de cluster à jour pour vous.



La mise à jour adaptée aux clusters est une fonctionnalité Windows Server 2012 qui permet aux administrateurs de mettre à jour automatiquement des nœuds de cluster, en entraînant peu ou pas de perte de disponibilité pendant le processus de mise à jour. Pendant une procédure de mise à jour, la mise à jour adaptée aux clusters place chaque nœud de cluster hors connexion de manière transparente, installe les mises à jour et les mises à jour dépendantes, exécute un redémarrage si nécessaire, replace le nœud en ligne et procède à la mise à jour du nœud suivant sur un cluster.

Pour de nombreux rôles en cluster, ce processus de mise à jour automatique déclenche un basculement planifié et il peut provoquer une interruption passagère de service pour les clients connectés. Cependant, pour des charges de travail disponibles en permanence dans Windows Server 2012, notamment Hyper-V avec la migration dynamique ou le serveur de fichiers avec le basculement transparent SMB, la mise à jour adaptée aux clusters peut orchestrer des mises à jour de cluster sans incidence sur la disponibilité des services.

Modes de mise à jour de cluster

La mise à jour adaptée aux clusters peut orchestrer l'opération complète de mise à jour de cluster dans deux modes :

- *Mode de mise à jour à distance*. Dans ce mode, un ordinateur qui exécute Windows Server 2012 ou Windows 8 est appelé orchestrateur et configuré tel quel. Pour configurer un ordinateur en tant qu'orchestrateur de mise à jour adaptée aux clusters, vous devez y installer des outils d'administration de clustering avec basculement. L'ordinateur orchestrateur n'est pas un membre du cluster qui fait l'objet de la mise à jour. À partir de l'ordinateur orchestrateur, l'administrateur déclenche une mise à jour à la demande en utilisant un profil d'Exécution de mise à jour par défaut ou personnalisé. Le mode de mise à jour à distance est utile pour surveiller la progression en temps réel de l'exécution de mise à jour et pour les clusters qui s'exécutent sur des installations minimales de Windows Server 2012.
- *Mode de mise à jour automatique*. Dans ce mode, le rôle en cluster de mise à jour adaptée aux clusters est configuré comme charge de travail sur le cluster de basculement qui doit être mis à jour, et une planification associée de mise à jour est définie. Dans ce scénario, la mise à jour adaptée aux clusters n'a pas d'ordinateur orchestrateur dédié. Le cluster se met à jour aux heures planifiées à l'aide d'un profil d'Exécution de mise à jour par défaut ou personnalisé. Pendant l'exécution de la mise à jour, le processus orchestrateur de mise à jour adaptée aux clusters démarre sur le nœud qui possède actuellement le rôle en cluster de mise à jour adaptée aux clusters, et le processus réalise des mises à jour sur chaque nœud de cluster de manière séquentielle. En mode de mise à jour automatique, la mise à jour adaptée aux clusters peut mettre à jour le cluster de basculement à l'aide d'un processus de mise à jour entièrement automatisé et de bout en bout. Dans ce mode, un administrateur peut également déclencher des mises à jour à la demande ou utiliser l'approche de mise à jour à distance. En mode de mise à jour automatique, un administrateur peut accéder à des informations résumées sur une exécution de mise à jour en cours en se connectant au cluster et en exécutant l'applet de commande Windows PowerShell **Get-CauRun**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour utiliser la mise à jour adaptée aux clusters, vous devez installer la fonctionnalité Clustering avec basculement dans Windows Server 2012 et créer un cluster de basculement. Les composants qui prennent en charge la fonctionnalité de mise à jour adaptée aux clusters sont automatiquement installés sur chaque nœud de cluster.

Vous devez également installer les outils de mise à jour adaptée aux clusters, qui sont inclus dans les outils de clustering avec basculement (qui font également partie des outils d'administration de serveur distant (RSAT, Remote Server Administration Tools)). Les outils de mise à jour adaptée aux clusters comprennent l'interface utilisateur de mise à jour adaptée aux clusters et les applets de commande Windows PowerShell de mise à jour adaptée aux clusters. Les outils de clustering avec basculement sont installés par défaut sur chaque nœud de cluster quand vous installez la fonctionnalité Clustering avec basculement. Vous pouvez également installer ces outils sur un ordinateur local ou distant qui exécute Windows Server 2012 ou Windows 8 et qui est connecté au cluster de basculement.

Démonstration : Configuration de CAU

Dans cette démonstration, vous allez voir comment configurer la mise à jour adaptée aux clusters :

Procédure de démonstration

Configurer les services CAU

1. Ajoutez la **fonctionnalité Clustering avec basculement** à LON-DC1.
2. Exécutez la fonctionnalité de **mise à jour adaptée aux clusters** sur LON-DC1 et configurez-le pour qu'il se connecte à **Cluster1**.
3. Affichez un aperçu des mises à jour disponibles pour les nœuds LON-SVR3 et LON-SVR4.
4. Examinez les options disponibles pour le profil Exécution de mise à jour.
5. Appliquez les mises à jour disponibles au **Cluster1** à partir de LON-DC1.
6. Après l'application des mises à jour, configurez **Ajouter le rôle en cluster de la mise à jour adaptée aux clusters avec la mise à jour automatique activée** sur LON-SVR3.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 5
Implémentation d'un cluster de basculement multisite

Dans certains scénarios, vous devez déployer des nœuds de cluster sur différents sites. Cela se fait généralement lors de l'établissement de solutions de récupération d'urgence. Dans cette leçon, vous découvrirez les clusters de basculement multisites et les conditions préalables pour les implémenter. Vous découvrirez également la réplication synchrone et asynchrone, ainsi que le processus de choix d'un mode de quorum pour les clusters multisites.

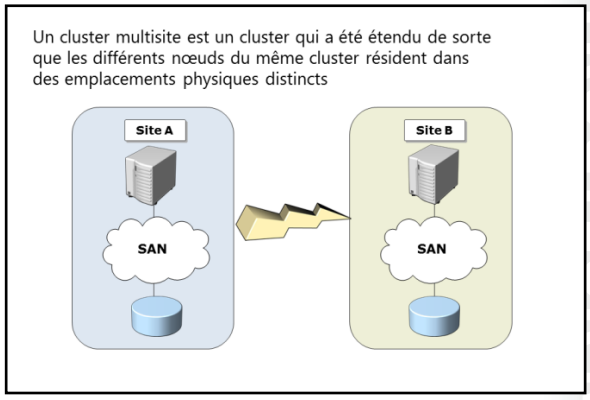
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire un cluster de basculement multisite ;
- décrire les conditions préalables pour implémenter un cluster de basculement multisite ;
- décrire des réplications synchrone et asynchrone ;
- expliquer comment choisir un mode de quorum pour les clusters multisites ;
- décrire le processus de déploiement de clusters multisites ;
- décrire les difficultés relatives à l'implémentation de clusters multisites ;

Qu'est-ce qu'un cluster de basculement multisite ?

Un cluster multisite est un cluster qui a été étendu de sorte que les différents nœuds du même cluster résident dans des emplacements physiques distincts. Un cluster multisite fournit des services à haut niveau de disponibilité disponibles dans plusieurs emplacements. Les clusters de basculement multisites peuvent résoudre plusieurs problèmes spécifiques, mais ils présentent également des difficultés spécifiques.



Dans un cluster multisite, chaque site possède habituellement un système de stockage distinct avec une réplication entre les sites. La réplication de l'espace de stockage en cluster multisite permet à chaque site d'être indépendant et fournit un accès rapide au disque local. Avec des systèmes de stockage distincts, vous ne pouvez pas partager un disque unique entre des sites.

Un cluster de basculement multisite présente trois principaux avantages dans un site de basculement, par comparaison à un serveur distant :

- Quand un site échoue, un cluster multisite fait automatiquement basculer le service ou l'application en cluster vers un autre site.
- La configuration du cluster étant automatiquement répliquée sur chaque nœud de cluster dans un cluster multisite, les coûts d'administration sont inférieurs à ceux associés à un serveur de reprise progressive qui requiert la réplication manuelle des modifications.
- L'automatisation des processus dans un cluster multisite réduit les risques d'erreur humaine, qui sont présents dans les processus manuels.

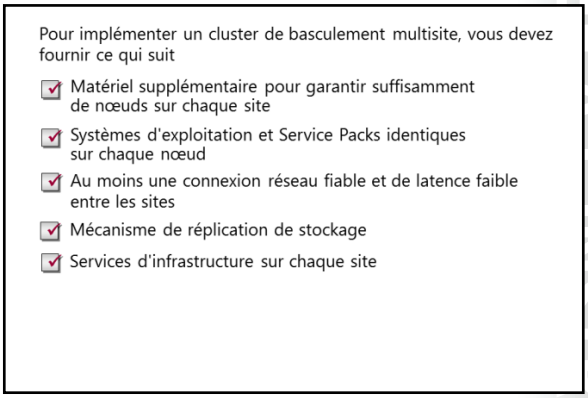
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En raison du coût et de la complexité accrus d'un cluster de basculement multisite, cela n'est peut-être pas la solution idéale pour chaque application ou entreprise. Avant d'envisager de déployer un cluster multisite, vous devez évaluer l'importance des applications pour l'entreprise, le type d'applications et l'ensemble des solutions alternatives. Certaines applications peuvent faciliter la redondance multisite grâce à la copie des journaux de transaction ou d'autres processus, tout en maintenant une disponibilité suffisante et en modérant l'augmentation des coûts et de la complexité. La Copie des journaux de transaction SQL Server, la réplication continue d'Exchange Server et la réplication DFS en sont des exemples.

La complexité d'un cluster multisite requiert une planification plus architecturale et matérielle. Elle exige également de développer des processus métier pour tester régulièrement les fonctionnalités du cluster.

Conditions préalables pour implémenter un cluster de basculement multisite

Les conditions préalables pour l'implémentation du cluster multisite sont différentes de celles de l'implémentation de cluster de site unique. Il est important de comprendre ce que vous devez préparer avant de commencer l'implémentation du cluster multisite.

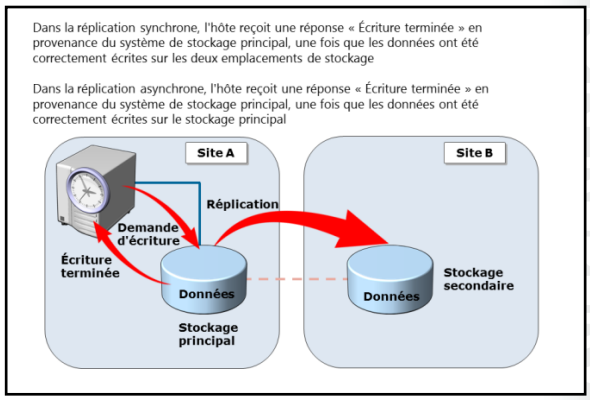


Avant d'implémenter le cluster de basculement multisite, vous devez vérifier ce qui suit :

- Vous devez avoir suffisamment de nœuds et de votes sur chaque site de sorte que le cluster puisse être en ligne même si un site est vers le bas. Cette installation requiert du matériel supplémentaire et peut engendrer des coûts financiers significatifs.
- Tous les nœuds disposent du même système d'exploitation et de la même version de Service Pack.
- Vous devez fournir au moins une connexion réseau fiable et de latence faible entre les sites. Cela est important pour les pulsations de cluster. Par défaut, quelle que soit la configuration de sous-réseau, la fréquence de pulsation (également appelé le retard de sous-réseau) se produit une fois par seconde (1 000 millisecondes). La plage de la fréquence de pulsation est d'une fois toutes les 250-2 000 millisecondes sur un sous-réseau commun et 250-4 000 millisecondes sur les sous-réseaux. Par défaut, lorsqu'un nœud manque une série de 5 pulsations, un autre nœud initialise le basculement. La plage pour cette valeur (également appelé le seuil de sous-réseau) est comprise entre 3 et 10 pulsations.
- Vous devez fournir un mécanisme de réplication de stockage. Le clustering avec basculement ne fournit aucun mécanisme de réplication de stockage, ainsi vous devez fournir une autre solution. Ceci requiert également que vous disposiez de plusieurs solutions de stockage, une pour chaque cluster que vous créez.
- Vous devez vous assurer que tous les autres services nécessaires pour le cluster, tel qu'Active Directory DS et le DNS sont également disponibles sur un deuxième site.
- Vous devez vérifier que les connexions clientes peuvent être redirigées vers un nouveau nœud de cluster lorsque le basculement se produit.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Réplication synchrone et asynchrone



Il n'est pas possible qu'un cluster de basculement géographiquement dispersé utilise le stockage partagé entre des emplacements physiques. Les liaisons de réseau étendu (WAN) sont trop lentes et présentent une latence trop importante pour prendre en charge le stockage partagé. Ceci signifie que vous devez avoir des instances de données distinctes. Pour avoir des copies exactes des données des deux côtés, les clusters de basculement dispersés géographiquement doivent synchroniser les données entre les emplacements à l'aide d'un matériel spécialisé. La réplication de données multisite peut être synchrone ou asynchrone :

- Lorsque vous utilisez la réplication synchrone, l'hôte reçoit une réponse Écriture terminée en provenance du système de stockage principal, une fois que les données ont été correctement écrites sur les deux systèmes de stockage. En cas d'échec de l'écriture des données sur les deux systèmes de stockage, l'application doit tenter d'écrire sur le disque une nouvelle fois. Avec la réplication synchrone, les deux systèmes de stockage sont identiques.
- Lorsque vous utilisez la réplication asynchrone, le nœud reçoit une réponse « Écriture terminée » en provenance du système de stockage principal, une fois que les données ont été correctement écrites sur le système de stockage principal. Les données sont écrites dans le système de stockage secondaire à un autre moment, en fonction de l'implémentation du fournisseur de matériel ou de logiciels. La réplication asynchrone peut être basée sur le système de stockage, sur l'hôte, voire sur l'application. Cependant, toutes les formes de réplication asynchrone ne sont pas suffisantes pour un cluster multisite. Par exemple, la réplication DFS fournit la réplication asynchrone au niveau des fichiers. Cependant, il ne prend pas en charge la réplication multisite de clustering avec basculement. C'est parce que la réplication DFS réplique de plus petits documents qui ne sont pas maintenus ouverts continuellement, et n'a pas été conçue pour la réplication haute vitesse de fichiers ouverts.

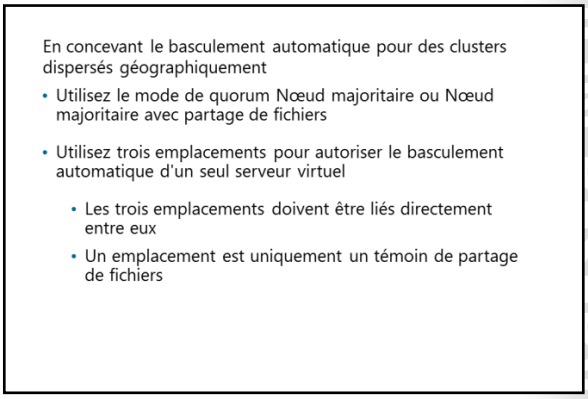
Quand utiliser la réplication synchrone ou asynchrone ?

Utilisez la réplication synchrone quand vous ne pouvez accepter aucune perte de données. Les solutions de réplication synchrone requièrent une faible latence d'écriture de disque, car l'application attend que les deux solutions de stockage reconnaissent les écritures de données. La configuration requise pour les écritures de disque à faible latence limite également la distance entre les systèmes de stockage, car une distance trop importante peut provoquer une latence plus élevée. Si la latence de disque est haute, les performances voire la stabilité de l'application peuvent être affectées.

La réplication asynchrone surmonte des limitations en matière de latence et de distance en reconnaissant les écritures de disque local uniquement, et en reproduisant l'écriture de disque sur le système de stockage distant dans une transaction distincte. Étant donné que la réplication asynchrone réalise des écritures sur le système de stockage distant après avoir écrit sur le système de stockage local, la possibilité de perte de données en cas de défaillance augmente.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sélection d'un mode de quorum pour les clusters multisites



Chaque cluster de basculement doit avoir un mode de quorum défini, de sorte qu'un vote majoritaire puisse être facilement déterminé à tout moment. Pour les clusters géographiquement dispersés, vous ne pouvez pas utiliser de configurations de quorum qui requièrent un disque partagé, car ce type de cluster n'utilise pas de disques partagés. Les modes de quorum Nœud et disque majoritaires et Pas de majorité : Disque uniquement requièrent un disque témoin partagé qui fournira un vote déterminant pour atteindre le quorum. Si le fabricant du matériel prend en charge ces deux modes de quorum et recommande de les utiliser spécifiquement, alors vous devez utiliser uniquement ces deux modes.

Pour utiliser les modes Nœud et disque majoritaires et Pas de majorité : Disque uniquement dans un cluster multisite, le disque partagé requiert que :

- vous conserviez la sémantique des commandes SCSI sur l'ensemble des sites, même en cas de panne totale de communication entre les sites ;
- vous répliquiez le disque témoin en mode synchrone dynamique sur tous les sites.

Étant donné que les clusters multisites peuvent rencontrer des pannes de réseau WAN, outre les défaillances sur le réseau local et sur les nœuds, l'utilisation des modes Nœud majoritaire et Nœud et partage de fichiers majoritaires constitue une meilleure option pour les clusters multisites. En cas de défaillance du réseau WAN entraînant la perte de communication entre le site principal et les sites secondaires, une majorité doit rester disponible pour poursuivre les opérations.

S'il y a un nombre impair de nœuds, alors utilisez le quorum Nœud majoritaire. S'il existe un nombre pair de nœuds, situation typique dans un cluster géographiquement dispersé, vous pouvez utiliser le mode de quorum Nœud majoritaire avec partage de fichiers.

Si vous utilisez le mode Nœud majoritaire et que les sites perdent la communication, vous avez besoin d'un mécanisme pour déterminer quels sont les nœuds encore actifs et quels sont les nœuds qui ont quitté le cluster. Le deuxième site exige un autre vote pour atteindre le quorum après une défaillance. Pour obtenir un nouveau vote pour le quorum, vous devez ajouter un autre nœud au cluster ou créer un témoin de partage de fichiers.

Le mode Nœud et partage de fichiers majoritaires peut aider à maintenir le quorum sans ajouter de nœud supplémentaire au cluster. Pour fournir une défaillance de site unique et activer le basculement automatique, il peut s'avérer nécessaire que le témoin de partage de fichiers existe sur un troisième site. Dans un cluster multisite, un serveur unique peut héberger le témoin de partage de fichiers. Cependant, vous devez créer un partage de fichier distinct pour chaque cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

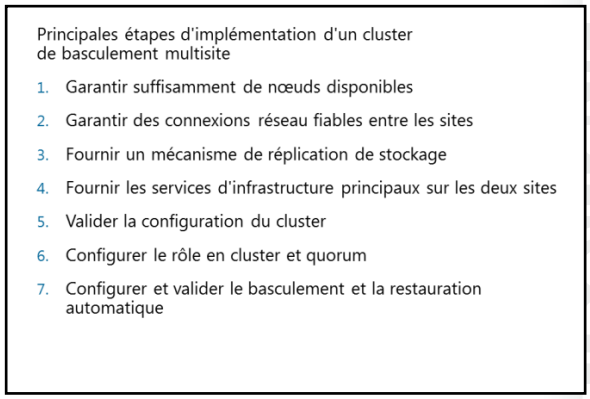
Vous devez utiliser trois emplacements pour activer le basculement automatique d'un service ou d'une application à haut niveau de disponibilité. Localisez un nœud dans l'emplacement principal qui exécute le service ou l'application à haut niveau de disponibilité. Localisez un deuxième nœud sur un site de récupération d'urgence, puis localisez le troisième nœud pour le témoin de partage de fichiers dans un autre emplacement.

Les trois emplacements doivent être directement connectés via un réseau. Ainsi, si un site devient non disponible, les deux sites restants peuvent continuer à communiquer et disposer d'un nombre suffisant de nœuds pour atteindre un quorum.

Remarque : Dans Windows Server 2008 R2, les administrateurs pouvaient configurer le quorum pour inclure des nœuds. Cependant, si la configuration de quorum comprenait des nœuds, tous les nœuds étaient traités de la même manière en fonction de leur vote. Dans Windows Server 2012, vous pouvez régler les paramètres de quorum du cluster de sorte que lorsque le cluster détermine s'il a le quorum, certains nœuds ont un vote et d'autres non. Ce réglage peut être utile quand des solutions sont implémentées sur plusieurs sites.

Procédure de configuration d'un cluster de basculement multisite

La configuration d'un cluster multisite est quelque peu différente de la configuration d'un cluster de site unique. Les clusters multisites sont plus complexes pour la configuration et la maintenance et requièrent plus de travail d'administration pour la prise en charge. Les étapes principales de configuration d'un cluster multisite sont les suivantes :



1. Assurez-vous que vous disposez de suffisamment de nœuds de cluster sur chaque site. En outre, assurez-vous que les nœuds de cluster ont des configurations matérielles semblables, et que le système d'exploitation et le Service Pack sont de version identique.
2. Assurez-vous que la mise en réseau entre les sites est opérationnelle, et que le temps de réponse du réseau est acceptable pour configurer le cluster. (Vous pouvez valider ceci à l'aide de l'Assistant Validation d'une configuration dans le gestionnaire du cluster de basculement.)
3. Assurez-vous que vous avez déployé un mécanisme de réplication de stockage fiable entre les sites. Choisissez également le type de réplication à utiliser.
4. Assurez-vous que les principaux services d'infrastructure tels qu'Active Directory DS, DNS et DHCP sont présents sur chaque site.
5. Exécutez l'Assistant Validation d'une configuration sur tous les nœuds de cluster pour déterminer si votre configuration est acceptable pour créer un cluster.

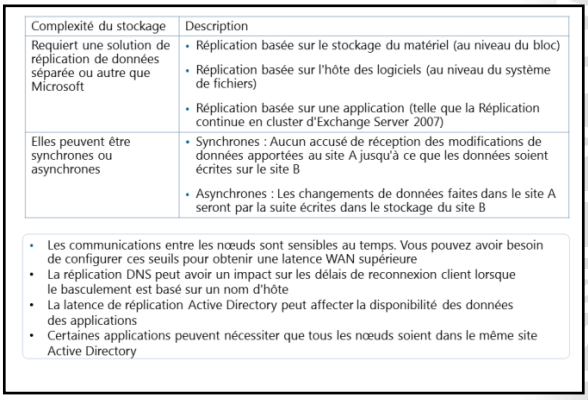
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Déterminez le rôle que vous configurerez dans un cluster.
7. Déterminez le mode de quorum du cluster que vous utiliserez.
8. Créez un rôle en cluster.
9. Configurez les paramètres de basculement/restauration automatique.
10. Validez le basculement et la restauration automatique.

Vous devez avoir conscience que les clusters multisites requièrent plus de travail d'administration pendant le basculement et la restauration automatique. Tandis que le basculement/la restauration automatique de cluster de site unique est en grande partie automatique, avec les clusters multisites, ce n'est pas le cas.

Difficultés relatives à l'implémentation d'un cluster multisite

L'implémentation de clusters multisites est plus complexe que l'implémentation de clusters sur site unique, et peut également présenter plusieurs difficultés pour l'administrateur. Le stockage et les problèmes de réseau sont les aspects les plus difficiles dans l'implémentation des clusters multisites.



Complexité du stockage	Description
Requiert une solution de réplication de données séparée ou autre que Microsoft	• Réplication basée sur le stockage du matériel (au niveau du bloc) • Réplication basée sur l'hôte des logiciels (au niveau du système de fichiers) • Réplication basée sur une application (telle que la Réplication continue en cluster d'Exchange Server 2007)
Elles peuvent être synchrones ou asynchrones	• Synchrones : Aucun accusé de réception des modifications de données apportées au site A jusqu'à ce que les données soient écrites sur le site B • Asynchrones : Les changements de données faites dans le site A seront par la suite écrites dans le stockage du site B

- Les communications entre les nœuds sont sensibles au temps. Vous pouvez avoir besoin de configurer ces seuils pour obtenir une latence WAN supérieure
- La réplication DNS peut avoir un impact sur les délais de reconnexion client lorsque le basculement est basé sur un nom d'hôte
- La latence de réplication Active Directory peut affecter la disponibilité des données des applications
- Certaines applications peuvent nécessiter que tous les nœuds soient dans le même site Active Directory

Dans un cluster multisite, les nœuds de cluster n'utilisent pas le stockage partagé. Cela signifie que chaque nœud sur chaque site doivent avoir leur propre instance de stockage. De plus, le clustering avec basculement n'inclut aucune fonctionnalité intégrée pour répliquer des données entre les sites. Pour cette raison, vous devez implémenter un mécanisme et une option de réplication de stockage distincts pour répliquer les données. Vous pouvez choisir entre trois options pour répliquer des données : la réplication de niveau bloc basée sur le matériel, la réplication de fichiers basée sur le logiciel et installée sur l'hôte, ou la réplication basée sur les applications. En fonction du scénario spécifique et des données du stockage, vous pouvez choisir l'option appropriée.

La réplication de données multisite peut être synchrone ou asynchrone. La réplication synchrone ne reconnaît pas les modifications de données qui sont apportées sur le Site A par exemple, tant que les données n'ont pas été correctement copiées sur le Site B. Avec la réplication asynchrone, les modifications de données qui sont apportées sur le Site A sont ultérieurement écrites sur le Site B.

Lorsque vous déployez un cluster multisite et exécutez l'Assistant Validation d'une configuration, les tests de disque ne trouveront aucun stockage partagé et par conséquent ne fonctionneront pas. Cependant, vous pouvez tout de même créer un cluster de basculement. Si vous suivez les recommandations du fabricant de matériel relatives au matériel de clustering avec basculement Windows Server, Microsoft prendra en charge la solution.

Windows Server 2012 permet l'existence de nœuds de cluster sur différents sous-réseaux IP, ce qui permet à une application ou un service en cluster de modifier son adresse IP en fonction du sous-réseau IP. Le système DNS met à jour l'enregistrement DNS de l'application en cluster de sorte que les clients puissent localiser la modification d'adresse IP. Étant donné que les clients utilisent le système DNS pour rechercher un service ou une application après un basculement, vous devrez peut-être ajuster la **durée de vie** des enregistrements DNS et la vitesse de réplication des données DNS. En outre, lorsque des nœuds de cluster se trouvent sur plusieurs sites, la latence du réseau pourra exiger que vous modifiiez le délai de communication entre les nœuds (pulsation) et les seuils d'expiration du délai d'attente.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation du clustering avec basculement

Scénario

À mesure que l'entreprise A. Datum Corporation se développe, il devient de plus en plus important qu'une grande partie des applications et des services du réseau soient disponibles à tout moment. A. Datum possède de nombreux services et applications qui doivent être disponibles pour les utilisateurs internes et externes travaillant dans différents fuseaux horaires partout dans le monde. Puisque plusieurs de ces applications ne peuvent pas être hautement disponibles à l'aide de l'équilibrage de la charge réseau (NLB, Network Load Balancing), vous devrez utiliser une technologie différente.

En tant qu'administrateur réseau expérimenté chez A. Datum, vous serez responsable d'implémenter le clustering avec basculement sur les serveurs Windows Server 2012 afin de garantir la haute disponibilité des services et des applications réseau. Vous devrez également planifier la configuration de cluster de basculement et déployer des applications et des services sur le cluster de basculement.

Objectifs

- Configurer un cluster de basculement avec le stockage de CSV.
- Déployer et configurer des applications et des services hautement disponibles sur un cluster de basculement ;
- Valider la haute disponibilité du cluster de basculement et du stockage.
- Configurer la mise à jour adaptée aux clusters sur le cluster de basculement.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **22412B-LON-SVR3** **22412B-LON-SVR4** **MSL-TMG1**
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22412B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22412B-LON-SVR1**, **22412B-LON-SVR3** et **22412B-LON-SVR4**.
6. Pour **MSL-TMG1**, répétez uniquement l'étape 2.

Exercice 1 : Configuration d'un cluster de basculement

Scénario

L'entreprise A. Datum possède des applications et des services importants qu'elle souhaite rendre hautement disponibles. Certains de ces services ne peuvent pas utiliser l'équilibrage de la charge réseau (NLB). Par conséquent, vous avez décidé d'implémenter le clustering avec basculement avec l'utilisation du stockage iSCSI, qui est déjà en place. Pour démarrer ce processus, vous devez implémenter les composants principaux pour le clustering avec basculement, valider le cluster, puis créer le cluster de basculement.

Les tâches principales de cet exercice sont les suivantes :

1. Connecter les nœuds de cluster aux cibles iSCSI (Internet Small Computer System Interface)
2. Installer la fonctionnalité Clustering avec basculement
3. Valider les serveurs pour le clustering avec basculement
4. Créer le cluster de basculement
5. Configurer les volumes partagés de cluster (CSV)

▶ Tâche 1 : Connecter les nœuds de cluster aux cibles iSCSI (Internet Small Computer System Interface)

1. Sur LON-SVR3, démarrez l'**Initiateur iSCSI** et configurez **Découvrir un portail** avec l'adresse IP **172.16.0.21**.
2. Connectez-vous à la cible découverte dans la liste **Cibles**.
3. Répétez les étapes 1 et 2 sur **LON-SVR4**.
4. Sur **LON-SVR3**, ouvrez l'outil **Gestion des disques**.
5. Mettez les trois nouveaux disques en ligne, puis initialisez-les.
6. Créez un volume simple sur chaque disque et formatez-le avec le système NTFS.
7. Sur LON-SVR4, ouvrez **Gestion des disques**, actualisez la console et mettez en ligne les trois nouveaux disques, puis initialisez-les.

▶ Tâche 2 : Installer la fonctionnalité Clustering avec basculement

1. Sur LON-SVR3, installez la fonctionnalité **Clustering avec basculement** à l'aide du Gestionnaire de serveur.
2. Sur LON-SVR4, installez la fonctionnalité **Clustering avec basculement** à l'aide du Gestionnaire de serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Valider les serveurs pour le clustering avec basculement

1. Sur LON-SVR3, ouvrez la console **Gestionnaire du cluster de basculement**.
2. Démarrez l'**Assistant Validation d'une configuration**.
3. Utilisez les ordinateurs **LON-SVR3** et **LON-SVR4** en tant que nœuds pour le test.
4. Consultez le rapport, puis fermez-le.
5. Sur la page **Résumé**, décochez la case en regard de **Créer le cluster maintenant en utilisant les nœuds validés**, puis cliquez sur **Terminer**.

▶ Tâche 4 : Créer le cluster de basculement

1. Sur LON-SVR3, dans le Gestionnaire du cluster de basculement, démarrez l'**Assistant Création d'un cluster**.
2. Utilisez les ordinateurs LON-SVR3 et LON-SVR4 en tant que nœuds de cluster.
3. Spécifiez **Cluster1** comme **Nom du point d'accès au cluster**.
4. Spécifiez l'**Adresse IP 172.16.0.125**.

▶ Tâche 5 : Configurer les volumes partagés de cluster (CSV)

1. Sur LON-SVR3, dans la console Gestionnaire du cluster de basculement, naviguez jusqu'à **Stockage->Disques**.
2. Localisez le disque qui est attribué à **Stockage disponible**. (Si possible, utilisez le disque du cluster 2).
3. Ajoutez-le à **Volumes partagés de cluster**.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré la fonctionnalité Clustering avec basculement.

Exercice 2 : Déploiement et configuration d'un serveur de fichiers hautement disponibles

Scénario

Dans la société A. Datum Corporation, Services de fichiers est l'un des services importants qui doit être hautement disponible, parce qu'il héberge des données très importantes qui sont utilisées à tout moment. Une fois que vous avez créé une infrastructure de cluster, vous décidez de configurer un serveur de fichiers hautement disponible et d'implémenter des paramètres de basculement et de restauration automatique.

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter l'application de serveur de fichiers au cluster de basculement
2. Ajouter un dossier partagé à un serveur de fichiers à haut niveau de disponibilité
3. Configurer les paramètres de basculement et de restauration automatique
4. Valider des paramètres de quorum de cluster

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Ajouter l'application de serveur de fichiers au cluster de basculement

1. Ajoutez le service de rôle de **serveur de fichiers** à LON-SVR3 et LON-SVR4.
2. Sur LON-SVR3, ouvrez la console Gestionnaire du cluster de basculement.
3. Ajoutez un **Serveur de fichiers** en tant que rôle de cluster.
4. Choisissez d'implémenter le **serveur de fichiers avec montée en puissance parallèle pour les données d'application**.
5. Spécifiez **AdatumFS** comme **Nom d'accès client**.

▶ Tâche 2 : Ajouter un dossier partagé à un serveur de fichiers à haut niveau de disponibilité

1. Sur LON-SVR3, dans le Gestionnaire du cluster de basculement, démarrez l'Assistant Nouveau partage pour ajouter un nouveau dossier partagé au rôle de cluster AdatumFS.

Remarque : Si vous recevez un message d'erreur qui indique que le cluster est encore indisponible, attendez une minute et redémarrez le gestionnaire du cluster de basculement sur un autre nœud.

2. Spécifiez le profil du partage en tant que **Partage SMB - Rapide**.
3. Nommez le dossier partagé **Data**.
4. Activez la **disponibilité continue**.

▶ Tâche 3 : Configurer les paramètres de basculement et de restauration automatique

1. Sur LON-SVR3, dans le Gestionnaire du cluster de basculement, ouvrez **Propriétés** pour le rôle de cluster **AdatumFS**.
2. Activez la restauration automatique entre **4** et **5** heures.
3. Sélectionnez **LON-SVR3** et **LON-SVR4** en tant que propriétaires favoris.
4. Déplacez **LON-SVR4** pour qu'il apparaisse en tête de la liste Propriétaires favoris.

▶ Tâche 4 : Valider des paramètres de quorum de cluster

- Dans la console Gestionnaire du cluster de basculement, vérifiez le paramétrage de la **Configuration de Quorum**. Il devrait être défini sur **Nœud et disque majoritaires**.

Résultats : À la fin de cet exercice, vous aurez déployé et configuré un serveur de fichiers à haut niveau de disponibilité.

Exercice 3 : Validation du déploiement du serveur de fichier hautement disponibles

Scénario

Lors du processus d'implémentation d'un cluster de basculement, vous pouvez envisager de réaliser des essais de basculement et de restauration automatique pour vérifier que le cluster fonctionne correctement.

Les tâches principales de cet exercice sont les suivantes :

1. Valider le déploiement du serveur de fichiers à haut niveau de disponibilité
2. Valider la configuration de basculement et de quorum pour le rôle de serveur de fichiers

▶ Tâche 1 : Valider le déploiement du serveur de fichiers à haut niveau de disponibilité

1. Sur LON-DC1, ouvrez l'Explorateur Windows et essayez d'accéder à l'emplacement **\\AdatumFS**. Vérifiez que vous pouvez accéder au dossier **Data**.
2. Créez un document texte de test dans ce dossier.
3. Sur LON-SVR3, dans le Gestionnaire du cluster de basculement, déplacez **AdatumFS** vers le deuxième nœud.
4. Sur LON-DC1, dans l'Explorateur Windows, vérifiez que vous pouvez encore accéder à **\\AdatumFS**.

▶ Tâche 2 : Valider la configuration de basculement et de quorum pour le rôle de serveur de fichiers

1. Sur LON-SVR3, déterminez le propriétaire actuel pour le rôle **AdatumFS**.
2. Arrêtez le service de cluster sur le nœud qui est le propriétaire actuel du rôle **AdatumFS**.
3. Vérifiez qu'**AdatumFS** a été déplacé vers un autre nœud et que l'emplacement **\\AdatumFS** est encore disponible sur l'ordinateur LON-DC1.
4. Démarrez le service de **cluster** sur le nœud dans lequel vous l'avez arrêté à l'étape 2.
5. À partir du nœud **Disques**, mettez le témoin de disque hors connexion.
6. Vérifiez que l'emplacement **\\AdatumFS** est encore disponible sur l'ordinateur LON-DC1.
7. Remettez le témoin de disque en ligne.

Résultats : À la fin de cet exercice, vous aurez testé les scénarios de basculement et de restauration automatique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Configuration de la mise à jour adaptée aux clusters sur le cluster de basculement

Scénario

Plus tôt, l'implémentation des mises à jour aux serveurs avec le service critique provoquait du temps mort non désiré. Pour activer une mise à jour de cluster transparente et sans temps mort, vous devez implémenter la fonctionnalité Mise à jour adaptée aux clusters et tester les mises à jour pour les nœuds de cluster.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer la mise à jour adaptée aux clusters (CAU)
2. Mettre à jour le cluster de basculement et configurer la mise à jour automatique

▶ Tâche 1 : Configurer la mise à jour adaptée aux clusters (CAU)

1. Sur LON-DC1, installez la fonctionnalité **Clustering avec basculement**.
2. Dans le Gestionnaire de serveur, ouvrez la **mise à jour adaptée aux clusters**.
3. Connectez-vous à **Cluster1**.
4. Affichez un aperçu des mises à jour disponibles pour les nœuds dans **Cluster1**.

Remarque : une connexion Internet est requise pour compléter cette étape. Vérifiez que le serveur MSL-TMG1 est opérationnel et que vous pouvez accéder à Internet sur LON-DC1.

Remarque : Dans un environnement de production, nous ne recommandons pas de déployer les outils CAU sur un contrôleur de domaine. Cela ne s'applique qu'à l'atelier pratique.

▶ Tâche 2 : Mettre à jour le cluster de basculement et configurer la mise à jour automatique

1. Sur LON-DC1, commencez le processus de mise à jour pour **Cluster1**.
2. À la fin du processus, ouvrez une session sur LON-SVR3 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
3. Sur LON-SVR3, ouvrez la mise à jour adaptée aux clusters et configurez la **mise à jour automatique pour Cluster1**, pour qu'elle soit **Chaque semaine**, le **Dimanche** à **04h00**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré la mise à jour adaptée aux clusters sur le cluster de basculement.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-SVR3**, **22412B-LON-SVR4** et **MSL-TMG1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Pourquoi l'utilisation d'une configuration de quorum Pas de majorité : Disque uniquement est-elle généralement déconseillée ?

Question : Quel est l'objectif de la mise à jour adaptée aux clusters ?

Question : Quelle est la principale différence entre la réplication synchrone et asynchrone dans un scénario de cluster multisite ?

Question : Qu'est-ce qu'une fonctionnalité améliorée dans les clusters multisites Windows Server 2012 ?

Problèmes réels et scénarios

Question : Votre entreprise envisage d'utiliser un cluster géographiquement dispersé qui inclut un centre de données alternatif. Votre entreprise possède un seul site physique, ainsi qu'un centre de données alternatif. Cette configuration vous permet-elle de fournir un basculement automatique ?

Outils

Les outils d'implémentation du clustering avec basculement comprennent :

- la console Gestionnaire du cluster de basculement ;
- la console Mise à jour adaptée aux clusters ;
- Windows PowerShell
- Gestionnaire de serveur
- Initiateur iSCSI
- Gestion des disques

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11

Implémentation du clustering avec basculement à l'aide d'Hyper-V

Table des matières :

Vue d'ensemble du module **11-1**

Leçon 1 : Vue d'ensemble de l'intégration d'Hyper-V au clustering avec basculement **11-2**

Leçon 2 : Implémentation des ordinateurs virtuels d'Hyper-V sur des clusters de basculement **11-9**

Leçon 3 : Implémentation des déplacements d'ordinateurs virtuels Hyper-V **11-19**

Leçon 4 : Gestion des environnements virtuels Hyper-V à l'aide de VMM **11-27**

Atelier pratique : Implémentation du clustering avec basculement à l'aide d'Hyper-V **11-39**

Contrôle des acquis et éléments à retenir **11-45**

Vue d'ensemble du module

La virtualisation de serveur présente l'avantage de fournir une haute disponibilité aux applications ou aux services qui ont la fonctionnalité de haute disponibilité intégrée et aux applications ou aux services qui ne fournissent pas la haute disponibilité autrement. Avec la technologie Hyper-V® pour Windows Server 2012®, de clustering avec basculement et Microsoft® System Center 2012 – Virtual Machine Manager (VMM), vous pouvez configurer la haute disponibilité à l'aide de plusieurs options différentes.

Dans ce module, vous allez apprendre à implémenter le clustering avec basculement dans un scénario Hyper-V pour mettre en œuvre un environnement virtuel à haut niveau de disponibilité. Vous découvrirez également les fonctionnalités de base des ordinateurs virtuels.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire l'intégration d'Hyper-V avec clustering avec basculement ;
- implémenter des ordinateurs virtuels Hyper-V sur des clusters de basculement ;
- implémenter des déplacements d'ordinateurs virtuels Hyper-V ;
- gérer un environnement virtuel Hyper-V à l'aide de VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1

Vue d'ensemble de l'intégration d'Hyper-V au clustering avec basculement

Le clustering avec basculement est une fonctionnalité Windows Server 2012 qui vous permet de rendre des applications ou des services à haut niveau de disponibilité. Afin de rendre les ordinateurs virtuels à haut niveau de disponibilité dans un environnement Hyper-V, vous devez implémenter le clustering avec basculement sur les ordinateurs hôtes Hyper-V.

Cette leçon propose un résumé des options de haute disponibilité pour les ordinateurs virtuels Hyper-V, et se concentre ensuite sur le fonctionnement du clustering avec basculement ainsi que sur la manière de concevoir et d'implémenter le clustering avec basculement pour Hyper-V.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options permettant de rendre les ordinateurs virtuels à haut niveau de disponibilité ;
- décrire le fonctionnement du clustering avec basculement avec les nœuds Hyper-V ;
- décrire les nouvelles fonctionnalités de clustering avec basculement pour Hyper-V dans Windows Server 2012 ;
- décrire les méthodes conseillées pour implémenter la haute disponibilité dans un environnement virtuel.

Options permettant de rendre à haut niveau de disponibilité les ordinateurs virtuels

Pour la plupart des organisations, certaines applications sont cruciales et doivent être à haut niveau de disponibilité. Pour rendre une application à haut niveau de disponibilité, vous devez la déployer dans un environnement fournissant une redondance pour tous les composants requis par l'application. Pour que les ordinateurs virtuels soient à haut niveau de disponibilité, vous avez le choix entre plusieurs options :

Options de haute disponibilité	Description
Clustering d'hôtes	• Les ordinateurs virtuels sont hautement disponibles • Ne requiert pas de système d'exploitation ni d'application de l'ordinateur virtuel pour prendre en charge les clusters
Clustering d'invités	• Les ordinateurs virtuels sont des nœuds de cluster de basculement • Les applications d'ordinateurs virtuels doivent prendre en charge les clusters • Requiert une interface iSCSI ou Fibre Channel virtuel pour les connexions au stockage partagé
NLB	• Les ordinateurs virtuels sont des nœuds de cluster d'équilibrage de la charge réseau • Utilisé pour les applications Web

- Clustering d'hôtes avec lequel vous implémentez des hôtes de virtualisation en tant que rôle de cluster
- Clustering d'invité avec lequel vous implémentez le clustering à l'intérieur des ordinateurs virtuels
- Équilibrage de la charge réseau à l'intérieur des ordinateurs virtuels

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Clustering d'hôtes

Le clustering d'hôtes vous permet de configurer un cluster de basculement en utilisant des serveurs hôtes Hyper-V. Lorsque vous configurez le clustering hôte pour Hyper-V, vous configurez l'ordinateur virtuel en tant que ressource à haut niveau de disponibilité. La protection par basculement est implémentée au niveau du serveur hôte. Autrement dit, le système d'exploitation invité et les applications exécutées sur l'ordinateur virtuel ne doivent pas être configurés pour prendre en charge les clusters. Cependant, l'ordinateur virtuel est toujours à haut niveau de disponibilité. Voici quelques exemples des applications ne prenant pas en charge les clusters : les serveurs d'impression ou les applications en réseau propriétaires telle qu'une application de comptabilité. Si le nœud hôte qui contrôle l'ordinateur virtuel devient indisponible de façon inattendue, le nœud hôte secondaire prend le contrôle et redémarre l'ordinateur virtuel aussi rapidement que possible.

Vous pouvez également déplacer, de manière contrôlée, l'ordinateur virtuel d'un nœud du cluster à un autre. Par exemple, vous pourriez déplacer l'ordinateur virtuel d'un nœud à l'autre tout en corrigeant le système d'exploitation d'hôtes. Les applications ou services exécutés sur l'ordinateur virtuel n'ont pas besoin d'être compatibles avec le clustering avec basculement, ni de savoir que l'ordinateur virtuel est mis en cluster. Étant donné que le basculement se situe au niveau de l'ordinateur virtuel, cela ne dépend pas du logiciel qui est installé à l'intérieur de l'ordinateur virtuel.

Clustering d'invités avec basculement

Vous configurez le clustering d'invités avec basculement de manière très similaire au clustering avec basculement sur un serveur physique, à l'exception près que les nœuds de cluster comprennent plusieurs ordinateurs virtuels. Dans ce scénario, vous créez deux ordinateurs virtuels ou plus, et activez le clustering avec basculement dans le système d'exploitation invité. L'application ou le service est alors activé pour une haute disponibilité entre les ordinateurs virtuels à l'aide du clustering avec basculement dans chaque ordinateur virtuel. Puisque le clustering avec basculement est implémenté dans chaque système d'exploitation invité du nœud d'ordinateur virtuel, vous pouvez localiser les ordinateurs virtuels sur un hôte unique. Ceci peut être une configuration rapide et rentable dans un environnement de test ou de transfert.

Pour des environnements de production, toutefois, vous pouvez protéger l'application ou le service de manière plus robuste si vous déployez les ordinateurs virtuels sur des ordinateurs hôtes distincts Hyper-V prenant en charge le clustering avec basculement. Avec l'implémentation du clustering avec basculement à la fois au niveau de l'hôte et au niveau de l'ordinateur virtuel, la ressource peut être redémarrée, peu importe si le nœud qui échoue est un ordinateur virtuel ou un hôte. Ce type de configuration est également connu en tant que *Cluster invité entre hôtes*. Cette configuration est considérée comme à haut niveau de disponibilité pour les ordinateurs virtuels exécutant des applications critiques dans un environnement de production.

Plusieurs facteurs doivent être pris en compte lors de l'implémentation du clustering invité :

- L'application ou le service doit prendre en charge le cluster de basculement. Cela inclut tous les services Windows Server 2012 qui prennent en charge les clusters, ainsi que toutes les applications, telles que Microsoft SQL Server® et Microsoft Exchange Server.
- Les ordinateurs virtuels Hyper-V peuvent utiliser les connexions Fibre Channel au stockage partagé (uniquement spécifique à Microsoft Hyper-V Server 2012) ou vous pouvez implémenter des connexions iSCSI (Internet Small Computer System Interface) des ordinateurs virtuels au stockage partagé.

Vous devez déployer plusieurs cartes réseau sur les ordinateurs hôtes et les ordinateurs virtuels. Dans l'idéal, lorsque vous utilisez une connexion iSCSI, vous devez consacrer une connexion réseau à la connexion iSCSI, au réseau privé entre les hôtes et à la connexion réseau utilisée par les ordinateurs clients.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Équilibrage de la charge réseau

L'équilibrage de la charge réseau fonctionne avec les ordinateurs virtuels comme il fonctionne avec des hôtes physiques. L'équilibrage de la charge réseau distribue le trafic IP à plusieurs instances d'un service TCP/IP, telles qu'un serveur Web en cours d'exécution sur un hôte au sein du cluster d'équilibrage de charge réseau. L'équilibrage de la charge réseau distribue de manière transparente les demandes des clients parmi les hôtes et permet aux clients d'accéder au cluster à l'aide d'un nom d'hôte virtuel ou d'adresses IP virtuelles. Du point de vue de l'ordinateur client, le cluster semble être un seul serveur répondant à ses demandes. À mesure que le trafic de l'entreprise augmente, vous pouvez ajouter un autre serveur au cluster.

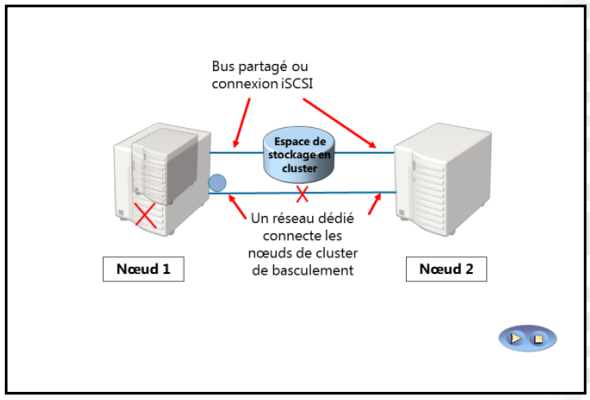
Par conséquent, l'équilibrage de la charge réseau est une solution appropriée pour les ressources qui ne doivent pas prendre en charge les demandes de lecture/écriture exclusive. Des exemples d'applications appropriées à l'équilibrage de la charge réseau s'étendent des applications Web frontales aux applications de base de données ou les serveurs d'accès au client Exchange Server.

Lorsque vous configurez un cluster d'équilibrage de la charge réseau, vous devez installer et configurer l'application sur tous les ordinateurs virtuels. Après la configuration de l'application, installez la fonctionnalité d'équilibrage de la charge réseau dans Windows Server 2012 dans chaque système d'exploitation invité de l'ordinateur virtuel (pas sur les hôtes Hyper-V), puis configurez un cluster d'équilibrage de la charge réseau pour l'application. Les versions antérieures de Windows Server prennent également en charge l'équilibrage de la charge réseau, ce qui signifie que le système d'exploitation invité n'est pas uniquement limité à Windows Server 2012. Comme pour un cluster invité entre hôtes, la ressource d'équilibrage de la charge réseau tire généralement profit de l'amélioration accrue des performances d'E/S lorsque les nœuds d'ordinateur virtuel sont situés sur différents hôtes Hyper-V.

Remarque : Comme avec les versions antérieures de Windows Server, l'équilibrage de la charge réseau et le clustering avec basculement ne doivent pas être implémentés dans le même système d'exploitation invité, car les deux technologies entrent en conflit.

Comment fonctionne un cluster de basculement avec des nœuds Hyper-V ?

Lorsque vous implémentez le clustering avec basculement et que vous configurez les ordinateurs virtuels comme des ressources à haut niveau de disponibilité, le cluster de basculement traite les ordinateurs virtuels comme tout autre service ou toute autre application. Notamment, si un hôte est défaillant, le clustering avec basculement restaurera l'accès à l'ordinateur virtuel aussi rapidement que possible sur un autre hôte dans le cluster. Seul un nœud à la fois exécute l'ordinateur virtuel. Cependant, vous pouvez également déplacer l'ordinateur virtuel vers tout autre nœud dans le même cluster.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le processus de basculement transfère la responsabilité de l'accès aux ressources dans un cluster d'un nœud à l'autre. Le basculement peut se produire, par exemple, lorsqu'un administrateur déplace des ressources vers un autre nœud à des fins de maintenance ou pour d'autres raisons, ou lorsqu'un temps mort non planifié se produit sur un nœud à la suite d'une défaillance matérielle ou pour d'autres raisons.

Le processus de basculement se déroule en plusieurs étapes :

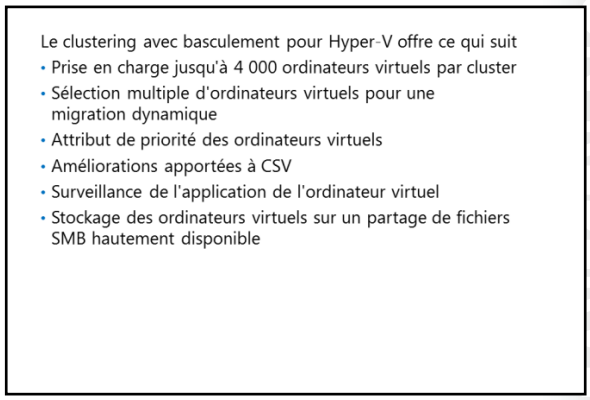
1. Le nœud sur lequel l'ordinateur virtuel est en cours d'exécution possède l'instance en cluster de l'ordinateur virtuel, contrôle l'accès au bus partagé ou la connexion iSCSI au stockage en cluster et est propriétaire de tous les disques, ou numéros d'unité logique (LUN) qui sont attribués à l'ordinateur virtuel. Tous les nœuds dans le cluster utilisent un réseau privé pour s'envoyer des signaux réguliers, connus en tant que *signaux de pulsation*, les uns aux autres. La pulsation signale qu'un nœud fonctionne et communique sur le réseau. La configuration de pulsation par défaut spécifie que chaque nœud envoie une pulsation par seconde (ou 1 000 millisecondes) sur le port 3343 TCP/UDP.
2. Le basculement débute lorsque le nœud hébergeant l'ordinateur virtuel n'envoie pas aux autres nœuds des signaux de pulsation réguliers sur le réseau. Par défaut, cela correspond à cinq pulsations consécutives manquées (ou 5 000 millisecondes). Le basculement peut se produire en raison d'une défaillance de nœud ou de réseau.
3. Lorsque les signaux de pulsation cessent d'être émis par le nœud défectueux, un des autres nœuds du cluster lance la récupération des ressources utilisées par les ordinateurs virtuels. Vous définissez le(s) nœud(s) qui pourrai(en)t continuer à fonctionner en configurant les propriétés **Propriétaires possibles et favoris**. Le propriétaire favori spécifie la hiérarchie de la propriété s'il y a plus d'un nœud de basculement possible pour une ressource. Par défaut, tous les nœuds appartiennent aux propriétaires possibles. Par conséquent, la suppression d'un nœud en tant que propriétaire possible l'empêche absolument de récupérer la ressource en cas de défaillance.

   Supposez, par exemple, que vous implémentez un cluster de basculement à l'aide de trois nœuds. Cependant, seulement deux nœuds sont configurés en tant que propriétaires possibles. Au cours d'un événement de basculement, la ressource peut être encore récupérée par le troisième nœud si aucun des propriétaires favoris n'est en ligne. Bien que le troisième nœud ne soit pas configuré comme propriétaire favori, dans la mesure où il demeure un propriétaire possible, le cluster de basculement peut l'utiliser si nécessaire pour restaurer l'accès à la ressource.

   Les ressources sont mises en ligne dans l'ordre de dépendance. Par exemple, si l'ordinateur virtuel fait référence à un numéro d'unité logique iSCSI, l'accès aux adaptateurs de bus hôte (HBA), réseaux et numéros d'unité logique appropriés sera enregistré dans cet ordre. Le basculement est terminé lorsque toutes les ressources sont en ligne sur le nouveau nœud. Pour les clients interagissant avec la ressource, il y a une brève interruption de service, que la plupart des utilisateurs ne remarqueront pas.
4. Vous pouvez également configurer le service de cluster pour une restauration automatique sur le nœud hors connexion une fois qu'il redevient actif. Quand le service de cluster se restaure automatiquement, il utilise les mêmes procédures auxquelles il a recours pendant le basculement. Autrement dit, le service de cluster déconnecte toutes les ressources associées avec cette instance, déplace l'instance, puis remet toutes les ressources de l'instance en ligne.

Nouveautés en matière de clustering avec basculement pour Windows Server 2012 Hyper-V

Dans Windows Server 2012, le clustering avec basculement a été fortement amélioré avec les clusters Hyper-V. Parmi les principales améliorations, citons :

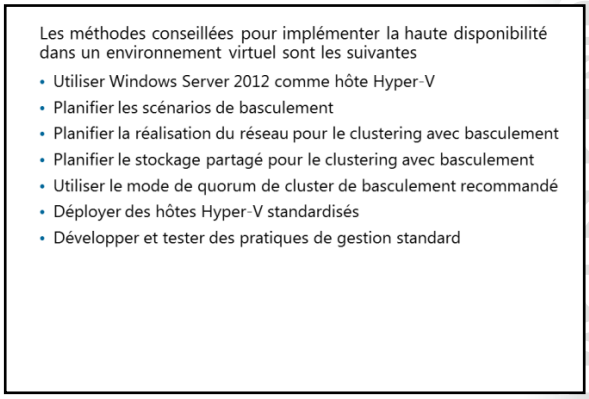


- Le clustering avec basculement prend désormais en charge jusqu'à 4 000 ordinateurs virtuels par cluster, et le composant logiciel enfichable amélioré Gestionnaire du cluster de basculement simplifie la gestion de plusieurs ordinateurs virtuels.
- Les administrateurs peuvent désormais exécuter des actions de sélection multiple afin de mettre en file d'attente les migrations dynamiques de plusieurs ordinateurs virtuels, plutôt que d'effectuer leur migration les unes après les autres comme cela était le cas dans les versions antérieures.
- Les administrateurs peuvent également configurer l'attribut prioritaire des ordinateurs virtuels pour contrôler l'ordre dans lequel démarrent les ordinateurs virtuels. La priorité permet également de s'assurer que les ordinateurs virtuels de priorité inférieure libèrent automatiquement des ressources pour les ordinateurs virtuels avec un niveau de priorité supérieur, si nécessaire.
- La fonctionnalité de volume partagé de cluster (CSV), qui simplifie la configuration et le fonctionnement des ordinateurs virtuels, peut contribuer à renforcer la sécurité et améliorer les performances. Désormais, elle prend en charge le stockage d'applications serveur basées sur des fichiers évolutifs, le renforcement de la sauvegarde et de la restauration ainsi que l'espace de noms de fichiers unique et cohérent. En outre, vous pouvez désormais protéger les volumes CSV à l'aide du chiffrement de lecteur Windows® BitLocker®, et en les configurant pour rendre le stockage visible seulement pour un sous-ensemble de nœuds.
- Surveillance de l'application de l'ordinateur virtuel. Vous pouvez désormais surveiller les services en cours d'exécution sur des ordinateurs virtuels en cluster. Dans les clusters exécutant Windows Server 2012, les administrateurs peuvent configurer la surveillance des services sur les ordinateurs virtuels en cluster qui exécutent également Windows Server 2012. Cette fonctionnalité étend la surveillance de haut niveau des ordinateurs virtuels qui est implémentée dans les clusters de basculement de Windows Server 2008 R2.
- Vous pouvez désormais enregistrer des ordinateurs virtuels sur des partages de fichiers SMB (Server Message Block) dans un cluster de serveur de fichiers. Il s'agit là d'une nouvelle méthode pour fournir des ordinateurs virtuels en haute disponibilité. Plutôt que de configurer un cluster entre les nœuds Hyper-V, vous pouvez désormais avoir des nœuds Hyper-V en dehors du cluster, mais avec des fichiers d'ordinateur virtuel sur un partage de fichiers à haut niveau de disponibilité. Pour que cela fonctionne, vous devez déployer un cluster de serveurs de fichiers en mode Serveurs de fichiers avec montée en puissance. Les serveurs de fichiers avec montée en puissance peuvent également utiliser les volumes partagés de cluster pour le stockage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Méthodes conseillées pour implémenter la haute disponibilité dans un environnement virtuel

Après avoir identifié les applications à déployer sur les clusters de basculement à haut niveau de disponibilité, l'étape suivante consiste à planifier et à déployer l'environnement de clustering avec basculement. Tenez compte des recommandations suivantes lors de l'implémentation du cluster de basculement :



- Utilisez Windows Server 2012 comme hôte Hyper-V. Windows Server 2012 offre des améliorations telles que Hyper-V Server 2012, les CSV améliorés, les migrations d'ordinateur virtuel et toute autre fonctionnalité qui améliore la flexibilité et la performance lors de l'implémentation du clustering avec basculement hôte.
- Planifiez les scénarios de basculement. Lorsque vous concevez la configuration matérielle requise pour les hôtes Hyper-V, vérifiez que vous incluez la capacité matérielle requise lorsque les hôtes échouent. Par exemple, si vous déployez un cluster de six nœuds, vous devez déterminer le nombre de défaillances d'hôtes que vous pouvez admettre. Si vous décidez que le cluster doit supporter la défaillance de deux nœuds, les quatre nœuds restants doivent alors avoir la capacité d'exécuter tous les ordinateurs virtuels du cluster.
- Planifiez la réalisation du réseau pour le clustering avec basculement. Pour optimiser les performances du cluster de basculement et le basculement, dédiez une connexion réseau rapide à la communication entre les nœuds. Comme avec les versions antérieures, ce réseau doit être logiquement et physiquement distinct des segments réseau utilisés par les clients pour communiquer avec le cluster. Vous pouvez également utiliser cette connexion réseau pour transférer la mémoire de l'ordinateur virtuel pendant une migration dynamique. Si vous utilisez iSCSI pour les ordinateurs virtuels, consacrez également une connexion réseau à la connexion réseau iSCSI.
- Planifiez le stockage partagé pour le clustering avec basculement. Lors de l'implémentation du clustering de basculement pour Hyper-V, le stockage partagé doit être à haut niveau de disponibilité. Toute défaillance du stockage partagé entraîne la défaillance de tous les ordinateurs virtuels, même si les nœuds physiques sont fonctionnels. Pour garantir la disponibilité de stockage, planifiez des connexions redondantes au stockage partagé ainsi qu'une redondance RAID sur le périphérique de stockage.
- Utilisez le mode de quorum de cluster de basculement recommandé. Si vous déployez un cluster avec un nombre de nœuds pair et si le stockage partagé est disponible pour le cluster, le Gestionnaire du cluster de basculement choisira automatiquement le mode de quorum de nœuds et disques majoritaire. Si vous déployez un cluster avec un nombre de nœuds impair, le Gestionnaire du cluster de basculement sélectionne automatiquement le mode de quorum de nœuds majoritaire. Ne modifiez la configuration par défaut que si vous en comprenez les conséquences.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Déployez des hôtes Hyper-V standardisés. Pour simplifier le déploiement et la gestion du cluster de basculement et des nœuds Hyper-V, développez un matériel serveur et une plateforme logicielle standard pour tous les nœuds.
- Développez des pratiques de gestion standard. Lorsque vous déployez plusieurs ordinateurs virtuels dans un cluster de basculement, vous augmentez le risque qu'une seule erreur arrête une grande partie du déploiement de serveur. Par exemple, si un administrateur configure le cluster de basculement de façon incorrecte et que le cluster échoue, tous les ordinateurs virtuels du cluster seront hors connexion. Pour éviter cela, développez des instructions standardisées pour toutes les tâches d'administration et testez-les rigoureusement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Implémentation des ordinateurs virtuels d'Hyper-V sur des clusters de basculement

L'implémentation d'ordinateurs virtuels à haut niveau de disponibilité est quelque peu différente de l'implémentation d'autres rôles dans un cluster de basculement. Le clustering avec basculement dans Windows Server 2012 fournit de nombreuses fonctionnalités pour le clustering Hyper-V, en plus des outils pour la gestion de la haute disponibilité des ordinateurs virtuels. Dans cette leçon, vous découvrirez la façon d'implémenter les ordinateurs virtuels à haut niveau de disponibilité.

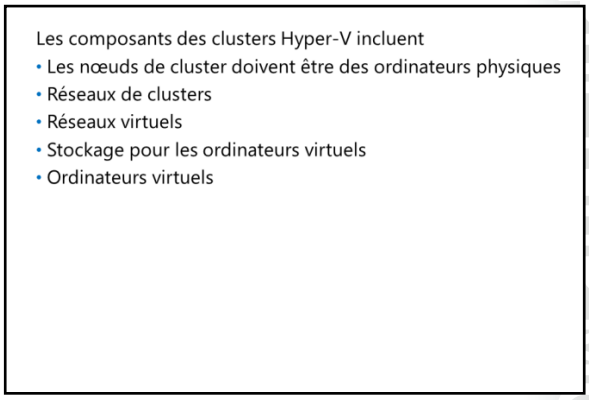
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les composants d'un cluster Hyper-V ;
- décrire les conditions préalables à l'implémentation des clusters Hyper-V ;
- implémenter le clustering avec basculement pour les ordinateurs virtuels Hyper-V ;
- configurer les services CSVs ;
- implémenter les ordinateurs virtuels à haut niveau de disponibilité sur partages de fichiers SMB 3.0 ;
- décrire les éléments à prendre en compte pour implémenter des clusters Hyper-V.

Composants des clusters Hyper-V

Hyper-V, en tant que rôle, a certaines exigences spécifiques pour les composants de cluster. Pour former un cluster Hyper-V, vous devez avoir au minimum deux nœuds physiques. Tandis que d'autres rôles en cluster (tels que le serveur DHCP (Dynamic Host Configuration Protocol) ou le serveur de fichiers) permettent aux nœuds d'être des ordinateurs virtuels, les nœuds Hyper-V doivent être composés d'hôtes physiques. Vous ne pouvez pas exécuter Hyper-V dans un ordinateur virtuel sur un hôte Hyper-V.



Vous devez disposer de nœuds, mais également de réseaux physiques et virtuels. Le clustering avec basculement nécessite un réseau pour la communication interne des clusters, ainsi qu'un réseau pour les clients. Vous pouvez également implémenter un réseau de stockage de manière distincte, selon le type de stockage utilisé. Encore une fois, en ce qui concerne le rôle Hyper-V, vous devez également tenir compte des réseaux virtuels pour les ordinateurs virtuels en cluster. Il est important de créer les mêmes réseaux virtuels sur tous les hôtes physiques qui appartiennent à un même cluster. Si tel n'était pas le cas, l'ordinateur virtuel perdrait la connectivité réseau en cas de déplacement d'un hôte vers un autre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le stockage est un composant important du clustering d'ordinateurs virtuels. Vous pouvez utiliser n'importe quel type de stockage pris en charge par le clustering avec basculement de Windows Server 2012. Il est également recommandé de configurer le stockage comme CSV. Ce sujet est présenté plus loin dans une rubrique de ce module.

Les ordinateurs virtuels sont des composants d'un cluster Hyper-V. Dans le Gestionnaire du cluster de basculement, vous pouvez créer de nouveaux ordinateurs virtuels à haut niveau de disponibilité, ou vous pouvez rendre les ordinateurs virtuels existants à haut niveau de disponibilité. Dans les deux cas, l'emplacement de stockage de l'ordinateur virtuel doit être un stockage partagé qui peut être accessible à tous les nœuds. Cependant, vous ne souhaiterez probablement pas rendre tous les ordinateurs virtuels à haut niveau de disponibilité. Dans le Gestionnaire du cluster de basculement, vous pouvez sélectionner les ordinateurs virtuels qui doivent faire partie de la configuration d'un cluster.

Conditions préalables à l'implémentation des clusters Hyper-V

Pour déployer Hyper-V sur un cluster de basculement, vous devez vérifier que vous répondez aux critères de configuration matérielle, logicielle, de compte et d'infrastructure réseau détaillés dans les sections suivantes.

Configuration matérielle requise pour les nœuds de cluster et le stockage	• Matériel du serveur • Cartes réseau • Adaptateurs de stockage • Stockage
Configuration logicielle requise pour les nœuds de cluster	• version x64 de Windows Server 2012, Enterprise Edition ou Datacenter Edition • Mises à jour logicielles et services packs identiques • Installation complète ou installation minimale
Configuration requise pour l'infrastructure réseau	• Paramètres réseau et adresses IP • DNS • Rôle de domaine • Compte d'administration du cluster

Configuration matérielle requise pour le clustering avec basculement à l'aide d'Hyper-V

Vous aurez besoin du matériel suivant pour un cluster de basculement de deux nœuds :

- Matériel du serveur. Hyper-V requiert un processeur x64, la virtualisation d'assistance matérielle et la prévention de l'exécution des données (DEP) appliquée par le biais du matériel. À titre de recommandation, les serveurs doivent avoir du matériel similaire. Si vous utilisez Windows Server 2008, les versions des processeurs sur les serveurs doivent être identiques. Si vous utilisez Windows Server 2008 R2 ou Windows Server 2012, les processeurs doivent utiliser la même architecture.



Remarque : Microsoft n'assure le support technique d'une solution de cluster de basculement que si la mention « Certifié pour Windows Server » est apposée sur tous les éléments matériels. En outre, la configuration complète (serveurs, réseau et système de stockage) doit passer avec succès tous les tests de l'Assistant Validation de cette configuration, qui est intégré au composant logiciel enfichable Gestion du cluster de basculement.

- Cartes réseau. À l'instar des autres fonctionnalités de la solution de cluster de basculement, le matériel réseau doit porter le logo « Certifié pour Windows Server ». Pour fournir la redondance réseau, vous pouvez connecter les nœuds de cluster à plusieurs réseaux distincts, ou connecter les nœuds à un réseau utilisant des cartes réseau associées, des commutateurs redondants, des routeurs redondants ou tout matériel similaire pour supprimer les points de défaillance unique. Il est également recommandé de configurer plusieurs cartes réseau sur l'ordinateur hôte que vous définirez en tant que nœud de cluster. Vous devez connecter une carte réseau au réseau privé utilisé par les communications entre les hôtes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Adaptateurs de stockage. Si vous utilisez SAS (Serial Attached SCSI) ou Fibre Channel sur tous les serveurs en cluster, les contrôleurs de périphérique de stockage de masse doivent être identiques et utiliser la même version du microprogramme. Si vous utilisez iSCSI, chaque serveur en cluster doit être équipé d'une ou plusieurs cartes réseau dédiées au stockage en cluster. Les cartes réseau qui vous permettent de vous connecter à la cible de stockage iSCSI doivent être identiques, et vous devez utiliser une carte Ethernet de 1 Gigabit ou une carte réseau plus rapide.
- Stockage. Vous devez utiliser le stockage partagé qui est compatible avec Windows Server 2012. Si vous déployez un cluster de basculement qui utilise un disque témoin, le stockage doit contenir au moins deux volumes distincts (ou numéros d'unité logique). Un volume fonctionne comme un disque témoin et les volumes supplémentaires contiennent les fichiers d'ordinateur virtuel partagés entre les nœuds de cluster. Les considérations et les recommandations de stockage comprennent les éléments suivants :
    - Utilisez des disques de base, pas des disques dynamiques. Formatez les disques avec le système de fichiers NTFS.
    - Utilisez l'enregistrement de démarrage principal (MBR) ou la table de partition GUID (GPT).
    - Si vous utilisez un réseau de stockage (SAN), le pilote miniport utilisé par le stockage doit fonctionner avec le pilote de stockage Storport.
    - Utilisez un logiciel MPIO (Multipath I/O) : Si votre réseau de stockage utilise une conception de réseau à haut niveau de disponibilité avec des composants redondants, vous pouvez déployer des clusters de basculement avec plusieurs adaptateurs de bus hôte en utilisant le logiciel Multipath I/O (MPIO). Cela permet de bénéficier du niveau de redondance et de disponibilité le plus élevé. Pour Windows Server 2008 R2 et Windows Server 2012, votre solution multivoie doit être basée sur Multipath I/O (MPIO).

Configuration logicielle requise pour l'utilisation de Hyper-V et du clustering avec basculement

Voici la configuration logicielle requise pour l'utilisation d'Hyper-V et du clustering avec basculement :

- Tous les serveurs dans un cluster de basculement doivent exécuter la version x64 des systèmes d'exploitation Windows Server 2012 Standard ou Windows Server 2012 Enterprise ou Datacenter. Les nœuds figurant dans un cluster de basculement unique ne peuvent pas exécuter des versions différentes.
- Tous les serveurs doivent posséder les mêmes mises à jour logicielles et Service Packs.
- Tous les serveurs doivent être installés dans le cadre d'une installation minimale ou complète.

Configuration requise pour l'infrastructure réseau

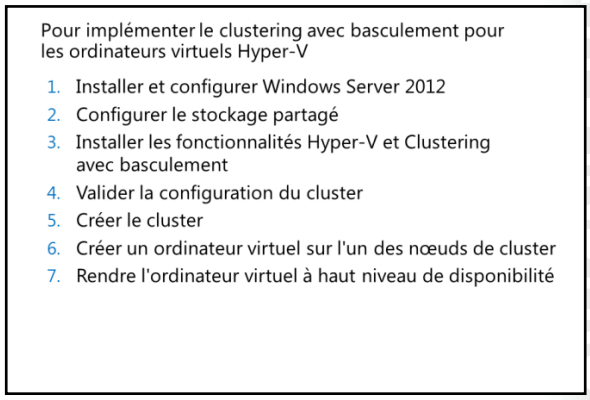
L'infrastructure réseau et les autorisations de domaine suivants sont requis pour un cluster de basculement :

- Paramètres réseau et adresses IP. Utilisez des paramètres de communication identiques sur toutes les cartes réseau, y compris les paramètres de vitesse, de mode duplex, de contrôle de flux et de type de média. Vérifiez que l'ensemble du matériel réseau prend en charge les mêmes paramètres.
- Si vous utilisez des réseaux privés qui ne sont pas acheminés vers l'ensemble de votre infrastructure réseau pour la communication entre les nœuds de cluster, vérifiez que chacun de ces réseaux privés utilise un sous-réseau unique.

- DNS. les serveurs du cluster doivent utiliser DNS (Domain Name System) pour la résolution de noms. Utilisez le protocole de mise à jour dynamique DNS.
- Rôle de domaine. Tous les serveurs du cluster doivent appartenir au même domaine Active Directory® Domain Services (AD DS) . Il est conseillé d'affecter à tous les serveurs en cluster le même rôle de domaine, serveur membre ou contrôleur de domaine. Le rôle recommandé est serveur membre. Évitez d'installer des nœuds de cluster sur des contrôleurs de domaine, parce qu'AD DS possède son propre système à haut niveau de disponibilité.
- Compte d'administration du cluster. Lorsque vous créez un cluster ou que vous y ajoutez des serveurs, vous devez être connecté au domaine à l'aide d'un compte d'administrateur sur tous les serveurs du cluster. En outre, si le compte n'est pas un compte Administrateurs du domaine, le compte doit avoir l'autorisation de **création d'objets ordinateur** dans le domaine.

Implémentation du clustering avec basculement pour les ordinateurs virtuels Hyper-V

Pour implémenter le clustering de basculement pour les ordinateurs virtuels Hyper-V, vous devez effectuer les étapes de haut niveau suivantes :



1. Installer et configurer les versions nécessaires de Windows Server 2012. À la fin de l'installation, configurez les paramètres réseau, associez les ordinateurs à un domaine Active Directory et configurez la connexion au stockage partagé.
2. Configurer le stockage partagé. Vous devez utiliser le Gestionnaire de disque pour créer des partitions sur le stockage partagé.
3. Installer les fonctionnalités Hyper-V et de clustering avec basculement sur les serveurs hôtes. Vous pouvez utiliser le Gestionnaire de serveurs dans MMC (Microsoft Management Console) ou Windows PowerShell® pour cela.
4. Valider la configuration du cluster. L'Assistant Valider ce cluster vérifie tous les composants requis pour la création d'un cluster et émet des avertissements ou signale des erreurs si certains des composants ne répondent pas aux critères. Avant de poursuivre, résolvez les problèmes identifiés par l'Assistant Valider ce cluster.
5. Créer le cluster. Une fois que les composants sont validés par l'Assistant Valider ce cluster, vous pouvez créer un cluster. Lorsque vous configurez le cluster, affectez un nom de cluster et une adresse IP. Un compte d'ordinateur pour le nom du cluster est créé dans le domaine Active Directory et l'adresse IP est enregistrée dans le système DNS.

Remarque : Vous ne pouvez activer le stockage partagé en cluster pour le cluster qu'une fois le cluster configuré. Si vous souhaitez utiliser des volumes partagés de cluster (CSV), vous devez configurer les CSV avant de passer à l'étape suivante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

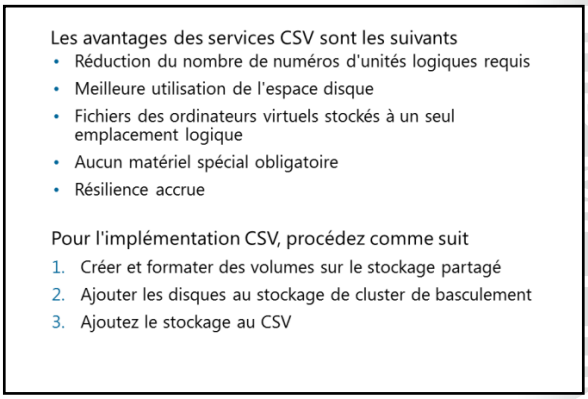
6. Créer un ordinateur virtuel sur l'un des nœuds de cluster. Lorsque vous créez l'ordinateur virtuel, vérifiez que tous les fichiers qui lui sont associés, notamment les fichiers de configuration du disque dur virtuel et de l'ordinateur virtuel, sont stockés sur le stockage partagé. Vous pouvez créer et gérer des ordinateurs virtuels dans le Gestionnaire Hyper-V ou le Gestionnaire du cluster de basculement. Lorsque vous créez un ordinateur virtuel à l'aide du Gestionnaire du cluster de basculement, cet ordinateur virtuel est automatiquement rendu à haut niveau de disponibilité.
7. Rendre l'ordinateur virtuel à haut niveau de disponibilité. Pour rendre l'ordinateur virtuel à haut niveau de disponibilité, dans le Gestionnaire du cluster de basculement, sélectionnez l'option permettant de rendre un nouveau service ou une nouvelle application à haut niveau de disponibilité. Le Gestionnaire du cluster de basculement affiche ensuite une liste de services et d'applications qui peuvent être rendues à haut niveau de disponibilité. Lorsque vous sélectionnez l'option permettant de rendre les ordinateurs virtuels à haut niveau de disponibilité, vous pouvez sélectionner l'ordinateur virtuel que vous avez créé sur le stockage partagé.

Remarque : Lorsque vous choisissez de rendre un ordinateur virtuel à haut niveau de disponibilité, une liste affiche tous les ordinateurs virtuels hébergés sur tous les nœuds du cluster, notamment les ordinateurs virtuels qui ne sont pas stockés sur le stockage partagé. Si vous rendez à haut niveau de disponibilité un ordinateur virtuel qui ne se trouve pas sur le stockage partagé, un avertissement s'affiche, mais Hyper-V ajoute l'ordinateur virtuel à la liste des services et applications. Toutefois, lorsque vous essayez d'effectuer la migration de l'ordinateur virtuel sur un hôte différent, la migration échoue.

8. Tester le basculement d'ordinateurs virtuels. Après avoir rendu l'ordinateur virtuel à haut niveau de disponibilité, vous pouvez effectuer la migration de l'ordinateur vers un autre nœud du cluster. Si vous exécutez Windows Server 2008 R2 ou Windows Server 2012, vous pouvez choisir d'effectuer une migration rapide ou une migration dynamique.

Configuration de CSVs

Vous ne devez pas configurer, ni utiliser CSV quand vous implémentez la haute disponibilité pour des ordinateurs virtuels dans Hyper-V. En fait, vous pouvez configurer un cluster Hyper-V sans utiliser CSV. Il est toutefois conseillé d'utiliser CSV pour profiter des avantages suivants :



- Numéros d'unité logique réduits pour les disques. Vous pouvez utiliser CSV pour réduire le nombre de numéros d'unité logique (LUN) requis par vos ordinateurs virtuels. Lorsque vous configurez un volume partagé de cluster, vous pouvez stocker plusieurs ordinateurs virtuels sur un numéro d'unité logique unique, et plusieurs ordinateurs hôtes peuvent accéder simultanément au même numéro d'unité logique.
- Meilleure utilisation de l'espace disque. Au lieu de placer chaque fichier .vhdx (virtual hard disk) sur un disque séparé avec de l'espace vide pour que le fichier .vhdx puisse augmenter, vous pouvez surutiliser l'espace disque en stockant plusieurs fichiers .vhdx sur le même numéro d'unité logique.

- Stockage des fichiers des ordinateurs virtuels dans un seul emplacement logique. Vous pouvez suivre les chemins d'accès des fichiers .vhdx et d'autres fichiers utilisés par les ordinateurs virtuels. Au lieu d'utiliser des lettres de lecteur ou des identificateurs GUID pour identifier des disques, vous pouvez spécifier les noms de chemin d'accès. Lorsque vous implémentez CSV, la totalité du stockage ajouté apparaît dans le dossier \ClusterStorage. Le dossier \ClusterStorage est créé dans le dossier système du nœud de cluster, et vous ne pouvez pas le déplacer. Cela signifie que tous les hôtes Hyper-V qui sont membres du cluster doivent utiliser la même lettre de lecteur que leur lecteur système ; à défaut, les basculements d'ordinateurs virtuels seront un échec.
- Aucune configuration matérielle requise spécifique. L'implémentation de CSV ne présente pas de configurations matérielles requises spécifiques. Vous pouvez implémenter CSV sur n'importe quelle configuration de disque prise en charge et sur des réseaux de stockage Fibre Channel ou iSCSI.
- Résilience accrue. CSV augmente la résilience parce que le cluster peut répondre correctement même si la connectivité entre un nœud et le réseau SAN est interrompue, ou si une partie d'un réseau est en panne. Le cluster réachemine le trafic sur le CSV via une partie intacte du SAN ou du réseau.

Implémentation de la réplication CSV

Une fois que vous avez créé le cluster de basculement, vous pouvez activer le CSV pour le cluster, puis ajouter le stockage au CSV.

Avant de pouvoir ajouter le stockage au CSV, le numéro d'unité logique doit être disponible comme stockage partagé pour le cluster. Lorsque vous créez un cluster de basculement, tous les disques partagés configurés dans le Gestionnaire de serveur sont ajoutés au cluster et vous pouvez ensuite les ajouter à un CSV. Si vous ajoutez davantage de numéros d'unité logique au stockage partagé, vous devez d'abord créer des volumes sur le numéro d'unité logique, puis ajouter le stockage au cluster, et enfin ajouter le stockage au CSV.

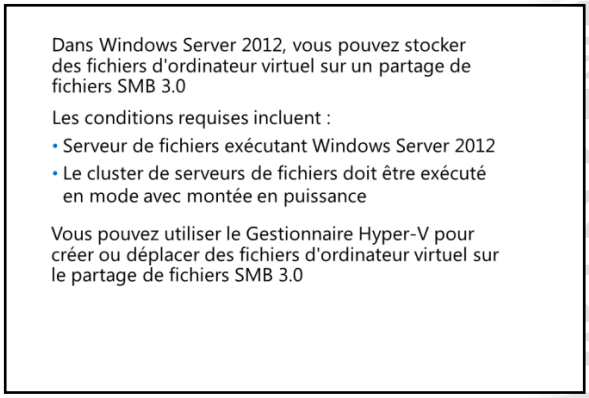
Il est conseillé de configurer le CSV avant de rendre tous les ordinateurs virtuels à haut niveau de disponibilité. Toutefois, vous pouvez convertir un accès disque standard en CSV après déploiement. Lors de l'implémentation de CSV, tenez compte des éléments suivants :

- La conversion d'un accès disque standard en LUN supprime la lettre de lecteur ou le point de montage du CSV. Cela signifie que vous devez recréer tous les ordinateurs virtuels qui sont stockés sur le stockage partagé. Si vous devez conserver les mêmes paramètres d'ordinateur virtuel, envisagez d'exporter les ordinateurs virtuels, de basculer vers CSV, puis d'importer les ordinateurs virtuels dans Hyper-V. En outre, envisagez d'utiliser l'option de migration de stockage disponible dans le rôle Hyper-V dans Windows Server 2012.
- Vous ne pouvez pas convertir le stockage partagé en CSV. Si vous disposez d'un ordinateur virtuel en cours d'exécution qui utilise un disque de cluster, vous devez arrêter l'ordinateur virtuel, puis ajouter le disque aux volumes partagés de cluster (CSV).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémenter les ordinateurs virtuels à haut niveau de disponibilité sur partage de fichiers SMB 3.0



Dans Windows Server 2012, vous pouvez utiliser une nouvelle technique pour rendre les ordinateurs virtuels à haut niveau de disponibilité. Au lieu d'utiliser le clustering d'hôte ou d'invité, vous pouvez désormais enregistrer les fichiers des ordinateurs virtuels sur un partage de fichier SMB 3.0 à haut niveau de disponibilité. À l'aide de cette approche, la haute disponibilité est obtenue non pas via le clustering de nœuds Hyper-V, mais via les serveurs de fichiers qui hébergent les fichiers de l'ordinateur virtuel sur leurs partages de fichiers. Avec cette nouvelle fonction, Hyper-V peut enregistrer tous les fichiers de l'ordinateur virtuel, y compris la configuration, les fichiers .vhdx et les captures instantanées, sur les partages de fichiers SMB 3.0 à haut niveau de disponibilité.

La haute disponibilité requiert l'infrastructure suivante :

- Un ou plusieurs ordinateurs exécutant Windows Server 2012 dotés du rôle Hyper-V.
- Un ou plusieurs ordinateurs exécutant Windows Server 2012 dotés du rôle Services de fichiers et de stockage.
- Membres du domaine dans l'infrastructure Active Directory. Les serveurs qui exécutent AD DS n'ont pas besoin d'exécuter Windows Server 2012.

Avant d'implémenter des ordinateurs virtuels sur un partage de fichiers SMB 3.0, configurez un cluster de serveurs de fichiers. Pour ce faire, vous devez avoir au minimum deux nœuds de cluster équipés de services de fichiers et du clustering avec basculement. Dans la console de clustering avec basculement, créez un cluster de serveurs de fichiers avec montée en puissance. Après la configuration du cluster, déployez le nouveau partage de fichiers SMB pour les applications. Ce partage stocke les fichiers des ordinateurs virtuels. Lorsque le partage est créé, vous pouvez utiliser la console du Gestionnaire Hyper-V pour déployer les nouveaux ordinateurs virtuels sur le partage de fichiers SMB 3.0 ou vous pouvez réaliser la migration des ordinateurs virtuels existants vers le partage de fichiers SMB à l'aide de la méthode de migration de stockage.

Démonstration : Implémentation des ordinateurs virtuels sur des groupes (facultatif)

Au cours de cette démonstration, vous allez apprendre à implémenter les ordinateurs virtuels sur un cluster de basculement.

Procédure de démonstration

Déplacer le stockage de l'ordinateur virtuel vers la cible iSCSI

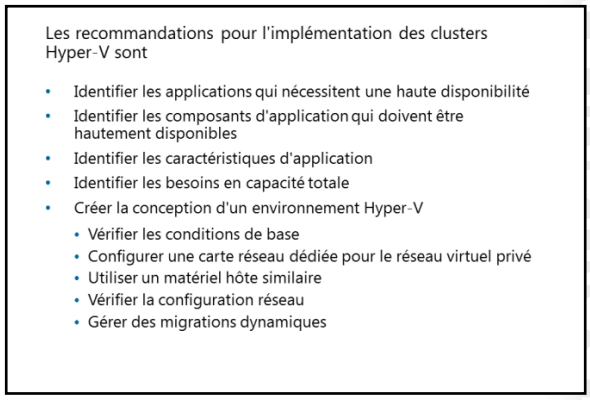
- Sur LON-HOST1, ouvrez Windows Explorer, accédez à **E:\Programmes\Microsoft Learning\22412\22412B-LON-CORE\Virtual Hard Disks**, et déplacez **22412B-LON-CORE.vhd** à l'emplacement **C:\ClusterStorage\Volume1**.

Configurer l'ordinateur en tant qu'ordinateur à haut niveau de disponibilité

1. Dans le Gestionnaire du cluster de basculement, cliquez sur **Rôles**, puis démarrez l'**Assistant Nouvel ordinateur virtuel**.
2. Dans l'Assistant Nouvel ordinateur virtuel, utilisez les paramètres suivants :
   - Nœuds du cluster : **LON-HOST2**
   - Nom de l'ordinateur : **TestClusterVM**
   - Enregistrez le fichier dans **C:\ClusterStorage\Volume1**.
   - RAM pour TestClusterVM : **1536** Mo
   - Connectez l'ordinateur au lecteur de disque dur virtuel 22412B-LON-CORE.vhd existant à l'emplacement **C:\ClusterStorage\Volume1**.
3. À partir du nœud **Rôles**, démarrez l'ordinateur virtuel.

Éléments à prendre en compte pour l'implémentation des clusters Hyper-V

Lors de l'implémentation du clustering avec basculement hôte, vous pouvez rendre les ordinateurs virtuels à haut niveau de disponibilité. Toutefois, l'implémentation du clustering avec basculement de l'hôte augmente également considérablement le coût et la complexité d'un déploiement Hyper-V. Vous devez investir dans du matériel serveur supplémentaire pour fournir la redondance, et vous devez implémenter une infrastructure de stockage partagé ou avoir accès à ce type d'infrastructure.



Tenez compte des recommandations suivantes pour vérifier que votre stratégie de clustering avec basculement répond aux besoins de votre organisation :

- Identifier les applications ou les services qui nécessitent une haute disponibilité. Sauf si vous avez la possibilité de rendre tous les ordinateurs virtuels à haut niveau de disponibilité, vous devez développer des priorités pour lesquelles les applications seront rendues à haut niveau de disponibilité.
- Identifiez les composants qui doivent être hautement disponibles pour rendre les applications hautement disponibles. Dans certains cas, l'application pourrait fonctionner sur un seul serveur, et vous devez juste rendre ce serveur à haut niveau de disponibilité. D'autres applications peuvent requérir que plusieurs serveurs, et d'autres composants (tels que le stockage ou le réseau), soient à haut niveau de disponibilité. En outre, assurez-vous que les contrôleurs de domaine sont à haut niveau de disponibilité, et que vous disposez au moins d'un contrôleur de domaine sur une infrastructure matérielle ou de virtualisation distincte.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Identifier les caractéristiques d'application. Vous devez comprendre plusieurs aspects à propos de l'application.
    - Le serveur qui exécute l'application virtualise-t-il une option ? Certaines applications ne sont pas prises en charge ou ne sont pas recommandées pour un environnement virtuel.
    - Quelles sont les options disponibles pour rendre l'application à haut niveau de disponibilité ? Vous pouvez rendre certaines applications à haut niveau de disponibilité via des options autres que le clustering hôte. Si d'autres options sont disponibles, évaluez les avantages et les inconvénients de chaque option.
    - Quels sont les exigences en matière de performances pour chaque application ? Collectez les informations de performances sur les serveurs sur lesquels les applications sont en cours d'exécution. Cela permet de mieux connaître les configurations matérielles requises dans le cadre de la virtualisation du serveur.
    - Quelle est la capacité requise pour rendre les ordinateurs virtuels Hyper-V à haut niveau de disponibilité ? Une fois que vous avez identifié toutes les applications qui doivent être à haut niveau de disponibilité en utilisant le clustering hôte, vous pouvez commencer à concevoir le déploiement Hyper-V proprement dit. En identifiant les exigences en matière de performances, et les exigences de réseau et du stockage, pour les applications, vous pouvez définir le matériel dont vous avez besoin pour implémenter toutes les applications dans un environnement à haut niveau de disponibilité.

La migration dynamique est l'un des aspects les plus importants du clustering Hyper-V. Utilisez la fonctionnalité de migration dynamique dans Windows Server 2012 pour exécuter des migrations dynamiques des ordinateurs virtuels. Lors de l'implémentation de la migration dynamique, tenez compte des éléments suivants :

- Vérifiez les conditions de base. Avec la migration dynamique, tous les hôtes doivent faire partie d'un cluster de basculement Windows Server 2012 et les processeurs hôtes doivent présenter la même architecture. Tous les hôtes du cluster doivent avoir accès au stockage partagé, ce qui répond aux exigences de CSV.
- Configurez une carte réseau dédiée pour le réseau virtuel privé. Lorsque vous implémentez le clustering avec basculement, vous devez configurer un réseau privé pour le trafic de pulsation du cluster. Vous utilisez ce réseau pour transférer la mémoire de l'ordinateur virtuel lors du basculement. Pour optimiser cette configuration, configurez pour ce réseau une carte réseau ayant une capacité de 1 gigabit par seconde (Gbps) ou supérieure.

 **Remarque :** Vous devez activer le composant Client pour les réseaux Microsoft et Partage de fichiers et d'imprimantes pour les réseaux Microsoft pour la carte réseau que vous souhaitez utiliser pour le réseau privé.

- Utilisez un matériel hôte similaire. À titre de recommandation, tous les nœuds de cluster de basculement doivent utiliser le même matériel pour se connecter au stockage partagé, et tous les nœuds de cluster doivent posséder des processeurs présentant la même architecture. Bien que vous puissiez activer le basculement pour les ordinateurs virtuels sur un hôte disposant de versions de processeur différentes en configurant les paramètres de compatibilité du processeur, l'expérience et les performances de basculement sont plus cohérentes si tous les serveurs sont équipés d'un matériel similaire.

- Vérifiez la configuration réseau. Tous les nœuds du cluster de basculement doivent se connecter via le même sous-réseau IP afin que l'ordinateur virtuel puisse continuer de communiquer via la même adresse IP après la migration dynamique. En outre, les adresses IP attribuées au réseau privé sur tous les nœuds doivent être sur le même sous-réseau logique. Autrement dit, les clusters multisites doivent utiliser un réseau local virtuel VLAN étiré, qui est un sous-réseau qui couvre une connexion de réseau étendu (WAN).
- Gérer les migrations dynamiques. Dans Windows Server 2008 R2, chaque nœud du cluster de basculement ne peut exécuter qu'une migration dynamique à la fois. Si, dans Windows Server 2008 R2, vous essayez de démarrer une deuxième migration dynamique avant que la première migration finisse, la migration échoue. Dans Windows Server 2012, vous pouvez maintenant exécuter plusieurs migrations dynamiques simultanément.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Implémentation des déplacements d'ordinateurs virtuels Hyper-V

Le déplacement des ordinateurs virtuels d'un emplacement à un autre est une procédure commune dans les environnements Hyper-V. Alors que le déplacement des ordinateurs virtuels dans les versions antérieures de Windows Server impliquaient un temps d'arrêt, Windows Server 2012 présente de nouvelles technologies pour activer un déplacement transparent des ordinateurs virtuels. Dans cette leçon, vous allez découvrir les options de migration et de déplacement des ordinateurs virtuels.

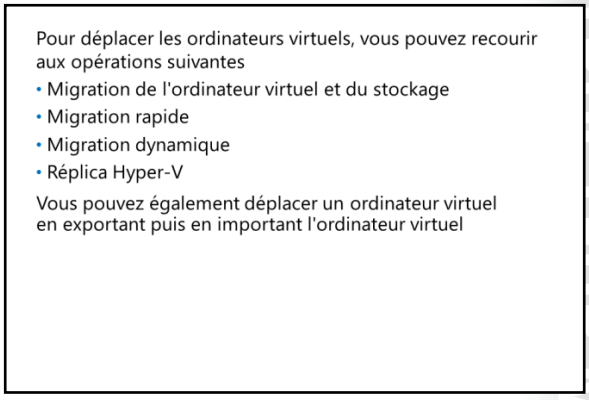
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options de migration pour les ordinateurs virtuels ;
- décrire la migration de stockage ;
- décrire la migration dynamique ;
- expliquer le mode de fonctionnement des réplications Hyper-V ;
- configurer un réplica Hyper-V.

Options de migration des ordinateurs virtuels

Il y a plusieurs scénarios dans lesquels vous souhaiterez peut être effectuer la migration d'ordinateurs virtuels d'un emplacement à un autre. Par exemple, il est probable que vous souhaitiez déplacer le disque dur virtuel (VHD) d'un ordinateur virtuel d'un lecteur physique à un autre sur le même hôte. Vous pouvez aussi déplacer un ordinateur virtuel d'un nœud d'un cluster vers un autre, ou simplement déplacer un ordinateur d'un serveur hôte vers un autre serveur hôte sans que les hôtes n'appartiennent à un cluster sont deux autres exemples possibles. Par rapport à Windows Server 2008 R2, Windows Server 2012 offre des améliorations significatives pour ce processus.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

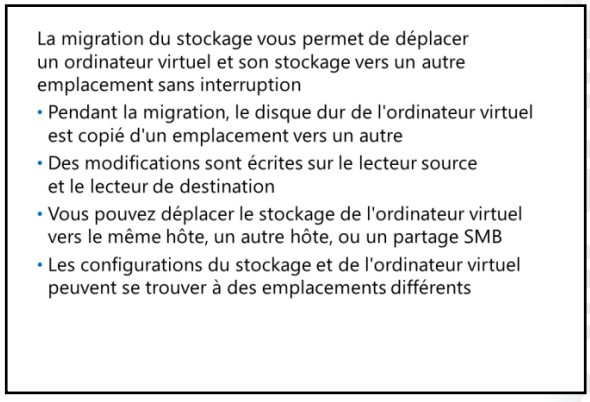
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Windows Server 2012, vous pouvez exécuter la migration des ordinateurs virtuels à l'aide des méthodes suivantes :

- Migration de l'ordinateur virtuel et du stockage. Avec cette méthode, vous déplacez un ordinateur virtuel sous tension d'un emplacement à un autre (ou d'un hôte à l'autre) à l'aide de l'Assistant Gestionnaire Hyper-V. Le fonctionnement de la migration du stockage et de l'ordinateur virtuel n'implique pas le clustering avec basculement ou toute autre technologie à haut niveau de disponibilité. En outre, vous n'avez pas besoin de stockage partagé lorsque vous déplacez juste l'ordinateur virtuel.
- Migration rapide. Cette méthode est également disponible dans Windows Server 2008. Elle requiert l'installation et la configuration du clustering avec basculement. Le processus de migration rapide enregistre l'état de l'ordinateur virtuel avant le basculement, puis redémarre l'ordinateur virtuel après le basculement s'achève.
- Migration dynamique. Cette fonction est une amélioration par rapport à la migration rapide et est également disponible dans Windows Server 2008 R2. Elle vous permet d'effectuer la migration d'un ordinateur virtuel d'un hôte à un autre sans subir un temps d'arrêt. À la différence du processus de migration rapide, la migration dynamique ne sauvegarde pas l'état de l'ordinateur virtuel. Elle synchronise en fait l'état pendant le basculement.
- Réplica Hyper-V. Cette nouvelle fonctionnalité dans Windows Server 2012 permet de répliquer, plutôt que de déplacer, un ordinateur virtuel vers un autre hôte, et de synchroniser toutes les modifications apportées à l'ordinateur virtuel à partir de l'hôte principal vers l'hôte qui contient le réplica.
- Exportation et importation d'un ordinateur virtuel. Il s'agit là d'une méthode établie de déplacement des ordinateurs virtuels sans utiliser de cluster. Vous exportez un ordinateur virtuel sur un hôte, puis déplacez physiquement les fichiers exportés vers un autre hôte en effectuant une opération d'importation. Il arrive souvent que cette opération longue nécessite l'arrêt des ordinateurs virtuels pendant l'exportation et l'importation. Dans Windows Server 2012, cette méthode de migration a été améliorée. Vous pouvez importer un ordinateur virtuel vers un hôte Hyper-V sans l'exporter avant importation. Le rôle Hyper-V dans Windows Server 2012 est désormais apte à configurer tous les paramètres nécessaires au cours de l'opération d'importation.

Comment fonctionne la migration du stockage et de l'ordinateur virtuel ?

Les administrateurs peuvent avoir plusieurs raisons pour déplacer les fichiers d'ordinateur virtuel vers un autre emplacement. Par exemple, si le disque sur lequel réside le disque dur de l'ordinateur virtuel vient à manquer d'espace, vous devez déplacer l'ordinateur virtuel vers un autre pilote ou volume. Le déplacement des ordinateurs virtuels sur d'autres hôtes est une procédure commune.



Dans Windows Server 2008 et Windows Server 2008 R2, le déplacement d'un ordinateur virtuel a entraîné un temps d'arrêt, car l'ordinateur virtuel devait être désactivé. Si vous avez déplacé un ordinateur virtuel entre deux hôtes, vous avez dû également effectuer les opérations d'exportation et d'importation pour cet ordinateur virtuel spécifique. Les opérations d'exportation peuvent être longues, selon la taille des disques durs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Windows Server 2012, la migration du stockage et de l'ordinateur virtuel permet de déplacer un ordinateur virtuel et son espace de stockage vers un autre emplacement sur le même hôte ou sur un autre ordinateur hôte sans avoir à éteindre l'ordinateur virtuel.

La migration du stockage et de l'ordinateur virtuel fonctionne comme suit :

1. Pour copier un disque dur virtuel, commencez la migration de stockage dynamique à l'aide de la console Hyper-V. Éventuellement, vous pouvez utiliser les applets de commande Windows PowerShell.
2. Le processus de migration crée un disque dur virtuel à l'emplacement de destination et démarre le processus de copie.
3. Au cours du processus de copie, l'ordinateur virtuel est totalement fonctionnel. Cependant, toutes les modifications qui se produisent au cours du processus de copie sont écrites à la fois dans l'emplacement source et l'emplacement de destination. Les opérations de lecture sont effectuées uniquement à partir de l'emplacement source.
4. Dès que le processus de copie de disque est terminé, Hyper-V bascule sur les ordinateurs virtuels pour s'exécuter sur le disque dur virtuel de destination. En outre, si vous déplacez l'ordinateur virtuel vers un autre hôte, la configuration de l'ordinateur est copiée, et l'ordinateur virtuel est associé à un autre hôte. Si une défaillance se produit du côté de la destination, il est toujours possible d'effectuer une restauration sur le répertoire source.
5. Après que l'ordinateur virtuel termine la migration, le processus supprime les disques durs virtuels source.

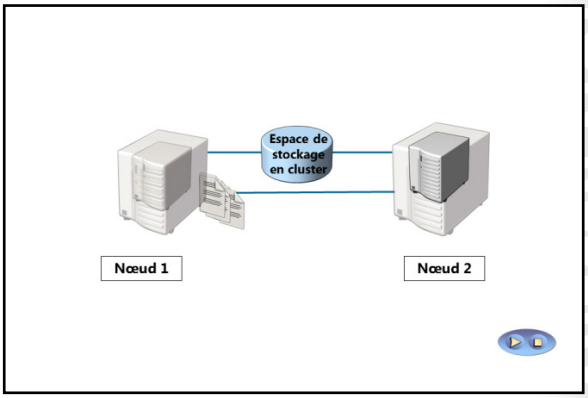
Le temps nécessaire pour déplacer un ordinateur virtuel dépend des emplacements source et de destination, de la vitesse des disques durs, du stockage ou du réseau et de la taille des disques durs virtuels. Le processus de déplacement est plus rapide si les emplacements source et de destination sont sur le stockage et que le stockage prend en charge les fichiers .odx. Au lieu d'utiliser les opérations de lecture/écriture avec mise en tampon, le fichier .odx démarre l'opération de copie avec une commande de lecture de déchargement et récupère un jeton représentant les données du périphérique de stockage. Il utilise ensuite une commande d'écriture de déchargement avec le jeton pour demander le transfert des données du disque de source vers le disque de destination.

Quand vous déplacez les disques durs virtuels d'un ordinateur virtuel vers un autre emplacement, l'assistant de déplacement des ordinateurs virtuels offre les trois options suivantes :

- **Déplacer toutes les données de l'ordinateur virtuel vers un emplacement unique**. Spécifie un emplacement cible unique, tel que le fichier de disque, la configuration, la capture instantanée et la pagination intelligente.
- **Déplacer toutes les données de l'ordinateur virtuel vers un emplacement différent**. Spécifie des emplacements individuels pour chacun des éléments de l'ordinateur virtuel.
- **Déplacer uniquement le disque dur virtuel de l'ordinateur virtuel**. Déplace uniquement le fichier de disque dur virtuel.

Comment fonctionne la migration dynamique ?

Grâce à la fonctionnalité de migration dynamique, vous pouvez déplacer des ordinateurs virtuels d'un nœud du cluster de basculement vers un autre nœud situé dans le même cluster. Avec la migration dynamique, les utilisateurs connectés à l'ordinateur virtuel ne doivent pratiquement subir aucune défaillance du serveur.



Remarque : Même si vous pouvez également effectuer une migration dynamique d'ordinateurs virtuels à l'aide de la méthode de migration de l'ordinateur virtuel et du stockage décrite dans la rubrique précédente, vous devez savoir que la migration dynamique est basée sur le clustering avec basculement. À la différence du scénario de migration du stockage, la migration dynamique est possible uniquement si les ordinateurs virtuels sont à haut niveau de disponibilité.

Vous pouvez lancer une migration dynamique en suivant l'une des méthodes suivantes :

- La console Gestionnaire du cluster de basculement.
- La console Administrateur Virtual Machine Manager, si vous utilisation VMM pour gérer vos hôtes physiques.
- Un script WMI (Windows Management Instrumentation) ou Windows PowerShell.

Remarque : La migration dynamique vous permet de réduire considérablement la panne perçue d'un ordinateur virtuel lors d'un basculement planifié. Lors d'un basculement planifié, vous démarrez manuellement le basculement. La migration dynamique ne s'applique pas lors d'un basculement non planifié, par exemple lorsque le nœud hébergeant l'ordinateur virtuel est victime d'une défaillance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

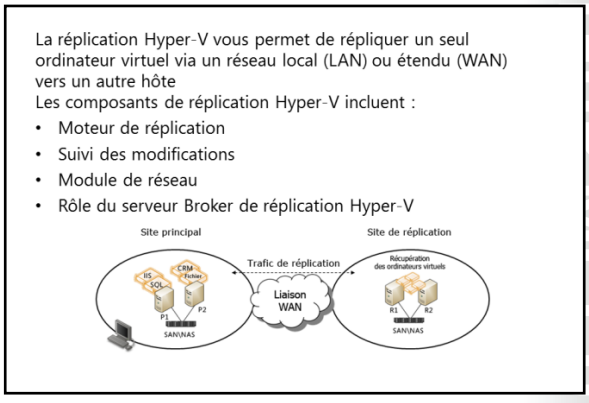
Processus de migration dynamique

Le processus de migration dynamique se déroule en quatre étapes exécutées en arrière-plan :

1. Configuration de la migration. Lorsque vous démarrez le basculement de l'ordinateur virtuel, le nœud source crée une connexion TCP (Transmission Control Protocol) avec l'hôte physique cible. Cette connexion est utilisée pour transférer les données de configuration de l'ordinateur virtuel vers l'hôte physique cible. La migration dynamique crée un ordinateur virtuel temporaire sur l'ordinateur hôte physique cible et alloue de la mémoire à l'ordinateur virtuel de destination. La préparation de la migration vérifie également si l'ordinateur virtuel peut être migré.
2. Transfert invité-mémoire. La mémoire invitée est transférée itérativement à l'hôte cible alors que l'ordinateur virtuel s'exécute toujours sur l'hôte source. Hyper-V sur l'hôte physique source analyse les pages dans la plage de travail. Quand le système modifie les pages en mémoire, il les suit et les marque comme modifiées. Au cours de cette phase de migration, l'ordinateur virtuel en cours de migration continue de s'exécuter. Hyper-V parcourt le processus de copie en mémoire plusieurs fois et, chaque fois, un plus petit nombre de pages modifiées sont copiées sur l'ordinateur physique de destination. Un processus final de copie en mémoire copie les pages en mémoire modifiées restantes vers l'hôte physique de destination. La copie s'arrête dès que le nombre de pages qui ont été modifiées dans la mémoire physique, mais pas encore réécrites sur disque (souvent appelées *pages de modifications*), passe au-dessous d'un seuil ou à l'issue de 10 itérations.
3. Transfert de l'état. Pour migrer réellement l'ordinateur virtuel sur l'hôte cible, Hyper-V interrompt la partition source, transfère l'état de l'ordinateur virtuel (y compris les pages mémoire modifiées restantes) vers l'hôte cible, puis restaure l'ordinateur virtuel sur l'hôte cible. L'ordinateur virtuel est suspendu pendant le transfert de l'état final.
4. Nettoyage. L'étape de nettoyage termine la migration en supprimant l'ordinateur virtuel de l'hôte source, en terminant les threads de travail et en signalant l'achèvement de la migration.

Comment fonctionne le réplica Hyper-V ?

Dans certains cas, vous souhaiterez probablement disposer d'une copie de remplacement d'un ordinateur virtuel que vous pouvez exécuter en cas de défaillance de l'ordinateur virtuel d'origine. Cependant, lorsque vous implémentez la haute disponibilité, vous ne disposez que d'une instance d'ordinateur virtuel. La haute disponibilité n'empêche pas la corruption du logiciel qui s'exécute sur l'ordinateur virtuel. Une façon de traiter le problème de corruption consiste à copier l'ordinateur virtuel. Vous pouvez également sauvegarder l'ordinateur virtuel et son stockage. Bien que cette solution génère l'effet escompté, elle consomme beaucoup de ressources et beaucoup de temps.



Pour résoudre ce problème et permettre à des administrateurs d'avoir une copie à jour d'un ordinateur virtuel unique, Microsoft a implémenté la fonction de réplication Hyper-V dans Windows Server 2012. Cette fonction permet aux ordinateurs virtuels en cours d'exécution sur un site principal ou hôte d'être répliqué de manière efficace vers un site secondaire (ou emplacement ou hôte) à travers un lien WAN ou LAN. Le réplica Hyper-V permet d'avoir deux instances d'un ordinateur virtuel unique résidant sur différents hôtes : une en tant que copie principale (en ligne) et l'autre en tant que copie de réplication (hors connexion). Ces copies sont synchronisées et vous pouvez effectuer un basculement à tout moment. En cas de défaillance d'un site principal, suite à un sinistre naturel, une mise hors tension ou une défaillance de serveur, un administrateur peut utiliser Réplica Hyper-V pour exécuter un basculement des charges de travail vers des serveurs de réplication sur un emplacement secondaire en quelques minutes, entrainant ainsi un temps d'arrêt minimum. Des réplicas Hyper-V sont mis à jour toutes les 5 minutes via un processus de synchronisation. Vous ne pouvez pas modifier cette planification de réplication.

Les configurations de site ne doivent pas utiliser le même serveur, ni le même matériel de stockage. La réplication Hyper-V permet à un administrateur de restaurer les charges de travail virtuelles jusqu'à une limite dans le temps selon les sélections de l'historique de récupération pour l'ordinateur virtuel.

La technologie Réplica Hyper-V se compose des éléments suivants :

- Moteur de réplication : Il gère les détails de la configuration de la réplication et gère les opérations de réplication initiale, de réplication delta, des opérations de basculement et de test de basculement. Il permet également d'effectuer un suivi des évènements de mobilité du stockage et de l'ordinateur virtuel et prend les mesures qui s'imposent, si nécessaire. C'est-à-dire qu'il suspend les événements de réplication jusqu'à ce que les événements de migration se terminent, puis reprend à l'endroit où ces évènements avaient été interrompus.
- Suivi des modifications : Ce composant suit les modifications qui se produisent sur la principale copie de l'ordinateur virtuel. Il est conçu pour suivre les modifications peu importe où résident les fichiers .vhdx de l'ordinateur virtuel.
- Module de réseau : Ce module réseau fournit une façon sécurisée et efficace de transférer les réplicas d'ordinateur virtuel entre les hôtes principaux et les hôtes de réplica. Il utilise la compression de données qui est activée par défaut. L'opération de transfert est sécurisée, car elle se fonde sur l'authentification basée sur des certificats et le protocole HTTPS.
- Rôle du serveur Broker de réplication Hyper-V : C'est un nouveau rôle de serveur qui est implémenté dans Windows Server 2012, et vous le configurez pendant le clustering avec basculement. Ce rôle de serveur vous permet de bénéficier de la fonctionnalité Réplica Hyper-V même lorsque l'ordinateur virtuel répliqué est à haut niveau de disponibilité et peut être déplacé entre deux nœuds de cluster. Le serveur Broker de Réplica Hyper-V redirige tous les événements propres à un ordinateur virtuel vers le nœud approprié dans le cluster de réplica. Le service Broker interroge la base de données d'un cluster pour déterminer quel nœud doit traiter quels événements. Cela garantit que tous les événements sont redirigés vers le nœud approprié du cluster en cas de migration rapide, de migration dynamique ou de migration du stockage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de la réplication Hyper-V

Avant d'implémenter Réplica Hyper-V, assurez-vous que votre infrastructure répond aux conditions requises :

- Le matériel serveur prend en charge le rôle Hyper-V sous Windows Server 2012. En outre, assurez-vous que le matériel serveur possède la capacité suffisante pour exécuter tous les ordinateurs virtuels sur lesquels vous effectuez les réplications.
- L'espace de stockage suffisant est disponible à la fois sur le serveur principal et sur le serveur de réplication pour héberger les fichiers qui sont utilisés par les ordinateurs virtuels répliqués.

Pour configurer un réplica Hyper-V, effectuez les opérations suivantes

1. Configurer les options d'authentification
2. Configurer les ports
3. Sélectionner les serveurs de réplication
4. Sélectionner un emplacement pour les fichiers de réplication
5. Activer la réplication sur l'ordinateur virtuel

- La connectivité réseau existe entre les emplacements hébergeant le serveur principal et le serveur de réplication. La connectivité peut être réalisée via un lien WAN ou LAN.
- Les règles du pare-feu sont correctement configurées pour permettre la réplication entre le site principal et le site de réplication. Par défaut, le trafic transite via le port TCP 80 ou 443.
- Si vous souhaitez utiliser l'authentification basée sur les certificats, assurez-vous qu'un certificat X.509v3 est disponible pour prendre en charge l'authentification réciproque avec des certificats.

Vous n'avez pas à installer Réplica Hyper-V séparément. La réplication Hyper-V est implémentée comme faisant partie du rôle serveur Hyper-V. Vous pouvez l'utiliser sur les serveurs Hyper-V qui sont autonomes ou sur les serveurs qui font partie d'un cluster de basculement (auquel cas vous devez configurer le rôle serveur Broker de Réplica Hyper-V). À la différence du clustering avec basculement, un rôle Hyper-V ne dépend pas d'Active Directory DS. Vous pouvez l'utiliser avec les serveurs Hyper-V autonomes ou qui appartiennent à différents domaines d'Active Directory (hormis lorsque les serveurs font partie d'un cluster de basculement).

Pour activer la fonction Réplica Hyper-V, vous devez tout d'abord configurer les paramètres du serveur Hyper-V. Dans le groupe d'options **Configuration de la réplication**, activez le serveur Hyper-V en tant que serveur de réplication, puis sélectionnez les options d'authentification et de port. Vous devez également configurer les options d'autorisation. Vous pouvez choisir d'activer la réplication à partir d'un serveur quelconque qui est authentifié avec succès, ce qui est commode dans les scénarios où tous les serveurs font partie du même domaine. Vous pouvez aussi saisir les noms de domaine complets des serveurs que vous acceptez comme serveurs de réplicas. En outre, vous devez configurer l'emplacement pour les fichiers de réplication. Vous devez configurer ces paramètres sur chaque serveur défini comme serveur de réplication.

Une fois les options configurées au niveau du serveur, activez la réplication sur un ordinateur virtuel. Au cours de cette configuration, vous devez spécifier à la fois le nom du serveur de réplication et les options de la connexion. Si l'ordinateur virtuel possède plusieurs disques durs virtuels, vous pouvez sélectionner les lecteurs de disque dur virtuel à répliquer. Vous pouvez également configurer l'historique de récupération et la méthode de réplication initiale. Démarrez le processus de réplication, après avoir configuré ces options.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Implémentation de la fonction Réplica Hyper-V (facultatif)

Dans cette démonstration, vous allez apprendre à implémenter la fonction Réplica Hyper-V.

Procédure de démonstration

Configurer un réplica

1. Sur LON-HOST1 et LON-HOST2, configurez chaque serveur afin qu'il soit un serveur de réplication Hyper-V.
   - Authentification : **Kerberos (HTTP)**
   - **Autoriser la réplication à partir de n'importe quel serveur authentifié**
   - Créez et utilisez le dossier **E:\VMReplica** comme emplacement par défaut pour stocker les fichiers de réplication.
2. Activez la règle de pare-feu nommée **Port d'écoute HTTP de réplica Hyper-V (TCP/IN)** sur les deux hôtes.

Configurer la réplication

1. Sur LON-HOST1, activez la réplication pour l'ordinateur virtuel 22412B-LON-CORE.
   - Authentification : **Kerberos (HTTP)**
   - Effectuez la sélection de sorte que seul le point de récupération le plus récent soit disponible.
   - Démarrez la réplication immédiatement.
2. Patientez jusqu'à la fin de la réplication initiale et assurez-vous que l'ordinateur virtuel **22412B-LON-CORE** s'affiche correctement dans le Gestionnaire Hyper-V sur LON-HOST2.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Gestion des environnements virtuels Hyper-V à l'aide de VMM

VMM est membre de la famille System Center 2012 des produits. C'est un successeur de System Center Virtual Machine Manager 2008 R2. VMM développe la fonctionnalité de gestion aux ordinateurs virtuels et hôtes Hyper-V ainsi qu'à permettre le déploiement et la mise en service des ordinateurs virtuels et des services. Dans cette leçon, vous allez découvrir plus en détail VMM.

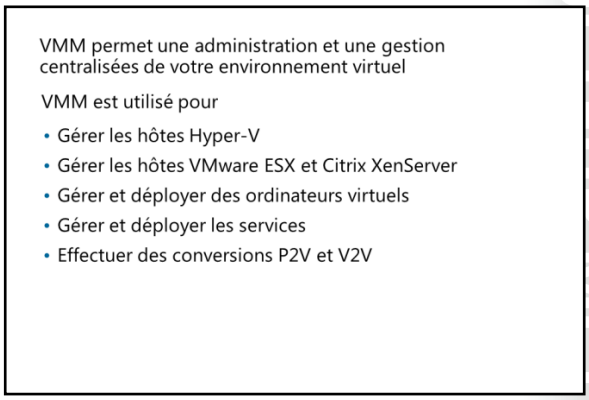
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire VMM ;
- décrire les conditions préalables à l'installation des Services de déploiement Windows ;
- décrire les composants de l'infrastructure du cloud privé dans VMM ;
- décrire comment gérer des hôtes et des groupes d'hôtes avec VMM ;
- décrire comment déployer les ordinateurs virtuels avec VMM ;
- décrire les services et les modèles de service ;
- décrire les migrations physiques-à-virtuelles (P2V) et virtuelles-à-virtuelles (V2V) ;
- décrire les recommandations pour le déploiement d'un serveur VMM à haut niveau de disponibilité.

Qu'est-ce que System Center 2012 - Virtual Machine Manager ?

VMM est une solution de gestion destinée à un centre de données virtuel. VMM vous permet de créer et de déployer des ordinateurs virtuels et des services vers les clouds privés en configurant et en gérant votre hôte de virtualisation, votre réseau et vos ressources de stockage. Vous pouvez également utiliser VMM de gérer les hôtes VMware ESX et Citrix XenServer.



Composant de System Center 2012, VMM découvre, capture et compile les connaissances de l'infrastructure de virtualisation. VMM gère également les stratégies, les processus ainsi que les méthodes conseillées en découvrant, capturant et compilant les connaissances de l'infrastructure de virtualisation.

VMM succède à VMM 2008 R2 et est un composant clé de l'activation des infrastructures de cloud privé, qui favorise la transition de l'infrastructure informatique de l'entreprise depuis un modèle de déploiement concentré sur l'infrastructure vers un environnement orienté utilisateur ou service.

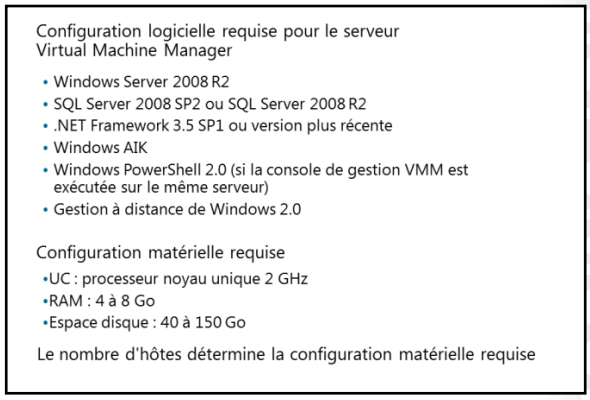
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'architecture VMM est constituée de plusieurs composants interdépendants. Ces composants sont les suivants :

- *Serveur Virtual Machine Manager*. Le serveur de Virtual Machine Manager est l'ordinateur sur lequel le service VMM s'exécute. Le serveur de Virtual Machine Manager exécute les commandes et contrôle les communications avec la base de données Virtual Machine Manager, le serveur de bibliothèques et les hôtes de l'ordinateur virtuel. Le serveur Virtual Machine Manager est le centre d'un déploiement VMM, au travers duquel les autres composants VMM interagissent et communiquent. Le serveur Virtual Machine Manager se connecte également à une base de données Microsoft SQL Server stockant toutes les informations de configuration VMM.
- *Base de données Virtual Machine Manager*. VMM utilise une base de données SQL Server pour stocker les informations affichées dans la console de gestion VMM, notamment les ordinateurs virtuels gérés, les hôtes d'ordinateur virtuel, les bibliothèques d'ordinateurs virtuels, les tâches et d'autres données liées aux ordinateurs virtuels.
- *Console de gestion VMM*. La console de gestion est un programme utilisé pour se connecter à un serveur de gestion VMM, pour visualiser et gérer les ressources physiques et virtuelles, notamment les hôtes d'ordinateur virtuel, les ordinateurs virtuels, les services et les ressources de bibliothèque.
- *Bibliothèque Virtual Machine Manager*. Une *bibliothèque* est un catalogue de ressources (par exemple, disques durs virtuels, modèles et profils) utilisées pour déployer les ordinateurs virtuels et les services. Un serveur de bibliothèque héberge également les dossiers partagés qui stockent les ressources basées sur des fichiers. Le serveur Virtual Machine Management est toujours le serveur de la bibliothèque par défaut, mais vous pouvez ajouter ultérieurement des serveurs de bibliothèques supplémentaires ultérieurement.
- *Interface de commande*. Windows PowerShell est l'interface de ligne de commande utilisée pour exécuter les applets de commande qui effectuent toutes les fonctions VMM disponibles. Vous pouvez utiliser ces applets de commande VMM spécifiques pour gérer toutes les actions d'un environnement VMM.
- *Portail libre-service*. Le portail libre service Virtual Machine Manager est un site Web que les utilisateurs qui sont affectés à un rôle d'utilisateur libre service peuvent utiliser pour déployer et gérer leurs propres ordinateurs virtuels.

Configuration requise pour l'installation de VMM 2012

Avant de déployer VMM et ses composants, assurez-vous que votre système répond aux configurations logicielles et matérielles requises. Même si les configurations logicielles requises ne changent pas en fonction du nombre d'hôtes que gère VMM, la configuration requise en matière de matériel peut varier. En outre, tous les composants VMM n'ont pas les mêmes exigences en termes de logiciel et de matériel.



Remarque : Windows Server 2008 R2 et Windows Server 2012 sont les seuls systèmes d'exploitation pris en charge pour VMM 2012.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Serveur Virtual Machine Manager

Non seulement vous devez disposer de Windows Server 2008 R2 ou Windows Server 2012, mais le logiciel suivant doit être installé sur le serveur qui exécutera le serveur Virtual Machine Manager :

- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) ou version ultérieure
- Kit d'installation automatisée (Windows AIK)
- Windows PowerShell 2.0 (si la console de gestion VMM est exécutée sur le même serveur)
- Gestion à distance de Windows 2.0. Notez que cette installation est effectuée par défaut dans Windows Server 2008 R2, vous laissant juste le soin de vérifier que le service est en cours d'exécution.
- SQL Server SP2 2008 Service Pack 2 (SP2) (Standard ou Enterprise) ou SQL Server 2008 R2 SP1 Standard, Enterprise ou Datacenter. Cela est indispensable uniquement en cas d'installation du serveur de gestion VMM et du serveur SQL sur un même ordinateur.

Les configurations matérielles requises varient, selon le nombre d'hôtes, et dans les limites suivantes :

- UC : processeur noyau unique 2 GHz, processeur double cœur 2,8 GHz
- Mémoire vive (RAM) : 4 à 8 gigaoctets (Go)
- Espace disque : 40 à 150 Go (si la base de données SQL Server est installée sur le même serveur). En outre, si la bibliothèque est sur le même serveur, l'espace disque dépendra alors également du contenu de la bibliothèque.

Base de données Virtual Machine Manager

La base de données Virtual Machine Manager stocke toutes les informations relatives à la configuration VMM, auxquelles vous pouvez accéder et que vous pouvez modifier à l'aide de la console de gestion VMM. La base de données Virtual Machine Manager nécessite SQL Server 2008 SP2 ou une version ultérieure. Pour cette raison, les configurations matérielles de base requises pour la base de données Virtual Machine Manager sont équivalentes à la configuration système minimale requise pour l'installation de SQL Server. En outre, si vous gérez plus de 150 hôtes, vous devez disposer d'au moins 4 Go de mémoire vive sur le serveur de la base de données. Les configurations logicielles requises pour la base de données Virtual Machine Manager sont les mêmes que pour SQL Server.

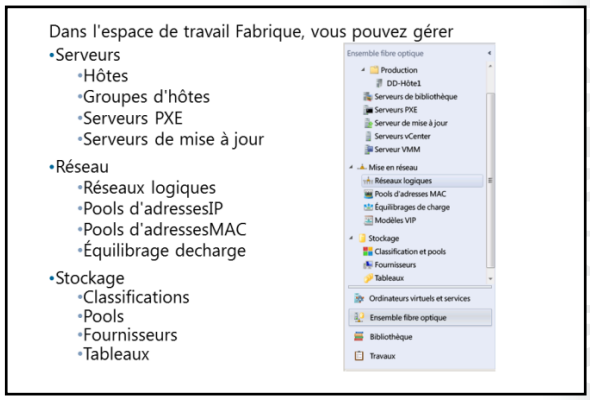
Bibliothèque Virtual Machine Manager

La bibliothèque Virtual Machine Manager est le serveur qui héberge les ressources pour créer des ordinateurs virtuels, des services et des clouds privés. Dans des environnements plus petits, vous installez habituellement la bibliothèque Virtual Machine Manager sur le serveur de gestion VMM. Si c'est le cas, les exigences en matière de logiciel et de matériel sont identiques aux exigences pour le serveur de gestion VMM. Dans des environnements plus grands et plus complexes, nous recommandons d'avoir la bibliothèque Virtual Machine Manager sur un serveur distinct avec une configuration à haut niveau de disponibilité. Si vous souhaitez déployer un autre serveur de bibliothèque Virtual Machine Manager, le serveur doit répondre aux exigences suivantes :

- Système d'exploitation pris en charge : Windows Server 2008 ou Windows Server 2008 R2
- Gestion du matériel : Gestion à distance de Windows 2.0
- UC : au moins 2,8 GHz
- RAM : au moins 2 Go
- Espace disque : varie en fonction du nombre de fichiers stockés et de leur taille

Composants de l'infrastructure du cloud privé dans VMM

Le concept architectural clé dans VMM est l'infrastructure du cloud privé. À l'instar des solutions de cloud public, telles que dans Windows Azure™, l'infrastructure de cloud privé dans VMM est une couche d'abstraction qui protège les complexités techniques sous-jacentes et vous permet de gérer les pools définis de ressources des serveurs, le réseau et le stockage dans l'infrastructure de l'entreprise.



À l'aide de l'interface utilisateur de la console de gestion VMM, vous pouvez créer un cloud privé à partir des hôtes Hyper-V, VMware ESX ou Citrix XenServer. Vous pouvez également tirer parti des caractéristiques du cloud computing, notamment le libre-service, le regroupement des ressources et l'élasticité.

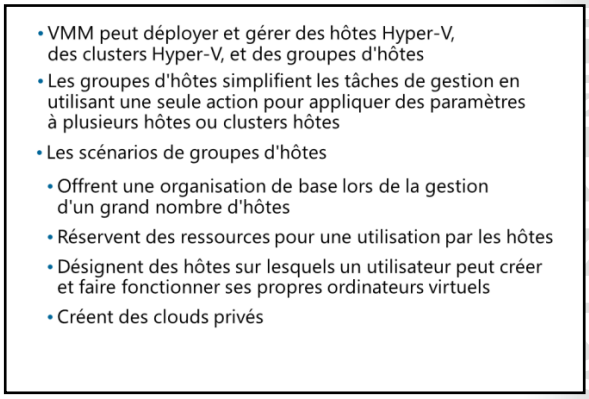
Vous pouvez configurer les ressources suivantes à partir de l'espace de travail Fabrique de la console de gestion VMM :

- Serveurs. Dans le nœud de serveurs, vous pouvez configurer et gérer plusieurs types de serveurs. Les groupes d'hôtes contiennent les hôtes de virtualisation, qui sont les destinations que vous pouvez utiliser pour déployer les ordinateurs virtuels. Les serveurs de bibliothèque sont les référentiels en matière de génération de blocs, tels que des images, les fichiers .iso et les modèles, pour créer des ordinateurs virtuels.
- Mise en réseau. Le nœud de réseau est l'emplacement où vous pouvez définir les réseaux logiques, attribuer des pools d'adresses IP statiques et d'adresses MAC et intégrer les services d'équilibrage de charge. Les réseaux logiques sont des regroupements définis par l'utilisateur de sous-réseaux IP et de réseaux locaux virtuels (VLAN) pour organiser et simplifier les attributions de réseau. Les réseaux logiques fournissent une abstraction de l'infrastructure physique sous-jacente et vous permettent de mettre en service et d'isoler le trafic réseau selon des critères sélectionnés, notamment les propriétés de connectivité et les contrats de niveau de service (SLA).
- Stockage. Vous pouvez découvrir, classifier et configurer le stockage à distance sur des baies de stockage prises en charge. VMM utilise le service de gestion du stockage Microsoft activé par défaut au cours de l'installation de VMM, pour communiquer avec les baies externes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des hôtes, des clusters d'hôtes et des groupes d'hôtes avec VMM

Outre la gestion des ordinateurs virtuels, VMM permet de gérer et de déployer les hôtes Hyper-V. Dans VMM, vous pouvez utiliser les technologies telles que les services de déploiement Windows (Windows DS) pour déployer les hôtes Hyper-V sur les ordinateurs dépourvus de systèmes d'exploitation, puis les gérer avec VMM. Quand les hôtes sont associés à VMM, vous pouvez configurer plusieurs options, telles que les réserves de l'hôte, les quotas, les autorisations, l'appartenance à un cloud. VMM peut également gérer les clusters de basculement Hyper-V.



VMM offre deux nouvelles fonctionnalités qui contribuent à l'optimisation de l'utilisation des ressources et de la consommation d'énergie sur les hôtes gérés par VMM : l'optimisation dynamique et l'optimisation de l'énergie. L'optimisation dynamique équilibre la charge de l'ordinateur virtuel dans un cluster hôte, tandis que l'optimisation de l'énergie permet à VMM d'évacuer les hôtes du cluster équilibrés, puis de les désactiver pour faire des économies d'énergie.

La méthode recommandée pour organiser les hôtes dans VMM consiste à créer des groupes d'hôtes. Cela simplifie les tâches de gestion. Un groupe d'hôtes permet d'appliquer les paramètres à plusieurs hôtes ou clusters d'hôtes avec une action unique. Par défaut, VMM dispose d'un unique groupe d'hôtes nommé Tous les hôtes. Toutefois, au besoin, vous pouvez créer des groupes supplémentaires pour votre environnement.

Les groupes d'hôtes sont hiérarchiques. Lorsque vous créez un nouveau groupe d'hôtes enfant, il hérite des paramètres du groupe d'hôtes parent. Lorsqu'un groupe d'hôtes enfant est déplacé vers un nouveau groupe d'hôtes parent, le groupe d'hôtes enfant conserve ses paramètres d'origine à l'exception des paramètres d'optimisation des ressources et des performances (PRO), qui sont gérés indépendamment. Lorsque les paramètres d'un groupe d'hôtes parent changent, vous pouvez appliquer ces modifications aux groupes d'hôtes enfants.

Voici les scénarios dans lesquels vous pourriez utiliser les groupes d'hôtes :

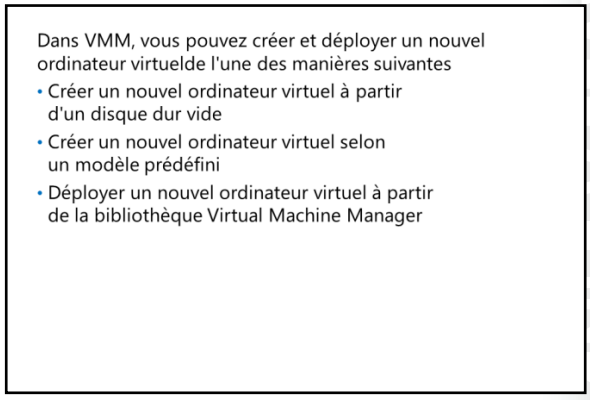
- Disposer d'une organisation de base lorsque vous gérez plusieurs hôtes et ordinateurs virtuels. Vous pouvez créer des vues personnalisées dans les vues Hôtes et Ordinateurs virtuels pour faciliter la surveillance de l'hôte et son accès. Par exemple, vous pouvez créer un groupe d'hôtes pour chaque succursale de votre organisation.
- Réservation de ressources pour une utilisation par les hôtes. Les réserves de ressources de l'ordinateur hôte sont utiles lorsque les ordinateurs virtuels sont placés sur un hôte. Les réserves de ressources de l'ordinateur hôte déterminent la quantité d'UC, de mémoire, d'espace disque, ainsi que la capacité d'E/S du disque et la capacité du réseau disponibles en continu pour le système d'exploitation de l'hôte.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Utiliser l'action propriétés du groupe hôte pour le groupe hôte racine, Tous les hôtes, afin de définir des pools hôte par défaut pour tous les hôtes gérés par VMM. Si vous souhaitez utiliser plus de ressources sur certains hôtes plutôt que sur d'autres, vous pouvez définir des réserves de ressources de l'ordinateur hôte de manière différente pour chaque groupe d'hôtes.
- Désignation d'hôtes sur lesquels les utilisateurs peuvent créer et faire fonctionner leurs propres ordinateurs virtuels. Lorsqu'un administrateur VMM ajoute des rôles d'utilisateur libre-service, une partie de la création du rôle consiste à identifier les hôtes sur lesquels les utilisateurs ou groupes libre-service de ce rôle ont l'autorisation de créer, de faire fonctionner et de gérer leurs propres ordinateurs virtuels. Il est également recommandé d'indiquer un groupe d'hôtes spécifique à cet effet.

Déploiement d'ordinateurs virtuels avec VMM

L'un des avantages que présente l'utilisation de VMM est la souplesse qu'il fournit pour créer et déployer rapidement de nouveaux ordinateurs virtuels.



Avec VMM, vous pouvez créer manuellement un nouvel ordinateur virtuel avec de nouveaux paramètres de configuration et un nouveau disque dur. Vous pouvez ensuite déployer le nouvel ordinateur virtuel à partir de l'une des sources suivantes :

- Un fichier .vhd ou .vhdx existant (vierge ou préconfiguré)
- Un modèle d'ordinateur virtuel
- Une bibliothèque Virtual Machine Manager

Vous pouvez créer des ordinateurs virtuels en convertissant un ordinateur physique existant ou en dupliquant un ordinateur virtuel existant.

Création d'un ordinateur virtuel à partir d'un disque dur virtuel existant

Vous pouvez créer un nouvel ordinateur virtuel basé sur un disque dur virtuel vide (VHD) ou selon un disque dur virtuel préconfiguré qui contient un système d'exploitation invité. VMM fournit deux modèles de disque dur virtuel vierges que vous pouvez utiliser pour créer de nouveaux disques :

- Disque vierge - Petit
- Disque vierge – Grand

Vous pouvez également utiliser un disque dur virtuel vierge quand vous souhaitez utiliser un système d'exploitation avec un environnement PXE (Pre-Boot Execution Environment). À défaut, vous pouvez placer une image .iso sur un DVD-ROM virtuel puis installer un système d'exploitation. Il s'agit d'une manière efficace de créer une image source d'un ordinateur virtuel que vous pourrez utiliser pour référence ultérieure. Pour installer le système d'exploitation sur un ordinateur de ce type, utilisez un fichier d'image .iso à partir de la bibliothèque ou à partir d'un disque local, puis mappez un disque physique de l'ordinateur hôte ou démarrez l'installation du système d'exploitation invité via un démarrage du service réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous avez une bibliothèque de disques durs virtuels que vous souhaitez utiliser dans votre environnement VMM, vous pouvez créer un ordinateur virtuel d'un disque dur virtuel existant. Vous pouvez également choisir des disques durs virtuels existants lors du déploiement de tout système d'exploitation à partir duquel VMM ne peut pas créer de modèle, notamment un système d'exploitation qui n'est pas basé sous Windows.

Lorsque vous créez un nouvel ordinateur virtuel à l'aide d'un disque dur virtuel existant, vous créez en fait une nouvelle configuration d'ordinateur virtuel associée au fichier du disque dur virtuel. VMM crée une copie du disque dur virtuel source pour vous éviter d'avoir à déplacer ou modifier le fichier VHD original. Dans ce scénario, le disque dur virtuel source doit répondre aux conditions suivantes :

- Vous devez laisser le mot de passe Administrateur sur le disque dur virtuel vierge original dans le cadre du processus de l'outil de préparation du système (Sysprep).
- Installez Virtual Machine Additions sur l'ordinateur virtuel.
- Utilisez Sysprep pour préparer le système d'exploitation pour la duplication.

 **Remarque :** Une fois que VMM 2012 SP1 est publié, VMM 2012 prendra en charge le format de disque dur virtuel .vhdx.

Déploiement à partir d'un modèle

Vous pouvez créer un ordinateur virtuel à partir d'un modèle de la bibliothèque de Virtual Machine Manager. Le modèle est une ressource de bibliothèque, qui établit la liaison avec un disque VHD doté d'un système d'exploitation, de paramètres matériels et de paramètres de système d'exploitation invité généralisés. Vous utilisez les paramètres du système d'exploitation invité pour configurer les paramètres du système d'exploitation tels que le nom de l'ordinateur, le mot de passe d'administrateur local et l'appartenance au domaine.

Le processus de déploiement ne modifie pas le modèle que vous pouvez réutiliser plusieurs fois. Si vous créez des ordinateurs virtuels dans le portail libre-service, vous devez utiliser un modèle.

Les conditions requises suivantes s'appliquent si vous souhaitez déployer un nouvel ordinateur virtuel à partir d'un modèle :

- Vous devez installer un système d'exploitation pris en charge sur le disque dur virtuel.
- Vous devez laisser le mot de passe Administrateur sur le disque dur virtuel vierge dans le cadre du processus SysPrep. Toutefois, le mot de passe Administrateur pour le profil du système d'exploitation invité ne doit pas être vide.
- Pour les schémas personnalisés, vous devez préparer le système d'exploitation sur le disque dur virtuel en supprimant les informations d'identité de l'ordinateur. Pour les systèmes d'exploitation Windows, vous pouvez préparer le disque dur virtuel à l'aide de l'outil Sysprep.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Déploiement à partir de la bibliothèque Virtual Machine Manager

Si vous déployez un ordinateur virtuel de la bibliothèque Virtual Machine Manager, l'ordinateur virtuel est supprimé de la bibliothèque, puis placé sur l'hôte sélectionné. Lorsque vous utilisez cette méthode, vous devez fournir les détails suivants dans l'Assistant Déploiement de l'ordinateur virtuel :

- Hôte du déploiement. Le modèle que vous utilisez fournit une liste d'hôtes potentiels et leurs évaluations.
- Le chemin d'accès des fichiers d'ordinateur virtuel sur l'hôte.
- Réseaux virtuels à utiliser pour l'ordinateur virtuel. Une liste des réseaux virtuels existants sur l'hôte s'affiche.

Que sont les services et les modèles de services ?

Les services sont un nouveau concept dans VMM. Vous devez bien comprendre la notion de services avant de déployer une infrastructure de cloud privé.

- Par rapport à VMM, un service est un ensemble d'un ou de plusieurs ordinateurs virtuels qui sont déployés ensemble et gérés en tant qu'entité unique
- Un modèle de service encapsule tous les composants nécessaires pour déployer et exécuter une nouvelle instance d'une application
  - Un service est déployé par un administrateur ou un utilisateur final
  - Un service peut contenir plusieurs composants différents
  - Un service peut être déployé vers un cloud privé ou vers un groupe d'hôtes
  - L'administrateur crée un modèle de service dans VMM
  - Le propriétaire de l'application déploie un service selon le modèle de service
  - L'administrateur utilise le Contrôleur ou le Gestionnaire VMM pour déployer le service en fonction du modèle

Scénario de services traditionnel

Les services désignent habituellement des applications ou des ensembles d'applications qui offrent des services aux utilisateurs finaux. Par exemple, vous pouvez non seulement déployer différents types de services basés sur le Web, mais vous pouvez également implémenter un service tel que la messagerie électronique. Dans un scénario de non-cloud computing, le déploiement de tout type de service nécessite généralement de la part des utilisateurs, des développeurs et des administrateurs qu'ils travaillent ensemble sur les phases de création, de déploiement, de test d'un service, sans oublier la phase d'entretien.

Un service inclut souvent plusieurs ordinateurs qui doivent travailler ensemble pour offrir un service aux utilisateurs finaux. Par exemple, un service Web est habituellement une application qui se déploie sur un serveur Web, se connecte à un serveur de base de données qui pourrait être hébergé sur un autre ordinateur, et exécute l'authentification sur un contrôleur de domaine Active Directory. L'activation de cette application nécessite trois rôles, et probablement trois ordinateurs : un serveur Web, un serveur de base de données et un contrôleur de domaine. Le déploiement d'un environnement de test pour un service de ce type peut prendre du temps et consommer de nombreuses ressources. Dans le meilleur des cas, les développeurs travaillent avec les administrateurs informatiques pour créer un environnement où ils peuvent déployer et tester leur application Web.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Concept d'un service dans un scénario de cloud privé

Avec le concept de cloud privé, la manière dont vous traitez les services peut varier considérablement. Vous pouvez préparer l'environnement pour un service, puis laisser aux développeurs le soin de le déployer à l'aide d'une application libre service, telle que System Center 2012 - Contrôleur de l'application.

Dans VMM, un *service* est un ensemble d'un ou plusieurs ordinateurs virtuels que vous déployez et gérez ensemble en tant qu'entité unique. Vous configurez ces ordinateurs afin qu'ils fonctionnent ensemble pour fournir un service. Avec Windows Server 2008, les utilisateurs pouvaient déployer de nouveaux ordinateurs virtuels à l'aide du portail libre-service. Dans VMM, les utilisateurs finaux peuvent déployer de nouveaux services. En déployant un service, les utilisateurs déploient en fait la totalité de l'infrastructure, notamment les ordinateurs virtuels, les connexions au réseau et les applications indispensables au bon fonctionnement du service.

Cependant, vous pouvez également utiliser les services pour déployer uniquement un seul ordinateur virtuel sans objectif spécifique. Au lieu de déployer des ordinateurs virtuels de manière habituelle, désormais vous pouvez créer un service qui déploiera un ordinateur virtuel avec, par exemple, Windows Server 2008 R2 et plusieurs rôles et fonctionnalités préinstallés et joints au domaine. Cela simplifie le processus de création et de mise à jour ultérieure des nouveaux ordinateurs virtuels.

Le déploiement d'un nouveau service nécessite un haut niveau d'automatisation et de composants prédéfinis et requiert également la prise en charge du logiciel de gestion. C'est la raison pour laquelle VMM propose des modèles de service. Un modèle de service est un modèle qui encapsule tout ce qui est nécessaire pour déployer et exécuter la nouvelle instance d'une application. De la même façon qu'un utilisateur de cloud privé peut créer de nouveaux ordinateurs virtuels à la demande, l'utilisateur peut également utiliser les modèles de service pour installer et démarrer de nouvelles applications à la demande.

Processus de déploiement d'un nouveau service

Utilisez la procédure suivante quand vous utilisez des modèles de service VMM pour déployer un nouveau service ou une nouvelle application :

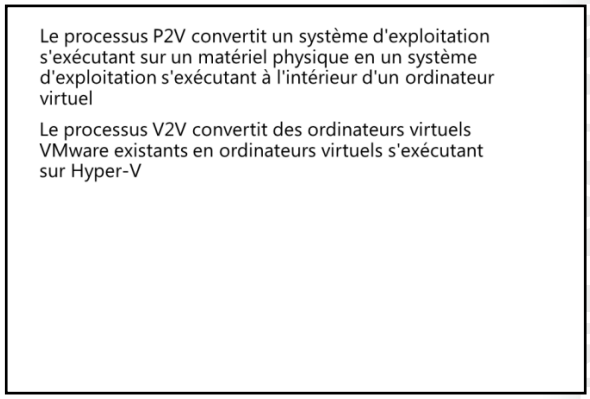
1. L'administrateur système crée et configure les modèles de service VMM à l'aide du concepteur de modèles de service.
2. Le propriétaire de l'application de l'utilisateur final (par exemple, un développeur qui doit déployer l'environnement de l'application) ouvre la console du contrôleur de l'application et demande un nouveau déploiement de service selon les modèles de service auxquels le développeur a accès. Le développeur peut déployer le service vers un cloud privé auquel un utilisateur a accès. En tant qu'alternative au contrôleur de l'application, l'utilisateur peut également utiliser la console de gestion VMM.
3. Le serveur Virtual Machine Manager évalue la demande envoyée. VMM recherche les ressources disponibles dans le cloud privé, puis calcule le quota de l'utilisateur et vérifie que le cloud privé a suffisamment de ressources pour le déploiement du service demandé.
4. Lorsque le nouveau service est créé automatiquement, les ordinateurs virtuels et les applications (le cas échéant) sont déployées sur l'hôte sélectionné par VMM.
5. Le propriétaire de l'application de l'utilisateur parvient à contrôler les ordinateurs virtuels des services via le contrôleur de l'application ou via le protocole RDP (Remote Desktop Protocol).
6. Si vous avez besoin de l'approbation manuelle pour la création des ressources, vous pouvez utiliser le gestionnaire de service System Center 2012 pour créer des workflows à cet effet.

Informations incluses dans le modèle de service

Le modèle de service comprend les informations relatives aux ordinateurs virtuels qui sont déployés en tant que partie du service, aux applications qu'il convient d'installer sur les ordinateurs virtuels ainsi qu'à la configuration de réseau nécessaire pour le service (y compris l'utilisation de services d'équilibrage de charge). Le modèle de service peut utiliser les modèles d'ordinateurs virtuels existants. Même si vous pouvez définir le service sans utiliser de modèle d'ordinateur virtuel existant, il est plus facile de créer un modèle si vous avez déjà créé des modèles d'ordinateur virtuel. Une fois que vous avez créé le modèle de service, il convient de le configurer pour son déploiement à l'aide de l'option **Configurer le déploiement**.

Migrations P2V et V2V

Bon nombre d'organisations ont des serveurs physiques qu'elles n'utilisent pas complètement. VMM peut convertir les ordinateurs physiques existants en ordinateurs virtuels via un processus appelé « conversion physique-à-virtuelle » (P2V). VMM simplifie la conversion P2V en fournissant un assistant basé sur des tâches pour l'automatisation de la majeure partie du processus de conversion. Étant donné que le processus P2V prend en charge les scripts, vous pouvez lancer des conversions P2V à grande échelle via l'interface en ligne de commande Windows PowerShell.



VMM convertit un système d'exploitation s'exécutant sur un matériel physique en système d'exploitation s'exécutant dans un environnement d'ordinateur virtuel Hyper-V. VMM fournit un assistant de conversion qui automatise une grande partie du processus de conversion.

Lors du processus de conversion P2V, VMM génère des images de disques sur les disques durs de l'ordinateur physique. Il crée les fichiers .vhd pour le nouvel ordinateur virtuel, à l'aide d'images de disque comme base. En outre, il crée une configuration matérielle pour l'ordinateur virtuel qui est similaire, voir identique, au matériel de l'ordinateur physique.

Le nouvel ordinateur virtuel a la même identité que l'ordinateur physique sur lequel il est basé. De ce fait, nous vous conseillons de ne pas utiliser simultanément un ordinateur physique et son réplica virtuel. Une fois la conversion P2V effectuée, vous devez généralement déconnecter l'ordinateur physique du réseau et le désaffecter.

La conversion P2V s'achève en mode connecté ou déconnecté. En mode connecté, le système d'exploitation source s'exécute pendant le processus de conversion. En mode déconnecté, le système d'exploitation ne s'exécute pas et la conversion se produit dans l'environnement de préinstallation Windows (Windows PE). Les rubriques ultérieures de cette leçon décrivent ces modes de manière plus approfondie.

Outre le fait de convertir les ordinateurs physiques peu employés, VMM prend en charge la gestion, le transfert et les conversions d'autres ordinateurs virtuels que vous avez créés dans VMware. Vous pouvez convertir ces ordinateurs virtuels en ordinateurs virtuels Hyper-V, les placer sur des hôtes Hyper-V, puis les gérer dans la console Administrateur Virtual Machine Manager. En outre, VMM et Hyper-V prennent en charge la migration des ordinateurs virtuels, d'un hôte vers un autre, avec un temps d'arrêt minimal voire nul.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

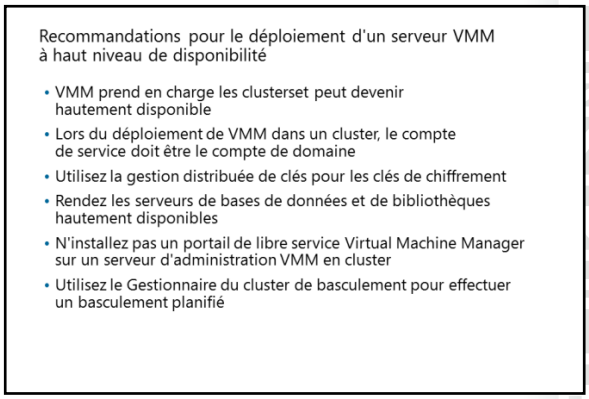
VMM vous permet de convertir les ordinateurs virtuels VMware existants en ordinateurs virtuels qui s'exécutent sur la plateforme Hyper-V. Ce processus est appelé *conversion V2V*. Avec la conversion V2V, les administrateurs peuvent consolider un environnement virtuel qui exécute différentes plateformes virtuelles sans déplacer de données, ni reconstruire les ordinateurs virtuels à partir de zéro.

VMM permet de copier les ordinateurs virtuels VMware existants et créer des ordinateurs virtuels Hyper-V. Vous pouvez copier les ordinateurs virtuels VMware qui sont situés sur des hôtes de serveur ESX, dans les bibliothèques Virtual Machine Manager ou sur des partages Windows. Même si V2V est appelé une conversion, V2V est une opération en lecture seule qui ne supprime ni n'affecte l'ordinateur virtuel source d'origine. En outre, le terme conversion désigne uniquement le processus de conversion d'ordinateurs virtuels VMware. Le terme migration est utilisé pour les serveurs virtuels.

Pendant le processus de conversion, VMM convertit les fichiers VMware .vmdk en fichiers .vhd, et rend le système d'exploitation de l'ordinateur virtuel compatible avec les technologies de virtualisation de Microsoft. L'ordinateur virtuel créé par l'Assistant respecte les propriétés de l'ordinateur virtuel VMware, y compris son nom, sa description, sa mémoire et les attributions disque-bus.

Recommandations pour le déploiement d'un serveur de gestion VMM à haut niveau de disponibilité

VMM prend désormais en charge un serveur de gestion VMM à haut niveau de disponibilité. Vous pouvez utiliser le clustering avec basculement pour bénéficier d'une disponibilité optimale pour VMM, car cette dernière est désormais une application qui prend en charge les clusters. Cependant, vous devez tenir compte de plusieurs éléments avant de déployer un cluster VMM.



Avant d'installer un serveur de gestion VMM à haut niveau de disponibilité, vérifiez les points suivants :

- Vous avez installé et configuré un cluster de basculement qui exécute Windows Server 2008 R2, Windows Server 2008 R2 SP1 ou Windows Server 2012.
- Tous les ordinateurs sur lesquels vous installez le serveur Virtual Machine Manager à haut niveau de disponibilité répondent à la configuration matérielle minimale requise et tout logiciel prérequis est installé sur tous les ordinateurs.
- Vous avez créé un compte de domaine à utiliser par le service VMM. Vous devez utiliser un compte d'utilisateur de domaine pour un serveur Virtual Machine Manager à haut niveau de disponibilité.
- Vous êtes prêt à utiliser la gestion distribuée de clés pour enregistrer les clés de chiffrement dans Active Directory DS. Vous devez utiliser la gestion distribuée de clés pour un serveur Virtual Machine Manager à haut niveau de disponibilité.
- Vous avez un ordinateur sur lequel SQL Server est pris en charge, installé et en cours d'exécution. À la différence de VMM 2008 R2, VMM n'installera pas automatiquement de version de SQL Server Express Edition.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Bases de données et serveurs de bibliothèque à haut niveau de disponibilité

Pour assurer la redondance totale, utilisez un serveur SQL à haut niveau de disponibilité. Installez un serveur SQL à haut niveau de disponibilité sur un cluster de basculement distinct à partir du cluster de basculement sur lequel vous installez le serveur Virtual Machine Manager à haut niveau de disponibilité. De même, utilisez également un serveur de fichiers à haut niveau de disponibilité pour héberger vos partages de bibliothèque.

Portail de libre service et serveur Virtual Machine Manager en cluster

Il est recommandé de ne pas installer le portail libre-service Virtual Machine Manager sur le même ordinateur que le serveur Virtual Machine Manager à haut niveau de disponibilité. Si votre portail en libre service Virtual Machine Manager réside actuellement sur le même ordinateur que le serveur Virtual Machine Manager, nous vous recommandons de désinstaller le portail en libre service Virtual Machine Manager pour VMM 2008 R2 SP1 avant l'installation de la mise à niveau VMM. Nous vous recommandons également d'installer le portail libre-service Virtual Machine Manager sur un serveur Web à haut niveau de disponibilité pour garantir la redondance et l'équilibrage de la charge.

Gestionnaire du cluster de basculement

Vous ne pouvez pas effectuer de basculement planifié, par exemple pour installer une mise à jour de sécurité ou effectuer la maintenance sur un nœud de cluster, à l'aide de la console Administrateur Virtual Machine Manager. Préférez un basculement planifié et pour ce faire, utilisez le Gestionnaire du cluster de basculement.

Au cours d'un basculement planifié, veillez à ce qu'il n'y ait aucune tâche en cours sur le serveur Virtual Machine Manager. Toutes les tâches en cours d'exécution pendant un basculement seront arrêtées et ne reprendront pas automatiquement. Toutes les connexions à un serveur Virtual Machine Manager à haut niveau de disponibilité depuis la console Administrateur Virtual Machine Manager ou le portail en libre service Virtual Machine Manager seront également perdues au cours d'un basculement. Cependant, la console Administrateur Virtual Machine Manager peut se reconnecter automatiquement au serveur Virtual Machine Manager à haut niveau de disponibilité après un basculement si la console était ouverte avant l'exécution du basculement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation du clustering avec basculement à l'aide d'Hyper-V

Scénario

Le déploiement initial des ordinateurs virtuels sur Hyper-V est une réussite pour A. Datum Corporation. En tant que prochaine étape du déploiement, A. Datum envisage à présent les moyens de garantir que les services et les applications déployés sur les ordinateurs virtuels présentent un haut niveau de disponibilité. Dans le cadre de l'implémentation, A. Datum considère également les options permettant d'exécuter les ordinateurs virtuels sur Hyper-V avec un haut niveau de disponibilité.

Vous êtes responsable de l'intégration d'Hyper-V avec le clustering avec basculement pour garantir que les ordinateurs virtuels déployés sur Hyper-V ont un haut niveau de disponibilité. Vous êtes également responsable de la planification de l'ordinateur virtuel et de la configuration du stockage, ainsi que de l'implémentation des ordinateurs virtuels en tant que services à haut niveau de disponibilité sur le cluster de basculement. En outre, vous envisagez d'autres outils, telles que Réplica Hyper-V, pour garantir un haut niveau de disponibilité pour les ordinateurs virtuels.

Objectifs

- Configuration de Réplica Hyper-V.
- Configuration d'un cluster avec basculement pour Hyper-V.
- Configuration d'un ordinateur virtuel à haute disponibilité.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateurs virtuels	**22412B-LON-DC1-B** **22412B-LON-SVR1-B** **22412B-LON-HOST1** **22412B-LON-HOST2**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Cet atelier pratique doit être effectué en binôme. Pour effectuer cet atelier pratique, vous devez démarrer les ordinateurs hôtes à partir de Windows Server 2012. Assurez-vous que vous et votre partenaire avez démarré dans différents hôtes (un doit démarrer dans 22412B-LON-HOST1 et l'autre doit démarrer dans 22412B-LON-HOST2) puis connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**. Une fois que vous avez démarré dans l'environnement Windows Server 2012, effectuez les tâches d'installation suivantes :

1. Sur l'ordinateur hôte, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, démarrez les ordinateurs virtuels suivants en fonction de votre hôte :
   - Pour LON-HOST1, démarrez **22412B-LON-DC1-B**.
   - Pour LON-HOST2, démarrez **22412B-LON-SVR1-B**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   a. Nom d'utilisateur : **Adatum\Administrateur**
   b. Mot de passe : **Pa$$w0rd**

Exercice 1 : Configuration des réplicas Hyper-V

Scénario

Avant de commencer avec le déploiement du cluster, vous devez évaluer la nouvelle technologie Hyper-V dans Windows Server 2012 pour la réplication des ordinateurs virtuels entre les hôtes. Vous souhaitez être apte à monter manuellement une copie d'un ordinateur virtuel sur un autre hôte en cas d'échec de la copie (ou de l'hôte) active.

Les tâches principales de cet exercice sont les suivantes :

1. Démarrez les ordinateurs hôtes physiques à partir du disque dur virtuel
2. Importation de l'ordinateur virtuel LON-CORE sur LON-HOST1
3. Configurer un réplica sur les deux ordinateurs hôtes
4. Configuration de la réplication pour l'ordinateur virtuel LON-CORE
5. Valider un basculement planifié vers le site de réplication

▶ Tâche 1 : Démarrez les ordinateurs hôtes physiques à partir du disque dur virtuel

1. Redémarrez l'ordinateur de la classe, et dans le **Windows Boot Manager**, cliquez sur **22412B-LON-HOST1** ou **22412B-LON-HOST2**.

Remarque : Si vous démarrez LON-HOST1, votre partenaire doit faire de même avec LON-HOST2.

2. Ouvrez une session en tant que **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Sur LON-HOST1, assurez-vous que l'ordinateur virtuel **22412B-LON-DC1** est en cours d'exécution.
4. Sur LON-HOST2, assurez-vous que l'ordinateur virtuel **22412B-LON-SVR1** est en cours d'exécution.

▶ Tâche 2 : Importation de l'ordinateur virtuel LON-CORE sur LON-HOST1

- Sur LON-HOST1, ouvrez le Gestionnaire Hyper-V, et importez l'ordinateur virtuel **22412B-LON-CORE** avec les paramètres suivants :
  - Chemin d'accès : **E:\Programmes\Microsoft Learning\22412\Drivers\22412B-LON-CORE**
  - Acceptez les valeurs par défaut

Remarque : La lettre du lecteur peut varier en fonction du nombre de lecteurs sur l'ordinateur hôte physique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer un réplica sur les deux ordinateurs hôtes

1. Sur LON-HOST1 et LON-HOST2, configurez chaque serveur comme serveur Réplica Hyper-V avec les paramètres suivants :
   - Authentification : **Kerberos (HTTP)**
   - **Autoriser la réplication à partir de n'importe quel serveur authentifié**
   - Créez et utilisez le dossier **E:\VMReplica** comme emplacement par défaut pour stocker les fichiers de réplication.
2. Activez la règle de pare-feu nommée **Écouteur HTTP de replica Hyper-V (TCP-IN)** sur les deux hôtes.

▶ Tâche 4 : Configuration de la réplication pour l'ordinateur virtuel LON-CORE

1. Sur LON-HOST1, activez la réplication pour l'ordinateur virtuel **22412B-LON-CORE** avec les paramètres suivants :
   - Serveur réplica : **LON-HOST2**
   - Authentification : **Authentification Kerberos (HTTP)**
   - Configurer l'historique de récupération : **Uniquement le dernier point de récupération**
   - **Démarrer la réplication immédiatement**
2. Patientez jusqu'à la fin de la réplication initiale et vérifiez que l'ordinateur virtuel **22412B-LON-CORE** s'affiche correctement dans la console Gestionnaire Hyper-V sur LON-HOST2.

▶ Tâche 5 : Valider un basculement planifié vers le site de réplication

1. Sur LON-HOST2, affichez l'intégrité de la réplication pour **22412B-LON-CORE**.
2. Sur LON-HOST1, effectuez le basculement planifié vers **LON-HOST2**. Vérifiez que **22412B-LON-CORE** est exécuté sur LON-HOST2.
3. Sur LON-HOST1, supprimez la réplication pour **22412B-LON-CORE**.
4. Sur LON-HOST2, arrêtez 22412B-LON-CORE.

Résultats : À l'issue de cet exercice, vous aurez configuré un réplica Hyper-V.

Exercice 2 : Configuration d'un cluster avec basculement pour Hyper-V

Scénario

A. Datum dispose de plusieurs ordinateurs virtuels qui hébergent les services importants avec un haut niveau de disponibilité. Puisque ces services ne prennent pas en charge les clusters, A. Datum a décidé d'implémenter le clustering de basculement au niveau de l'hôte Hyper-V. Vous prévoyez d'utiliser des lecteurs iSCSI comme stockage pour ces ordinateurs virtuels.

Les tâches principales de cet exercice sont les suivantes :

1. Connectez-vous à la cible iSCSI à partir des deux ordinateurs hôtes
2. Configurer un clustering avec basculement sur les deux ordinateurs hôtes
3. Configuration des disques pour le cluster de basculement

UTILISATION RÉSERVÉE À L'INSTRUCTEUR – MCT UNIQUEMENT

▶ Tâche 1 : Connectez-vous à la cible iSCSI à partir des deux ordinateurs hôtes

1. Sur LON-HOST1, démarrez l'**initiateur iSCSI**.
2. Utilisez **172.16.0.21** pour l'adresse qui sera utilisée pour découvrir la cible iSCSI et s'y connecter.
3. Sur LON-HOST2, démarrez l'**initiateur iSCSI**.
4. Utilisez **172.16.0.21** pour l'adresse qui sera utilisée pour découvrir la cible iSCSI et s'y connecter.
5. Sur LON-HOST2, accédez à **Gestion des disques**, et initialisez et mettez en ligne tous les lecteurs iSCSI en procédant comme suit :
   - Formatez le premier lecteur et nommez-le **ClusterDisk**.
   - Formatez le second lecteur et nommez-le **ClusterVMs**.
   - Formatez le troisième lecteur et nommez-le **Quorum**.
6. Sur LON-HOST1, accédez à **Gestion des disques**, et mettez en ligne les trois lecteurs iSCSI.

▶ Tâche 2 : Configurer un clustering avec basculement sur les deux ordinateurs hôtes

1. Sur LON-HOST1 et LON-HOST2, installez le clustering avec basculement.
2. Sur LON-HOST1, créez un cluster de basculement avec les paramètres suivants :
   - Ajoutez **LON-HOST1** et **LON-HOST2**
   - Nommez le cluster **VMCluster**
   - Attribuez l'adresse **172.16.0.126**
   - Désélectionnez l'option **Ajouter la totalité du stockage disponible au cluster**

▶ Tâche 3 : Configuration des disques pour le cluster de basculement

1. Sur LON-HOST1, Dans le Gestionnaire du cluster de basculement, ajoutez les trois disques iSCSI au cluster.
2. Vérifiez que chacun des trois disques iSCSI est disponible pour le stockage en cluster.
3. Ajoutez le disque nommé **ClusterVMs** à **Volumes partagés de cluster**.
4. À partir du nœud **VMCluster.adatum.com**, sélectionnez **Autres actions**, puis configurez les **paramètres de quorum du cluster** pour utiliser les paramètres standard.

Résultats : Après avoir terminé cet exercice, vous aurez configuré un cluster de basculement pour Hyper-V.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Configuration d'un ordinateur virtuel hautement disponible

Scénario

Après avoir configuré le cluster de basculement Hyper-V, vous souhaitez ajouter des ordinateurs virtuels en tant que ressources à haut niveau de disponibilité. En outre, il est conseillé d'évaluer la migration dynamique et tester la migration du stockage.

Les tâches principales de cet exercice sont les suivantes :

1. Déplacer le stockage de l'ordinateur virtuel vers la cible iSCSI
2. Configurer l'ordinateur virtuel en tant qu'ordinateur à haut niveau de disponibilité
3. Exécuter une migration dynamique pour l'ordinateur virtuel
4. Réalisation d'une migration du stockage pour l'ordinateur virtuel

▶ Tâche 1 : Déplacer le stockage de l'ordinateur virtuel vers la cible iSCSI

1. Dans le Gestionnaire du cluster de basculement, vérifiez que **LON-HOST1** est le propriétaire du disque **ClusterVMs**. Si tel n'est pas le cas, déplacez le disque ClusterVMs vers LON-HOST1.
2. Sur LON-HOST1, ouvrez une fenêtre de l'Explorateur de fichiers, et accédez à **E:\Programmmes\Microsoft Learning\22412\Drivers\22412B-LON-CORE\Virtual Hard Disks**.
3. Déplacez **22412B-LON-CORE.vhd** à l'emplacement **C:\ClusterStorage\Volume1** .

▶ Tâche 2 : Configurer l'ordinateur virtuel en tant qu'ordinateur à haut niveau de disponibilité

1. sur LON-HOST1, dans le Gestionnaire du cluster de basculement, cliquez sur **Rôles**, puis démarrez l'Assistant Nouvel ordinateur virtuel.
2. Configurez un ordinateur virtuel avec les paramètres suivants :
   - Nœuds du cluster : **LON-HOST1**
   - Nom de l'ordinateur : **TestClusterVM**
   - Enregistrez le fichier dans **C:\ClusterStorage\Volume1**
   - RAM pour TestClusterVM : **1536** Mo
   - Connectez l'ordinateur au lecteur de disque dur virtuel **22412B-LON-CORE.vhd** existant à l'emplacement **C:\ClusterStorage\Volume1**
3. À partir du nœud **Rôles**, démarrez l'ordinateur virtuel.

▶ Tâche 3 : Exécuter une migration dynamique pour l'ordinateur virtuel

1. Sur LON-HOST1, dans le Gestionnaire du cluster de basculement, démarrez le basculement de **migration dynamique** de **TestClusterVM** entre LON-HOST1 et LON-HOST2.
2. Connectez-vous à **TestClusterVM**, assurez-vous que vous pouvez l'utiliser pendant sa migration vers un autre hôte.

▶ Tâche 4 : Réalisation d'une migration du stockage pour l'ordinateur virtuel

1. Sur LON-HOST2, ouvrez le **Gestionnaire Hyper-V**.
2. Déplacez **22412B-LON-SVR1-B** de sa position actuelle vers **C:\LON-SVR1**.
3. Déterminez si l'ordinateur est opérationnel pendant le processus de déplacement.
4. À l'issue de la migration, arrêtez tous les ordinateurs virtuels en cours d'exécution.

Résultats : À la fin de cet exercice, vous aurez déployé et configuré un ordinateur virtuel à haut niveau de disponibilité.

▶ Préparer le prochain module

1. Redémarrez **LON-HOST1**.
2. À l'invite du menu de démarrage, sélectionnez **Windows Server 2008 R2**, et appuyez sur Entrée.
3. Connectez-vous à l'ordinateur hôte, comme demandé par votre instructeur.
4. Répétez les étapes 1 à 3 sur **LON-HOST2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée :

- Développez les configurations standard avant d'implémenter les ordinateurs virtuels à haut niveau de disponibilité. Les ordinateurs hôtes doivent être configurés de la façon la plus proche possible. Afin de vous assurer que vous avez une plateforme Hyper-V cohérente, configurez des noms réseau standard et utilisez des normes d'affectation de noms cohérentes pour les volumes CSV.
- Implémentez la protection VMM. VMM fournit une couche de gestion sur Hyper-V et le Gestionnaire du cluster de basculement pouvant vous empêcher de réaliser des erreurs de gestion des ordinateurs virtuels hautement disponible. Par exemple, cela vous empêche de créer des ordinateurs virtuels sur un stockage qui n'est pas accessible à partir de tous les nœuds du cluster.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Le basculement d'ordinateur virtuel échoue après l'implémentation de CSV et la migration du stockage partagé sur CSV	
Un ordinateur virtuel bascule vers un autre nœud du cluster hôte, mais perd toute la connectivité réseau	
Quatre heures après le redémarrage d'un hôte Hyper-V membre d'un cluster hôte, aucun ordinateur virtuel ne s'exécute encore sur l'hôte.	

Questions de contrôle des acquis

Question : Dans Windows Server 2008 R2, devez-vous implémenter CSV afin de fournir une haute disponibilité aux ordinateurs virtuels dans VMM ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12

Implémentation de la récupération d'urgence

Table des matières :

Vue d'ensemble du module **12-1**

Leçon 1 : Vue d'ensemble de la récupération d'urgence **12-2**

Leçon 1 : Implémentation de la Sauvegarde Windows Server **12-8**

Leçon 1 : Implémentation de la récupération de données et de serveurs **12-19**

Atelier pratique : Implémentation des fonctionnalités de sauvegarde et de restauration de Windows Server **12-25**

Contrôle des acquis et éléments à retenir **12-31**

Évaluation du cours **12-32**

Vue d'ensemble du module

Les organisations sont toujours vulnérables à la perte de certaines de leurs données, pour des raisons telles que la suppression accidentelle, la corruption du système de fichiers, les défaillances matérielles, les utilisateurs malveillants et les catastrophes naturelles. De ce fait, les organisations doivent avoir des stratégies de récupération bien définies et testées, qui les aideront à rétablir l'état de santé et de fonctionnement de leurs serveurs et données, et ce le plus rapidement possible.

Dans ce module, vous allez apprendre à identifier des risques de sécurité de votre organisation. Vous découvrirez également la récupération d'urgence et ses configurations requises. Vous apprendrez à organiser une sauvegarde au sein de votre organisation et à évaluer les mesures à prendre pour récupérer des données.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- Décrire les concepts de récupération d'urgence.
- Implémenter la fonctionnalité Sauvegarde Windows Server dans Windows Server® 2012.
- implémenter la récupération de données et de serveurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble de la récupération d'urgence

La récupération d'urgence est une méthodologie qui décrit les étapes nécessaires à la résolution d'un incident une fois qu'il s'est produit, pour faire en sorte que les données, les services et les serveurs soient de nouveau opérationnels. Un plan de récupération d'urgence efficace satisfait les besoins de l'organisation sans fournir un niveau de couverture inutile. Bien que la protection absolue peut paraître souhaitable, il est peu probable qu'elle soit économiquement viable. En créant un plan de récupération d'urgence, vous devez équilibrer le coût à l'organisation d'un incident particulier, avec le coût à l'organisation de la protection de cet incident.

Objectifs de la leçon

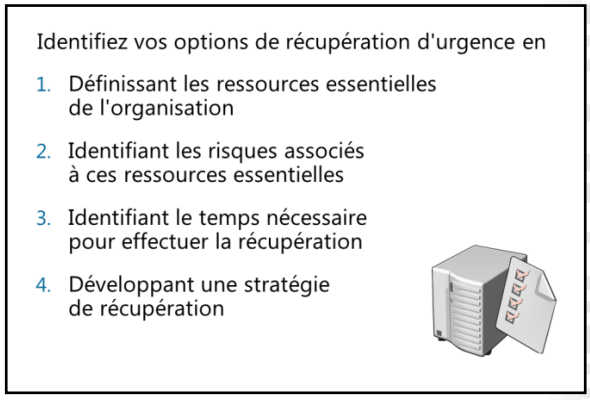
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Identifier les configurations requises de récupération d'urgence.
- Décrire les contrats de niveau de service.
- Décrire les stratégies de récupération d'urgence d'entreprise.
- Décrire les stratégies d'atténuation des risques d'incident.
- décrire les meilleures pratiques pour implémenter une récupération d'urgence.

Identification des configurations requises pour la récupération d'urgence

Avant de développer une stratégie de récupération d'urgence, les organisations doivent identifier leurs propres besoins en matière de récupération afin de garantir la protection des ressources essentielles la plus appropriée.

Voici une liste d'étapes de haut niveau permettant d'identifier les configurations requises pour une récupération d'urgence :



1. Définissez les ressources essentielles de l'organisation. Ces ressources comprennent les données, les services et les serveurs sur lesquels les données et les services s'exécutent.
2. Identifiez les risques associés à ces ressources essentielles. Par exemple, des données peuvent être supprimées par erreur ou intentionnellement et un disque dur ou un contrôleur de stockage où les données sont enregistrées peut être défaillant. En outre, les services qui utilisent les données essentielles peuvent ne pas fonctionner pour de nombreuses raisons (comme un problème réseau), et les serveurs peuvent ne pas répondre en raison de défaillances matérielles. D'importantes coupures électriques peuvent également causer le blocage de sites entiers.

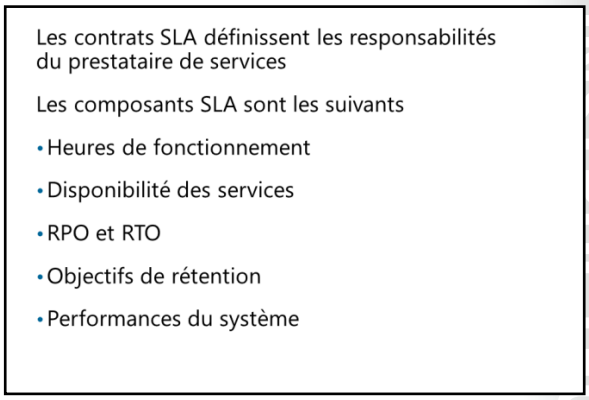
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Identifiez le temps nécessaire pour exécuter la récupération. En fonction de leurs exigences stratégiques, les organisations doivent déterminer la durée acceptable pour récupérer les ressources essentielles. Les scénarios peuvent varier de minutes en heures, voire même en jour.
4. Développez une stratégie de récupération. Selon les étapes précédentes, les organisations définiront un contrat de niveau de service qui contiendra des informations, telles que le niveau de disponibilité et les horaires des services. Les organisations doivent développer une stratégie de récupération d'urgence qui leur permet de réduire les risques, et parallèlement, de récupérer leurs ressources essentielles en un temps minimum acceptable pour leurs exigences stratégiques.

Remarque : L'organisation aura des configurations requises différentes de récupération d'urgence selon ses exigences et objectifs professionnels. Les configurations requises de récupération d'urgence ne doivent pas être statiques, mais elles doivent être évaluées et mises à jour régulièrement ; par exemple, une fois tous les x mois. Il est également important que les administrateurs testent régulièrement les stratégies de récupération d'urgence. Le test doit être réalisé dans un environnement de non-production isolé, à l'aide d'une copie des données de production.

Que sont les contrats de niveau de service ?

Un *contrat de niveau de service* (contrat SLA, Service Level Agreement) est un document qui décrit les responsabilités du service informatique ou du prestataire de services informatiques par rapport à un ensemble d'objectifs spécifiques. En<termes de contrats SLA de protection des données, généralement ces accords spécifient précisément les parties de l'infrastructure informatique et les données faisant l'objet de la protection, ainsi que le délai d'intervention en cas de défaillance.



Dans certaines organisations, les contrats SLA sont formalisés et les performances du service informatique sont mesurées par rapport aux objectifs qui sont<définis dans le contrat SLA. Ces mesures font partie de l'évaluation des performances du service informatique et ont une influence directe sur des éléments, tels que les budgets et les salaires. Pour les services gérés ou les fournisseurs de cloud, les contrats SLA sont essentiels pour la facturation. Dans d'autres organisations, les contrats SLA correspondent à des directives et sont moins formalisés. Il est important de concevoir un contrat SLA qui soit réaliste et réalisable, plutôt que d'en faire une simple norme irréaliste et irréalisable.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Certains des éléments du contrat SLA sont les suivants :

- Heures de fonctionnement. *Heures de fonctionnement* définit le nombre d'heures durant lesquelles les<données et les services sont disponibles aux utilisateurs, ainsi que le temps d'interruption planifié en cas de maintenance du système.
- Disponibilité des services. *Disponibilité des services* est défini sous forme d'un pourcentage de temps annuel durant lequel les données et les services seront à la disposition des utilisateurs. Par exemple, une disponibilité des services de 99,9 % par an signifie que les données et les services auront un temps d'interruption non planifié inférieur à 0,1 % par an, ou 8,75 heures par an 24 heures sur 24 et 7 jours sur 7.
- Objectif de point de récupération (RPO, Recovery point objective). Un objectif *RPO* fixe une limite à la quantité de données pouvant être perdues en cas de défaillance, mesurée en tant qu'unité de temps. Par exemple, si une organisation définit un RPO de six heures, il faudrait effectuer une sauvegarde toutes les six heures ou créer une copie de réplication à différents emplacements à des intervalles de six heures. En cas d'une défaillance, il serait nécessaire de revenir à la sauvegarde la plus récente, qui, dans le pire des cas s'il est supposé que la défaillance s'est produite juste avant (ou pendant) la sauvegarde suivante, remonterait à six heures.

  Vous pouvez configurer le logiciel de sauvegarde pour effectuer des sauvegardes toutes les heures, offrant un RPO théorique de 60 minutes. En calculant le RPO, il est également important de prendre en considération le temps d'exécution de la sauvegarde. Par exemple, supposez que cela prend 15 minutes d'effectuer une sauvegarde et que la sauvegarde est réalisée toutes les heures. Si une défaillance se produit pendant le processus de sauvegarde, votre meilleur RPO sera de 1 heure et 15 minutes. Un RPO réaliste doit toujours équilibrer le temps de récupération désiré avec les réalités de l'infrastructure réseau. Vous ne devez pas viser un objectif RPO de deux heures si la sauvegarde elle-même dure trois heures.

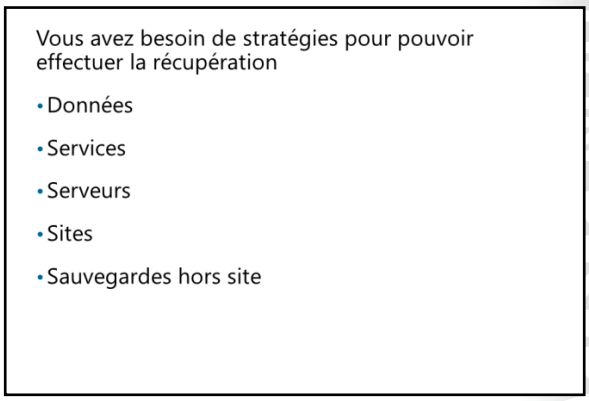
  Le RPO dépend également de la technologie logicielle de sauvegarde. Par exemple, si vous utilisez la fonctionnalité de capture instantanée dans la Sauvegarde Windows Server, ou si vous utilisez un autre logiciel de sauvegarde qui utilise le service VSS (Volume Shadow Copy Service), vous effectuez une sauvegarde à l'instant où la sauvegarde a été lancée.
- Objectif de temps de récupération (RTO, Recovery time objective). Un objectif *RTO* détermine la durée de récupération nécessaire après une panne. Les RTO varient en fonction du type de défaillance. La perte d'une carte mère sur un serveur critique aura un RTO différent de la perte d'un disque sur un serveur critique, parce qu'un de ces composants demande sensiblement plus de temps pour être remplacé.
- Objectifs de rétention. La *Rétention* est une mesure de la durée nécessaire pour le stockage des données sauvegardées. Par exemple, vous pouvez avoir besoin de récupérer des données antérieures à un mois pour en enregistrer certaines durant plusieurs années. La vitesse à laquelle vous acceptez de récupérer les données dans votre contrat SLA dépendra de l'âge des données, avec certaines données étant rapidement récupérables et d'autres devant être récupérées dans les archives.
- Performances du système. Bien que non directement liées à la récupération d'urgence, les performances du système sont également une composante importante des contrats SLA, car les applications qui sont incluses au contrat SLA doivent être disponibles et avoir des temps de réponse aux demandes des utilisateurs acceptables. Si les performances système sont lentes, alors les exigences stratégiques ne seront pas réunies.

 **Remarque :** Chaque contrat SLA de protection des données de l'organisation dépend des composants qui sont importants pour l'organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des stratégies de récupération d'urgence d'entreprise

Lors de la planification de la sauvegarde des données de votre entreprise, vous devez développer des stratégies pour récupérer les données, les services, les serveurs et les sites. Vous devez également prendre des dispositions pour la sauvegarde hors site.



Stratégies de récupération de données

Les données sont la catégorie généralement la plus récupérée dans un environnement d'entreprise. En effet, il est plus probable que les utilisateurs suppriment des fichiers par erreur, que le matériel serveur échoue ou que les applications provoquent la corruption des données. Par conséquent, en développant une stratégie de récupération d'urgence d'entreprise, prenez en considération les petits incidents, tels que la suppression de données, en plus de grands incidents, tels que la défaillance de site ou de serveur.

En considérant les stratégies de récupération de données, la sauvegarde n'est pas la seule technologie de récupération de données. Vous pouvez adresser de nombreux scénarios de récupération de fichiers et dossiers en implémentant les versions précédentes de la fonctionnalité de fichier sur les partages de fichiers. Vous pouvez également répliquer des données dans différents emplacements physiques, ou sur un cloud public ou privé.

Stratégies de récupération de services

La fonctionnalité du réseau dépend de la disponibilité de certains services réseau critiques. Bien que les réseaux bien conçus établissent la redondance dans des services de noyau tels que les services DNS (Domain Name System) et AD DS (Active Directory® Domain Services), même ces services pourraient rencontrer des problèmes, comme lors la réplication d'un défaut important qui requiert une restauration à partir d'une sauvegarde. En outre, une solution de sauvegarde d'entreprise doit vérifier que des services tels que le protocole DHCP (Dynamic Host Configuration Protocol) et AD CS, ainsi que les ressources importantes telles que les partages de fichiers, peuvent être restaurés et actualisés dans les temps.

Stratégies de récupération de serveur complète

Développer une stratégie de récupération de serveur complète implique que vous déterminiez les serveurs concernés par la récupération, ainsi que le RPO et le RTO pour les serveurs critiques. Supposez que vous disposez d'un site avec deux ordinateurs fonctionnant comme contrôleurs de domaine. Lors du développement de votre stratégie de sauvegarde, devez-vous envisager d'avoir deux serveurs capables d'effectuer une récupération de serveur complète avec un RPO de 15 minutes ? Ou est-il seulement nécessaire pour un serveur d'être récupéré rapidement en cas d'échec, vu que l'un ou l'autre des serveurs pourra fournir le même service réseau et assurer la poursuite de l'activité ?

En développant le composant de récupération de serveur complète du plan de sauvegarde de l'entreprise de votre organisation, déterminez quels serveurs sont requis pour garantir la poursuite de l'activité, ainsi que leur sauvegarde régulière.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégies de récupération de site

La plupart des plus grandes organisations ont des filiales. Bien qu'il pourrait être souhaitable de sauvegarder tous les ordinateurs à ces emplacements, il peut ne pas être économiquement possible de procéder de la sorte. Développer une stratégie de récupération de site implique de déterminer les données, les services et les serveurs sur un site spécifique devant être récupérables pour garantir la poursuite de l'activité.

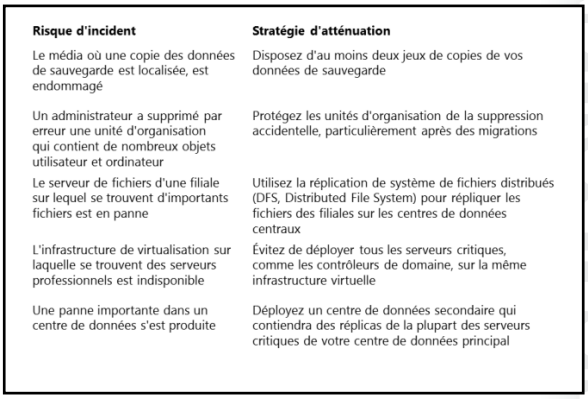
Stratégies de sauvegarde hors site

De nombreuses organisations qui ne stockent pas les sauvegardes hors site, n'effectuent pas de récupération suite à un sinistre sur le site principal. Si le site du siège social de votre organisation subit un incendie ou la catastrophe du siècle, tremblement de terre ou tornade, peu importe les stratégies de sauvegarde mises en place si toutes les sauvegardes sont stockées à l'emplacement qui a été détruit par la catastrophe.

Une stratégie de protection des données complètes de l'entreprise implique le déplacement des données sauvegardées vers un emplacement hors site sécurisé de sorte que vous puissiez les récupérer, quel que soit le sinistre qui se produit. Cette opération n'a pas besoin de se produire chaque jour. Le RPO pour la récupération sur l'emplacement hors site—est souvent appelé *site de récupération d'urgence*—est habituellement différent du RPO au niveau du site principal.

Stratégies d'atténuation des risques d'incident

Peu importe comment les organisations sont préparées, elles ne peuvent pas empêcher des incidents de se produire. Par conséquent, les organisations doivent également développer des stratégies d'atténuation des risques qui réduiront l'incidence d'une perte inattendue de données, de serveur, de services ou de sites. Pour préparer des stratégies d'atténuation des risques, les organisations doivent créer des évaluations des risques qui analysent tous les scénarios d'incidents possibles, ainsi que le document indiquant comment atténuer chacun de ces scénarios.



Risque d'incident	Stratégie d'atténuation
Le média où une copie des données de sauvegarde est localisée, est endommagé	Disposez d'au moins deux jeux de copies de vos données de sauvegarde
Un administrateur a supprimé par erreur une unité d'organisation qui contient de nombreux objets utilisateur et ordinateur	Protégez les unités d'organisation de la suppression accidentelle, particulièrement après des migrations
Le serveur de fichiers d'une filiale sur lequel se trouvent d'importants fichiers est en panne	Utilisez la réplication de système de fichiers distribués (DFS, Distributed File System) pour répliquer les fichiers des filiales sur les centres de données centraux
L'infrastructure de virtualisation sur laquelle se trouvent des serveurs professionnels est indisponible	Évitez de déployer tous les serveurs critiques, comme les contrôleurs de domaine, sur la même infrastructure virtuelle
Une panne importante dans un centre de données s'est produite	Déployez un centre de données secondaire qui contiendra des réplicas de la plupart des serveurs critiques de votre centre de données principal

Le tableau suivant présente certains des risques associés à la perte de données ou de services, ainsi que les stratégies d'atténuation des risques appropriées.

Risque d'incident	Stratégie d'atténuation
Le média où une copie des données de sauvegarde est localisée est endommagé.	Disposez d'au moins deux copies de vos données de sauvegardes et validez vos sauvegardes régulièrement.
Un administrateur a supprimé par erreur une unité d'organisation (OU, Organizational Unit) qui contient de nombreux objets utilisateur et ordinateur.	Protégez les unités d'organisation de la suppression accidentelle, particulièrement après des migrations.

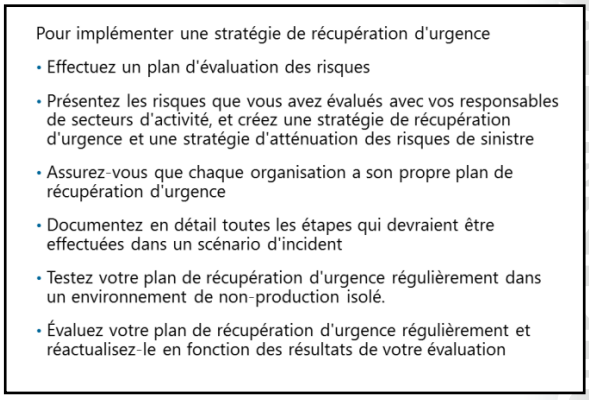
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Risque d'incident	Stratégie d'atténuation
Le serveur de fichiers d'une filiale sur lequel se trouvent d'importants fichiers est en panne.	Utilisez la réplication de système de fichiers distribués (DFS, Distributed File System) pour répliquer les fichiers des filiales sur les centres de données centraux.
L'infrastructure de virtualisation sur laquelle se trouvent des serveurs professionnels est indisponible.	Évitez de déployer tous les serveurs critiques, comme les contrôleurs de domaine, sur la même infrastructure virtuelle.
Une panne importante dans un centre de données s'est produite.	Déployez un centre de données secondaire qui contiendra des réplicas des serveurs critiques de votre centre de données principal.

Meilleures pratiques pour implémenter une récupération d'urgence

En implémentant une stratégie de récupération d'urgence, les organisations doivent suivre ces recommandations :



- Effectuez un plan d'évaluation des risques. Il vous aidera à identifier tous les risques associés à la disponibilité de vos données, serveurs, services et sites d'organisation.
- Discutez des risques que vous avez évalués avec les responsables de secteurs d'activité. Déterminez ensemble quelles sont les ressources devant être protégées par le plan de récupération d'urgence, et quelles sont les ressources devant être protégées par l'atténuation des risques d'incident, et à quel niveau. Plus les configurations requises pour la récupération d'urgence sont élevées, plus elles seront coûteuses. Vous souhaitez également avoir un plan de récupération d'urgence de bas niveau pour les ressources qui sont protégées par l'atténuation des risques d'incident.
- Assurez-vous que chaque organisation a son propre plan de récupération d'urgence.
- Documentez en détail toutes les étapes qui devraient être effectuées dans un scénario d'incident.
- Testez votre plan de récupération d'urgence régulièrement dans un environnement de non-production isolé.
- Évaluez votre plan de récupération d'urgence régulièrement et réactualisez-le en fonction de votre évaluation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Implémentation de la Sauvegarde Windows Server

Pour protéger des données essentielles, chaque organisation doit effectuer des sauvegardes régulières. Disposer d'une stratégie de sauvegarde bien définie et testée permet aux entreprises de s'assurer qu'elles peuvent restaurer des données en cas de défaillance ou de perte inattendue. Cette leçon décrit la fonctionnalité Sauvegarde Windows Server dans Windows Server 2012 et Windows Azure Online Backup™ pour Windows Server 2012.

Objectifs de la leçon

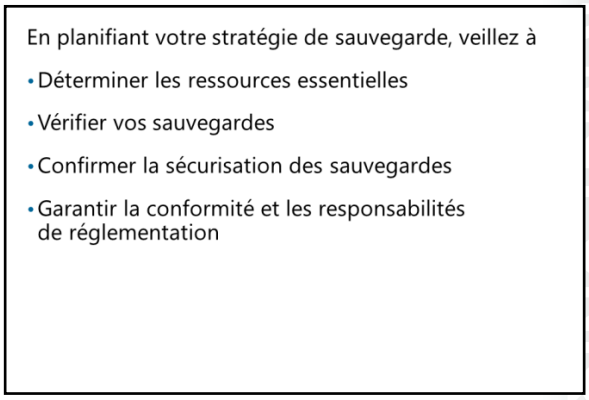
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les informations sur les services et les données devant être sauvegardées dans un environnement Windows Server.
- Décrire les types de sauvegarde.
- Décrire les technologies de sauvegarde.
- Expliquer comment planifier la capacité de la sauvegarde.
- Expliquer comment planifier la sécurité de la sauvegarde.
- Décrire la fonctionnalité Sauvegarde Windows Server.
- Expliquer comment configurer une sauvegarde planifiée à l'aide de la fonctionnalité Sauvegarde Windows Server.
- Décrire Windows Azure Online Backup.
- Décrire les éléments à prendre en considération pour une solution de sauvegarde d'entreprise.
- Résumer les fonctionnalités disponibles avec Microsoft® System Center 2012 – Data Protection Manager.

Qu'est-ce qui doit être sauvegardé ?

Pour avoir l'assurance de protéger les ressources de votre organisation qui sont considérées comme essentielles, votre planification doit prendre en compte les éléments suivants :

- Ressources essentielles
- Vérification des sauvegardes
- Sécurité des sauvegardes
- Conformité et exigences réglementaires



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Détermination des ressources essentielles à sauvegarder

Dans un scénario idéal, vous sauvegarderiez tout et restaureriez les données instantanément à un point donné à un moment particulier au cours des dernières années. En réalité, une telle stratégie de sauvegarde générerait un coût de possession élevé. Par conséquent, la première étape de la planification du processus de sauvegarde au sein de l'entreprise est de déterminer ce qui mérite réellement d'être sauvegardé.

Par exemple, devriez-vous sauvegarder chaque contrôleur de domaine au sein du domaine, vu que les informations Active Directory seront répliquées de nouveau sur un contrôleur de domaine de rechange suite au changement ? Est-il nécessaire de sauvegarder chaque serveur de fichiers sur tous les partages de fichiers si chaque fichier est répliqué sur plusieurs serveurs par un système de fichiers distribués ?

Vous devez également distinguer les raisons techniques et les raisons de réglementation liées à la sauvegarde des données. En raison des obligations légales, vous pouvez devoir fournir à votre société des données vitales pour l'entreprise relatives aux dix dernières années, voire même plus.

Pour déterminer ce qui doit être sauvegardé, considérez ce qui suit :

- Si les données ne sont stockées qu'à un emplacement, assurez-vous qu'elles sont sauvegardées.
- Si les données sont répliquées, il n'est peut être pas nécessaire de sauvegarder chaque réplica. Cependant, vous devez sauvegarder au moins un emplacement pour vérifier que la sauvegarde peut être restaurée.
- Le serveur ou les données sont-ils des composants essentiels ?
- En cas d'échec du serveur ou du disque, ou en cas de corruption des données, quelles mesures devraient être prises pour les récupérer ?

Beaucoup d'organisations vérifient la disponibilité des services et des données essentielles par la redondance. Par exemple, Microsoft Exchange Server 2010 fournit la réplication continue des bases de données de boîtes aux lettres sur d'autres serveurs à l'aide d'une technologie appelée Groupes de disponibilité de la base de données (DAG, Database Availability Groups). Bien que les DAG ne signifient pas qu'une organisation ne devrait pas sauvegarder ses serveurs de boîtes aux lettres Exchange Server 2010, cela change la manière dont une organisation devrait penser à sauvegarder ses serveurs de boîtes aux lettres ou à centraliser ses stratégies de sauvegarde.

Vérification de vos sauvegardes

L'exécution d'une sauvegarde et la garantie que la sauvegarde contient tout ce dont vous avez besoin, sont deux tâches différentes. Vous devez disposer d'une méthode qui vous permet de vérifier que chaque sauvegarde s'est achevée avec succès. Vous devez également savoir quand les sauvegardes ont échoué. Au minimum, ceci signifie que vous devez vérifier les journaux de chaque serveur pour déterminer si une défaillance s'est produite. Si vous avez configuré des sauvegardes sur chaque serveur toutes les six heures, combien de fois devriez-vous vérifier les journaux ? Une meilleure solution serait d'utiliser un mécanisme permettant de vous prévenir de l'échec d'une sauvegarde, ce qui est possible dans System Center 2012 - Operations Manager. Il faut éviter de découvrir que les sauvegardes d'un serveur particulier a échoué au moment même où vous avez besoin de ces sauvegardes pour exécuter une récupération.

Une manière de vérifier les sauvegardes consiste à effectuer un test régulier des procédures de récupération, dans lesquelles vous simulez une défaillance particulière. Ceci vous permet de vérifier l'intégrité des données que vous utilisez pour effectuer une récupération, et que les procédures de récupération que vous avez mises en place résolvent la défaillance efficacement. Il vaut mieux découvrir que vous devez ajouter des étapes à votre procédure de récupération lors d'un test, plutôt que lors d'une défaillance réelle.

Confirmation de la sécurisation des sauvegardes

Par définition, un bon jeu de sauvegardes contient toutes les données essentielles de votre organisation. Ces données doivent être protégées contre tout accès non autorisé. Bien que des données pourraient être protégées par des autorisations et des contrôles d'accès alors qu'elles sont hébergées sur des serveurs dans un environnement de production, n'importe quel utilisateur ayant accès au média qui héberge ces données de sauvegarde, peut les restaurer. Par exemple, certains produits, tels que la Sauvegarde Windows Server, ne permettent pas aux administrateurs de chiffrer les données de sauvegarde. Cela signifie que la sécurité physique est la seule manière de s'assurer que ces données essentielles ne terminent pas dans les mains d'utilisateurs non autorisés.

En développant une stratégie de sauvegarde d'entreprise, assurez-vous que les données de sauvegarde sont enregistrées à un emplacement sécurisé.

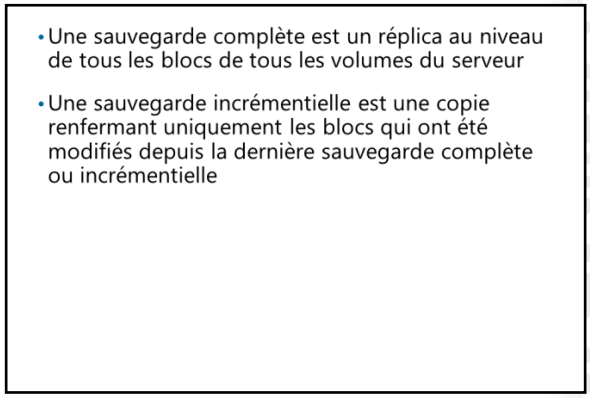
Vous pourriez également considérer le logiciel d'utilisation de la sauvegarde qui vous permet de fractionner les rôles de sauvegarde et de restauration de sorte que les utilisateurs qui ont des autorisations pour sauvegarder les données ne disposent pas des autorisations pour restaurer ces données ; et inversement les utilisateurs qui disposent des autorisations pour restaurer les données, n'aient pas les autorisations pour les sauvegarder.

Conformité et responsabilités de réglementation

Les administrateurs système doivent être bien conscients des réglementations et des responsabilités de conformité de l'organisation en vigueur en matière d'archivage des données. Par exemple, certaines juridictions requièrent que les données des messages électroniques relatives à l'entreprise soient conservées durant une période allant jusqu'à sept ans. Malheureusement, les exigences réglementaires varient d'un pays à l'autre, et même d'une région à une autre. En développant la stratégie de protection des données de votre organisation, vous devez prévoir une réunion avec l'équipe juridique de votre organisation pour déterminer avec précision quelles sont les données devant être enregistrés, et pendant combien de temps.

Types de sauvegardes

Dans Windows Server 2012, vous pouvez effectuer les types de sauvegarde suivants :



- Sauvegarde complète. Une sauvegarde complète est un réplica au niveau de tous les blocs de tous les volumes du serveur. Plutôt que de copier des fichiers et dossiers sur le média de sauvegarde, les blocs sous-jacents sont copiés sur le média de sauvegarde.
- Sauvegardes incrémentielles. Une sauvegarde incrémentielle est une copie renfermant uniquement les blocs qui ont été modifiés depuis la dernière sauvegarde complète ou incrémentielle. Pendant une sauvegarde incrémentielle, ces blocs sont copiés sur le média de sauvegarde. Lorsque ce processus s'achève, les blocs sont alors marqués comme sauvegardés. Pendant la récupération, l'ensemble de blocs d'origine est restauré. Puis, chaque ensemble de blocs incrémentiels sont appliqués, remettant les données récupérées à l'état approprié d'une façon cohérente.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Technologies de sauvegarde

- La technologie de sauvegarde VSS résout des problèmes de cohérence de données en créant des clichés instantanés
- Vous pouvez également utiliser les sauvegardes en continu pour les applications plus anciennes ne prenant pas en charge VSS

La plupart des produits de sauvegarde utilisent de nos jours l'infrastructure VSS qui est présente dans Windows Server 2012. Quelques applications plus anciennes, cependant, utilisent la sauvegarde en continu. Il peut être nécessaire de prendre en charge ces applications plus anciennes, dans des environnements complexes et hétérogènes.

L'une des difficultés d'effectuer des sauvegardes est d'assurer la cohérence des données que vous sauvegardez. Les sauvegardes ne se produisent pas immédiatement ; elles peuvent durer des secondes, des minutes ou des heures. Malheureusement, les serveurs ne sont pas statiques et l'état d'un serveur au début d'une sauvegarde ne peut pas être le même à la fin de celle-ci. Si vous ne tenez pas compte de la cohérence, cela peut poser des problèmes pendant la restauration parce que la configuration du serveur peut avoir changé lors de la sauvegarde.

VSS

La technologie VSS (que Microsoft a inclus dans Windows Server 2003 R2 et qui est présente dans tous les systèmes d'exploitation de serveurs récents résout le problème de cohérence au niveau des blocs de disque en créant ce que l'on appelle un cliché instantané. Un *cliché instantané* est une collection de blocs sur un volume qui est figé à un moment spécifique. Des modifications peuvent encore être apportées au disque, mais lorsqu'une sauvegarde se produit, la collection de blocs figés est sauvegardée, ce qui signifie que toutes les modifications qui pourraient s'être produites depuis le figeage ne sont pas sauvegardées.

La création d'un cliché instantané indique au système d'exploitation de placer d'abord tous les fichiers, tels que les fichiers de base de données DHCP et de base de données Active Directory, à un état cohérent pendant un instant. Ensuite, l'état actuel du système de fichiers est enregistré à ce moment spécifique. Après que VSS ait créé le cliché instantané, tous les accès en écriture qui remplaceraient des données, enregistrent au préalable les blocs de données précédents. Par conséquent, un cliché instantané est petit au début et il se développe au cours du temps lorsque les données changent. Par défaut, le système d'exploitation est configuré pour réserver 12 % du volume aux données VSS et VSS supprime automatiquement les captures instantanées antérieures lorsque cette limite est atteinte. Vous pouvez modifier cette valeur par défaut, tout comme l'emplacement par défaut des données VSS. Cela garantit que la sauvegarde a une capture instantanée du système à un état cohérent, peut importe la durée d'écriture des données de sauvegarde sur le périphérique de stockage de sauvegarde.

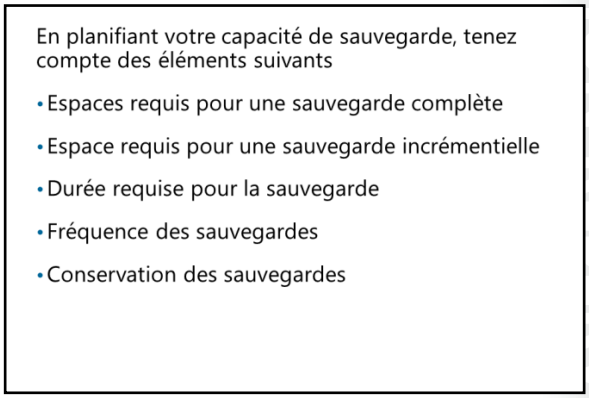
Sauvegarde en continu

La sauvegarde en continu est souvent utilisée par les applications antérieures qui n'utilisent pas la technologie VSS. Les applications qui ne prennent pas en charge la technologie VSS sont sauvegardées à l'aide d'une méthode appelée *sauvegarde en continu* Contrairement à la technologie VSS où le système d'exploitation garantit la conservation des données dans un état cohérent et à un moment actuel, lorsque vous utilisez la sauvegarde en continu, l'application ou l'application de protection des données doit garantir que les données demeurent dans un état cohérent. En outre, après la sauvegarde en continu, certains fichiers retrouvent leur état avant le début de la sauvegarde, alors que d'autres fichiers adoptent l'état de la fin de la fenêtre de sauvegarde.

Planification de la capacité de sauvegarde

Si vous développez une stratégie de récupération d'entreprise, vous devez déterminer la capacité de stockage dont votre organisation a besoin pour effectuer les sauvegardes. Les facteurs suivants affectent la quantité d'espace qui est requise pour enregistrer des données de sauvegarde :

- Espaces requis pour une sauvegarde complète
- Espace requis pour une sauvegarde incrémentielle
- Durée requise pour la sauvegarde
- Fréquence des sauvegardes
- Conservation des sauvegardes



Conditions requises pour la sauvegarde complète

Pour calculer l'espace requis pour une sauvegarde complète, déterminez l'espace contenu sur tous les volumes que vous devrez sauvegarder. Si le serveur a un lecteur dédié aux sauvegardes, vous n'effectuerez pas de sauvegarde sur ce lecteur.

Pour les produits qui effectuent des sauvegardes basées sur une image, telles que la Sauvegarde Windows Server, ces données ne sont pas compressées. Sur certains types de serveurs, notamment les serveurs de fichiers, la quantité d'espace requise pour une sauvegarde complète se développe au fil du temps. Vous pouvez réduire cette tendance à l'aide des stratégies d'expiration de fichiers, comme celles disponibles dans le Gestionnaire de ressources du serveur de fichiers (FSRM, File Server Resource Manager).

Conditions requises pour une sauvegarde incrémentielle

Une sauvegarde incrémentielle sur la Sauvegarde Windows Server enregistre tous les blocs de disque dur qui ont changé depuis la dernière sauvegarde complète ou incrémentielle. Les sauvegardes incrémentielles sont sensiblement plus rapides que les sauvegardes complètes et requièrent moins d'espace. L'inconvénient des sauvegardes incrémentielles est qu'elles peuvent avoir besoin d'un temps de récupération supérieur.

Durée requise pour la sauvegarde

La durée requise pour écrire les données du serveur en cours de sauvegarde sur le périphérique de stockage de sauvegarde, peut avoir une incidence sur le RPO projeté, car il n'est pas recommandé de commencer une nouvelle opération de sauvegarde avant l'achèvement de la sauvegarde en cours.

Fréquence des sauvegardes

La *fréquence de sauvegarde* est une mesure du nombre de fois où des sauvegardes sont effectuées. Avec les sauvegardes de blocs incrémentielles, il n'y a aucune différence substantielle entre la quantité de données écrites sur la somme de quatre sessions de 30 minutes et une session incrémentielle de deux heures sur le même serveur. C'est parce qu'au cours des deux heures, le même nombre de blocs aura changé sur le serveur par rapport aux quatre sessions de 30 minutes. Cependant, les quatre sessions de 30 minutes les ont fractionné en parties inférieures. Si les sauvegardes se produisent plus fréquemment, elles réduisent le temps requis pour effectuer la sauvegarde en la fractionnant en parties inférieures. Le total global sera à peu près identique.

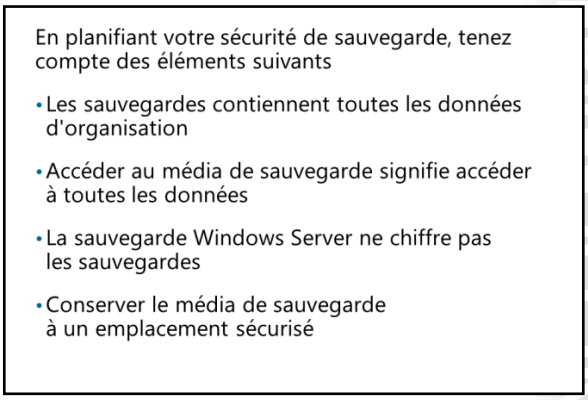
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conservation des sauvegardes

En tentant de déterminer la capacité de sauvegarde requise, vous devez déterminer avec précision combien de temps vous devez conserver les données de sauvegarde. Par exemple, si vous devez effectuer une récupération à n'importe quel point de sauvegarde au cours des 28 derniers jours, et si vous disposez de points de récupération générés à chaque heure, vous aurez besoin de plus d'espace que si vous aviez des points de récupération générés une fois par jour, alors que vous devez restaurer uniquement les données des 14 derniers jours.

Planification de la sécurité de sauvegarde

En planifiant votre sécurité de sauvegarde, tenez compte des éléments suivants :

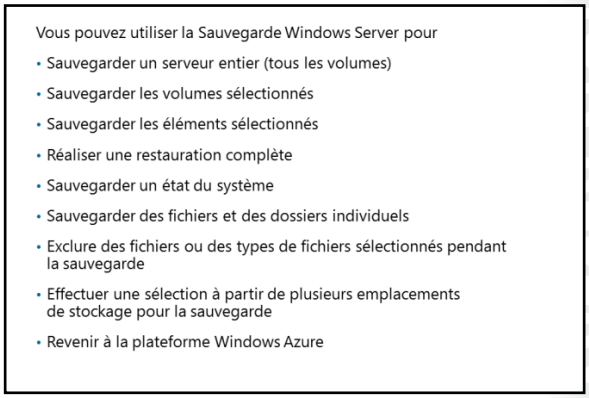


- Les sauvegardes contiennent toutes les données d'organisation. Par nature, les sauvegardes contiendront toutes les données nécessaires pour garantir la capacité continue de votre organisation à fonctionner en cas de défaillance. Puisque ces données sont susceptibles de renfermer des informations confidentielles, vous devriez les protéger avec le même niveau de vigilance avec lequel elles sont protégées une fois hébergées sur le serveur.
- Accédez au média de sauvegarde signifie accéder à toutes les données. Si possible, utilisez la séparation des rôles d'administration pour vous assurer que les utilisateurs qui sauvegardent les données ne sont pas les utilisateurs qui peuvent les restaurer. Dans les environnements de niveau de sécurité élevé, assurez-vous que les opérations de sauvegarde et de restauration sont correctement auditées de sorte que vous puissiez suivre les sauvegardes et restaurer l'activité fonctionnelle.
- La sauvegarde Windows Server ne chiffre pas les sauvegardes. La sauvegarde Windows Server écrit des sauvegardes au format VHD. Cela signifie que n'importe quel utilisateur ayant accès à Windows 8® ou à Windows Server 2012 peut monter ces sauvegardes en volumes, puis en extraire les données. Une attaque encore plus sophistiquée pourrait inclure le démarrage du disque dur virtuel de sauvegarde pour personnifier le système sauvegardé sur le réseau d'organisation.
- Conservez le média de sauvegarde à un emplacement sécurisé. Au minimum, les sauvegardes doivent être conservées enfermées en lieu sûr. Si votre organisation effectue des sauvegardes sur des lecteurs de disques qui sont reliés aux serveurs par câble USB, assurez-vous que ces lecteurs de disques sont verrouillés sur place, même si ils sont situés dans une salle de serveurs sécurisée, et même si la salle des serveurs de votre organisation dispose d'une caméra de surveillance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que l'utilitaire Sauvegarde Windows Server ?

La fonctionnalité Sauvegarde Windows Server dans Windows Server 2012 se compose d'un composant logiciel enfichable Microsoft Management Console (MMC), de la commande wbadmin et des commandes Windows PowerShell®. Vous pouvez utiliser des assistants dans la fonctionnalité Sauvegarde Windows Server pour vous guider dans l'exécution de sauvegardes et de restaurations.



Vous pouvez utiliser la Sauvegarde Windows Server pour sauvegarder :

- un serveur entier (tous les volumes).
- Volumes sélectionnés.
- Sélectionnez les éléments spécifiques pour la sauvegarde, telle que des dossiers spécifiques ou l'état du système.

En outre, la Sauvegarde Windows Server 2012 vous permet d'effectuer les opérations suivantes :

- Réaliser une restauration complète. Une sauvegarde complète contient au moins tous les volumes critiques, et vous permet d'effectuer une restauration sans devoir installer au préalable un système d'exploitation. Pour cela, utilisez le média de produit sur un DVD ou une clé USB et l'Environnement de récupération Windows (Windows RE, Windows Recovery Environment). Vous pouvez utiliser ce type de sauvegarde, ainsi que Windows RE, pour récupérer d'une défaillance de disque dur, ou si vous devez récupérer l'image entière d'un ordinateur sur un nouveau matériel.
- Utiliser l'état du système. La sauvegarde contient toutes les informations pour restaurer un serveur à un moment spécifique. Cependant, il est nécessaire qu'un système d'exploitation soit installé avant de récupérer l'état du système.
- Récupérer chaque fichier, dossier ou volume. L'option **Chaque fichier et dossier** vous permet de choisir de sauvegarder et de restaurer des fichiers, des dossiers ou des volumes spécifiques, ou encore d'ajouter des fichiers, des dossiers ou des volumes spécifiques à la sauvegarde lorsque vous utilisez une option telle que le volume critique ou l'état du système.
- Exclure des fichiers ou des types de fichiers sélectionnés. Par exemple, vous pouvez exclure des fichiers temporaires de la sauvegarde.
- Sélectionner à partir de plusieurs emplacements de stockage. Il est possible de stocker des sauvegardes sur des volumes distants partagés ou non dédiés.
- Utiliser Windows Azure Online Backup. Windows Azure Online Backup est une solution de sauvegarde basée sur le cloud pour Windows Server 2012 qui permet la sauvegarde et la récupération de fichiers et dossiers à partir du cloud public ou privé pour permettre la sauvegarde hors site.

Si des incidents tels que des défaillances de disque dur se produisent, vous pouvez effectuer la restauration du système à l'aide d'une sauvegarde de serveur complète et de Windows RE ; ceci restaurera votre système entier sur le nouveau disque dur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration d'une sauvegarde planifiée

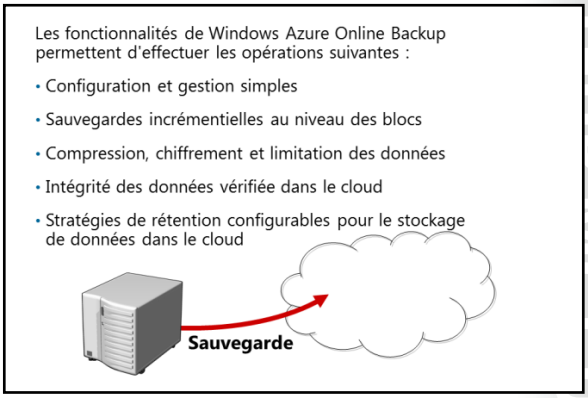
Dans cette démonstration, vous allez apprendre à configurer Windows Server 2012 pour effectuer une sauvegarde planifiée de dossiers spécifiques qui comprend un filtre permettant d'exclure d'autres types de fichiers spécifiques.

Procédure de démonstration

1. Sur LON-SVR1, démarrez la fonctionnalité **Sauvegarde Windows Server**.
2. Configurez la planification de sauvegarde avec les options suivantes :
   - Configuration de la sauvegarde : **Personnalisée**
   - Sélectionner les éléments à sauvegarder : **C:\HR Data**
   - Ajouter une exclusion : **C:\HR Data\Old HR file.txt**
   - Heure de la sauvegarde : **Une fois par jour, à 01:00**
   - Type de destination : **Sauvegarder dans un dossier réseau partagé**
   - Dossier partagé distant : **\\LON-DC1\Sauvegarde**:
     - Enregistrer la planification de sauvegarde : Nom d'utilisateur : **Administrateur**
     - Mot de passe : **Pa$$w0rd**
3. Exécutez **l'Assistant Sauvegarde unique** à l'aide des options de sauvegarde planifiée.
4. Fermez l'utilitaire Sauvegarde Windows Server.

Qu'est-ce que Windows Azure Online Backup ?

Windows Azure Online Backup est une solution de sauvegarde dans le cloud pour Windows Server 2012 qui est gérée par Microsoft. Vous pouvez utiliser ce service d'abonnement pour assurer une protection hors site contre la perte de données provoquée par des incidents. Vous sauvegardez des fichiers et dossiers, et les récupérer alors du cloud public ou privé autant que nécessaire. Où que vous soyez, vous pouvez utiliser l'outil Windows Azure Online Backup pour sauvegarder et protéger les données essentielles.



Windows Azure Online Backup est basé sur la plate-forme Windows Azure et utilise le stockage BLOB de Windows Azure pour conserver les données client. Windows Server 2012 utilise l'agent Windows Azure Online Backup pour transférer des données de fichiers et dossiers de manière sécurisée vers Windows Azure Online Backup. Cet agent peut être téléchargé. Après que vous avez installé l'agent Windows Azure Online Backup, celui-ci intègre sa fonctionnalité par l'intermédiaire de l'interface de sauvegarde de Windows Server. Vous pouvez télécharger l'agent Windows Azure Online Backup du site Web de Microsoft.

Fonctionnalités clés

Les fonctionnalités clés que Windows Server 2012 offre par l'intermédiaire de Windows Azure Online Backup comprennent :

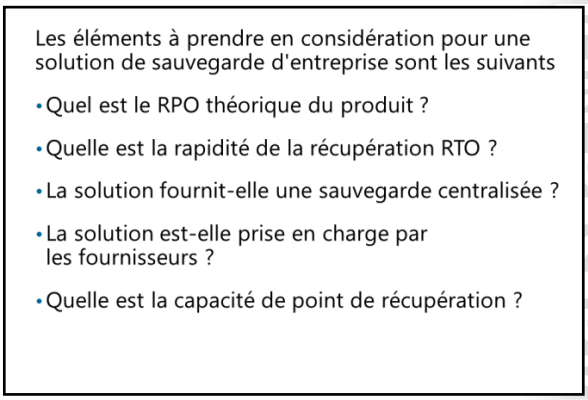
- Une configuration et une gestion simples. L'intégration à l'utilitaire Sauvegarde Windows Server fournit une expérience transparente de sauvegarde et restauration sur un disque local ou vers une plateforme en cloud. Voici d'autres fonctionnalités :
  - Une interface utilisateur simple pour configurer et surveiller les sauvegardes.
  - Une expérience de récupération intégrée pour récupérer des fichiers et dossiers à partir d'un disque local ou d'une plateforme en cloud.
  - Une faculté de récupération des données qui a été sauvegardée sur tous les serveurs de votre choix.
  - une fonction d'écriture de scripts qui est fournie par l'interface de ligne de commande Windows PowerShell.
- Des sauvegardes incrémentielles au niveau des blocs. L'agent Windows Azure Online Backup effectue des sauvegardes incrémentielles en suivant le fichier et les modifications au niveau des blocs, transférant seulement les blocs modifiés, réduisant de ce fait le stockage et l'utilisation de la bande passante. Les différentes versions des sauvegardes, enregistrées à des moments différents, utilisent le stockage de manière efficace en ne conservant que les blocs ayant été modifiés d'une version à l'autre.
- Compression, chiffrement et limitation des données. L'agent Windows Azure Online Backup vérifie que les données sont compressées et chiffrées sur le serveur avant qu'elles soient envoyées au service de Windows Azure Online Backup sur le réseau. Par conséquent, Windows Azure Online Backup stocke uniquement les données chiffrées dans le stockage dans le cloud. Windows Azure Online Backup ne dispose pas de la phrase secrète de chiffrement. Par conséquent, les données ne sont jamais chiffrées au niveau du cloud. De plus, les utilisateurs peuvent installer la limitation de requêtes et configurer la manière dont le service de Windows Azure Online Backup utilise la bande passante réseau en sauvegardant ou en restaurant les informations.
- L'intégrité des données vérifiée dans le cloud. En plus des sauvegardes sécurisées, l'intégrité des données sauvegardées est également automatiquement vérifiée à la fin de la sauvegarde. Par conséquent, toutes les corruptions qui peuvent surgir en raison du transfert de données peuvent être facilement identifiées. Ces corruptions sont résolues automatiquement lors de la sauvegarde suivante.
- Stratégies de rétention configurables pour le stockage de données dans le cloud. Windows Azure Online Backup accepte et implémente des stratégies de rétention pour recycler des sauvegardes qui dépassent la plage de rétention souhaitée, répondant ainsi aux stratégies de l'entreprise et permettant une gestion des coûts de sauvegarde.

 **Liens de référence :** Pour plus d'informations sur Windows Azure, consultez la page http://go.microsoft.com/fwlink/?LinkId=270041.

 **Remarque :** Pour l'instant, Windows Azure Online Backup n'est pas disponible dans tous les pays. Pour obtenir des informations mises à jour, consultez la page http://go.microsoft.com/fwlink/?LinkId=270042.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en considération pour une solution de sauvegarde d'entreprise



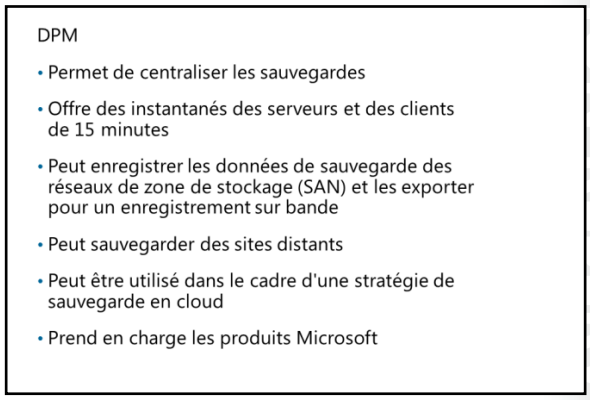
La sauvegarde Windows Server est une solution de sauvegarde de serveur unique. En planifiant la sauvegarde pour une entreprise, considérez les points suivants :

- Quantité maximale de données perdues. Quel est le RPO théorique du produit ? Les produits qui offrent la restauration la plus proche du point de défaillance sont susceptibles de coûter plus que les produits qui offrent des RPO de 15 ou 30 minutes. Vous devez déterminer les besoins de votre organisation. Votre organisation a-t-elle besoin de récupérer la dernière transaction SQL Server ou la fenêtre de récupération de 15 minutes est-elle un compromis acceptable ?
- Quelle est la rapidité de la récupération RTO ? Combien de temps est nécessaire entre la défaillance à la fonctionnalité restaurée ? Pouvoir effectuer une restauration à la dernière transaction SQL Server est la solution optimale, mais si l'opération nécessite deux jours pour atteindre ce point de récupération, la solution n'est peut-être pas aussi utile qu'elle puisse paraître.
- La solution fournit-elle une sauvegarde centralisée ? Le produit vous permet-il de centraliser votre solution de sauvegarde sur un serveur, ou les sauvegardes doivent-elles être effectuées directement sur chaque serveur de l'organisation ?
- La solution est-elle prise en charge par les fournisseurs ? Certains fournisseurs utilisent les interfaces de programmation d'applications (API) non documentées pour sauvegarder et récupérer des produits spécifiques, ou pour sauvegarder des fichiers sans vérifier si le service est dans un état cohérent.
- La solution de sauvegarde est-elle compatible avec vos applications ? Par exemple, une nouvelle mise à jour d'un produit peut rendre votre solution de sauvegarde incompatible avec l'application. Contactez le fournisseur de l'application pour déterminer si la solution de sauvegarde d'entreprise est prise en charge.
- Capacité de point de récupération. Déterminez ce qu'est la capacité de point de récupération du produit. Combien de points de restauration la solution de protection des informations de l'entreprise offre t-elle et est-elle appropriée aux besoins de votre organisation ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que Data Protection Manager ?

Data Protection Manager (DPM) est un produit de protection et de récupération de données d'entreprise de Microsoft System Center. DPM offre les fonctionnalités suivantes :



- Centralisation de la sauvegarde. DPM utilise une architecture client/serveur, où le logiciel client est installé sur tous les ordinateurs qui doivent être sauvegardés. Ces clients diffusent en continu des données de sauvegarde au serveur DPM. Cela permet à chaque serveur DPM de prendre en charge des petites ou moyennes entreprises. Vous pouvez également gérer plusieurs serveurs DPM à partir d'une console DPM centralisée.
- RPO de 15 minutes DPM propose des captures instantanées de 15 minutes des produits pris en charge. Cela concerne la majeure partie de la suite des produits d'entreprise de Microsoft, notamment Windows Server avec ses rôles et services, Exchange Server, Hyper-V® et Microsoft SQL Server®.
- Prend en charge les charges de travail de Microsoft. DPM a été conçu spécifiquement par Microsoft pour prendre en charge des applications Microsoft telles que Exchange Server, SQL Server et Hyper-V. Cependant, DPM n'a pas été spécifiquement conçu pour prendre en charge les applications serveur non-Microsoft sans états de disque cohérents ou sans prise en charge VSS.
- Sauvegarde sur disque. DPM peut effectuer des sauvegardes planifiées sur des baies de disques et des réseaux de zone de stockage (SAN, Storage Area Network). Vous pouvez également configurer DPM pour exporter des données de sauvegarde spécifiques destinées à être enregistrées sur bande pour des tâches de conservation et de conformité.
- Sauvegarde de site distant. DPM utilise une architecture qui lui permet de sauvegarder les clients qui sont situés sur des sites distants. Cela signifie qu'un serveur DPM qui se trouve sur le site du siège social peut effectuer des sauvegardes des serveurs et des clients qui sont situés sur les liaisons de réseau étendu.
- Prend en charge les stratégies de sauvegarde en cloud. DPM prend en charge la sauvegarde des serveurs DPM sur une plateforme de cloud. Cela signifie qu'un serveur DPM d'une installation d'hébergement en cloud peut être utilisé pour sauvegarder le contenu d'un serveur DPM du siège social. Pour la redondance d'incidents, vous pouvez également configurer des serveurs DPM pour une sauvegarde mutuelle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Implémentation de la récupération de données et de serveurs

La récupération des serveurs et des données requiert des procédures bien définies et documentées que les administrateurs peuvent suivre en cas de défaillance. Le processus de récupération requiert également la connaissance du matériel et logiciel de sauvegarde et de restauration, comme DPM et les périphériques de bibliothèques de bandes.

Cette leçon décrit la démarche de restauration de donnée et serveurs à l'aide de la fonctionnalité Sauvegarde Windows Server dans Windows Server 2012 et de Windows Azure Online Backup dans Windows Server 2012.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les choix existants en matière de récupération de serveurs.
- Décrire les choix existants en matière de restauration de serveurs.
- Décrire les options de récupération de données.
- Expliquer comment effectuer une restauration avec la fonctionnalité Sauvegarde Windows Server.
- Expliquer comment effectuer une restauration avec Windows Azure Online Backup.

Options pour la récupération de serveurs

La Sauvegarde Windows Server dans Windows Server 2012 fournit les options de récupération suivantes :

Les options en matière de récupération de serveurs incluent
- Fichiers et dossiers
- Applications et données
- Volumes
- Système d'exploitation
- Serveur complet
- État du système

- Fichiers et dossiers. Vous pouvez sauvegarder individuellement les fichiers ou les dossiers si la sauvegarde se trouve sur un volume distinct ou dans un dossier partagé distant.
- Applications et données. Vous pouvez récupérer des applications et des données si le rédacteur de l'application est de type VSS, et que l'application est abonnée à la Sauvegarde Windows Server.
- Volumes. La restauration d'un volume restaure toujours tout son contenu. Lorsque vous choisissez de restaurer un volume, vous ne pouvez pas restaurer des fichiers ou des dossiers spécifiques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

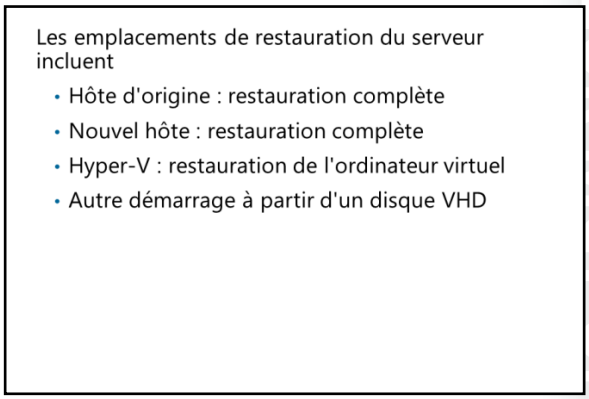
- Système d'exploitation. Vous pouvez récupérer le système d'exploitation via Windows RE, le DVD du produit ou un lecteur flash USB.
- Serveur complet. : Vous pouvez récupérer le serveur complet à l'aide de Windows RE.
- État du système. *L'état du système* crée une sauvegarde à un moment donné, que vous pouvez utiliser pour restaurer un serveur à un état de fonctionnement précédent.

L'Assistant de récupération de la Sauvegarde Windows Server propose plusieurs options pour gérer la récupération de fichiers et dossiers. Les voici :

- **Destination de récupération**. Dans l'option Destination de récupération, vous pouvez sélectionner n'importe quelle option suivante :
  - **Emplacement d'origine**. L'option Emplacement d'origine restaure les données à l'emplacement de la sauvegarde initiale.
  - **Autre emplacement**. L'option Autre emplacement restaure les données à un emplacement différent.
- **Résolution des conflits**. La restauration de données à partir d'une sauvegarde crée fréquemment des conflits avec des versions existantes des données. L'option Résolution de conflit vous permet de déterminer comment ces conflits seront gérés. Lorsque ces conflits se produisent, vous avez la possibilité de choisir entre les actions suivantes :
  - **Créer des copies et conserver les deux versions.**
  - **Remplacer la version existante par la version récupérée.**
  - **Ne pas récupérer les éléments s'ils existent déjà dans l'emplacement de récupération.**
- **Paramètres de sécurité**. Utilisez cette option pour restaurer des autorisations aux données en cours de récupération.

Options pour la restauration de serveurs

Pour effectuer la restauration de serveur, démarrez l'ordinateur à partir des médias d'installation de Windows Server 2012, en sélectionnant l'option de réparation d'ordinateur, puis en sélectionnant l'option de restauration de serveur complète. Autrement, vous pouvez utiliser le média d'installation sur un lecteur flash USB ou à l'aide de Windows RE.



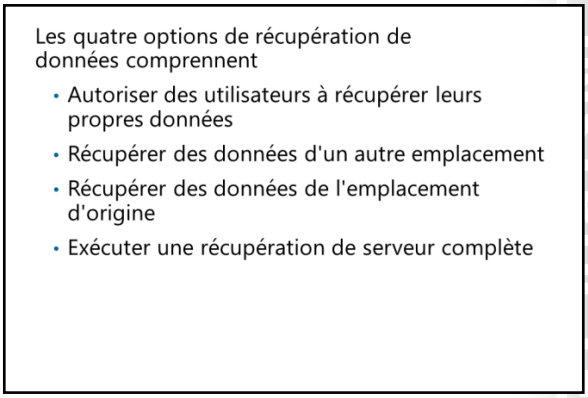
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous effectuez une restauration de serveur complète, prenez en compte les éléments suivants :

- Restauration complète. La restauration complète est le processus pendant lequel vous restaurez un serveur existant dans sa totalité sur le nouveau matériel ou le matériel de remplacement. Quand vous effectuez une restauration complète, la restauration continue et le serveur redémarre. Le serveur devient opérationnel ultérieurement. Dans certains cas, il peut être nécessaire de réinitialiser le compte Active Directory de l'ordinateur parce que ces comptes peuvent parfois être désynchronisés.
- Lecteurs de disques identiques ou supérieurs. Le serveur sur lequel vous restaurez doit disposer de disques durs de capacité identique ou supérieure à ceux du serveur hôte d'origine. Si ce n'est pas le cas, la restauration échouera. Il est possible, bien que non recommandé, de réussir une restauration vers des hôtes qui ont des processeurs plus lents et disposent de moins de mémoire vive (RAM).
- Importation sur Hyper-V Puisque les données de sauvegarde du serveur sont écrites au format VHD, qui est également le format utilisé pour des disques durs d'ordinateurs virtuels, il est possible d'utiliser les données d'une sauvegarde de serveur complète comme base pour créer un ordinateur virtuel. En procédant ainsi, vous garantissez la poursuite de l'activité pendant la recherche du matériel de remplacement approprié.

Options pour la récupération de données

Les données constituent le composant le plus fréquemment récupéré d'une infrastructure informatique. Cela est dû aux utilisateurs supprimant par erreur des données et ayant besoin de les récupérer. Pour développer une procédure de récupération de données, il est possible de mettre en œuvre plusieurs stratégies. Vous pouvez :



- Autoriser des utilisateurs à récupérer leurs données.
- Exécuter une récupération vers un autre emplacement.
- Exécuter une récupération vers l'emplacement d'origine.
- Exécuter une récupération de serveur complète.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les utilisateurs récupèrent leurs propres données

La récupération de données la plus couramment effectuée par les services informatiques est la récupération de fichiers et dossiers que les utilisateurs ont supprimés, perdus, ou d'une certaine façon endommagés. La fonctionnalité **Version précédente des fichiers** qui a été introduite dans Windows Server 2003, (que vous pouvez également activer sur tous les ordinateurs exécutant Windows Server 2012) permet aux utilisateurs de récupérer leurs propres fichiers à l'aide des propriétés de fichiers ou dossiers depuis leur station de travail. Une fois que les utilisateurs finaux sont formés à cette procédure, le service informatique passe moins de temps à récupérer les données d'utilisateur, ce qui lui permet de se concentrer sur des tâches plus importantes.

Du point de vue de la planification, vous devriez envisager d'augmenter la fréquence à laquelle les captures instantanées des versions précédentes des fichiers sont générées. Cela offre aux utilisateurs davantage d'options lorsqu'ils tentent de récupérer leurs fichiers.

Récupération de données sur un autre emplacement

Lors d'une récupération à partir d'une sauvegarde, un problème courant peut se produire : le remplacement involontaire de données importantes. Ceci peut se produire quand la récupération est réalisée sur un emplacement contenant des données actives, au lieu d'un emplacement distinct où les données utiles peuvent être récupérées et les données inutiles ignorées.

Lorsque vous effectuez une récupération vers un autre emplacement, vérifiez toujours quel les autorisations sont également restaurées. Il arrive couramment que lorsque des administrateurs récupèrent des données contenant des informations sensibles d'un emplacement où des autorisations ne sont pas appliquées, ils autorisent involontairement l'accès aux données aux utilisateurs qui ne devraient pas pouvoir y accéder.

Récupération de données de l'emplacement d'origine

Dans certains types de défaillances, tels que la corruption ou la suppression des données, vous devez restaurer des données à l'emplacement d'origine. C'est le cas lorsque des applications ou des utilisateurs qui accèdent aux données, sont préconfigurés avec des informations sur la localisation des données.

Récupération d'un volume

Si un disque est défaillant, il arrive que la manière la plus rapide pour récupérer les données soit de procéder à une récupération de volume, au lieu d'une récupération sélective de fichiers et dossiers. Lorsque vous effectuez une récupération de volume, vérifiez si des dossiers partagés sont configurés pour les disques et si les quotas et les stratégies de gestion de Gestionnaire de ressources du serveur de fichiers sont toujours effectives.

 **Remarque :** Dans le cadre du processus de restauration, vous devriez copier les journaux des événements avant de démarrer le processus de restauration. Si vous remplacez les fichiers journaux d'événements (par une récupération système, par exemple), vous pourrez lire les informations de journal des événements qui se sont produits avant le lancement de la restauration. Ces données de journal des événements pourraient vous mener aux informations relatives à l'origine du problème.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Utilisation de l'utilitaire Sauvegarde Windows Server pour restaurer un dossier

Dans cette démonstration, vous allez apprendre à utiliser l'assistant de récupération pour restaurer un dossier.

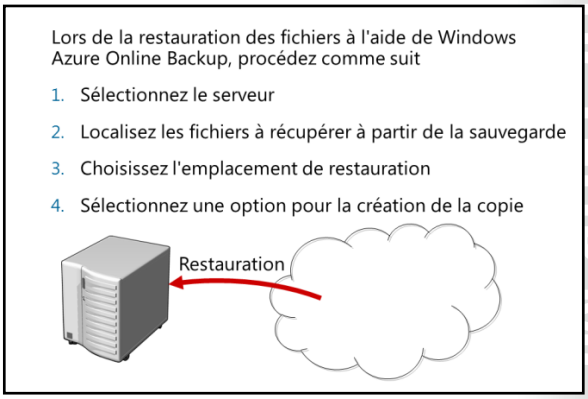
Procédure de démonstration

1. Sur LON-SVR1, supprimez le dossier **C:\HR Data**.
2. Dans Sauvegarde Windows Server, exécutez l'**assistant de récupération** et spécifiez les informations suivantes :
   - Mise en route : **Un autre emplacement**
   - Spécifier un type d'emplacement : **Dossier partagé distant**
   - Spécifier un dossier distant : **\\LON-DC1\Sauvegarde**
   - Sélectionner une date de sauvegarde : **Valeur par défaut, Aujourd'hui**
   - Sélectionner le type de récupération : **Valeur par défaut, fichiers et dossiers**
   - Sélectionner les éléments à récupérer : **LON-SVR1\Disque local (C:)\HR Data**
   - Spécifiez les options de récupération : **Autre emplacement (C:)**
3. Dans l'Explorateur de fichiers, accédez au lecteur C et vérifiez que le dossier **HR Data** est restauré.

Restauration à l'aide de Windows Azure Online Backup

Vous ne pouvez utiliser Windows Azure Online Backup que sur des serveurs Windows Server 2012. Cependant, vous ne devez pas restaurer des données sur le même serveur à partir duquel vous avez effectué la sauvegarde.

Vous pouvez récupérer des fichiers et dossiers à l'aide de la console MMC de Windows Azure Online Backup dans le Gestionnaire de serveurs, ou de l'interface de ligne de commande Windows PowerShell, en procédant comme suit : Pour utiliser la console MMC de Windows Azure Online Backup, procédez comme suit :



1. Sélectionnez le serveur sur lequel les données de sauvegarde ont été initialement créées. Ce serveur pourrait être un serveur local ou un autre serveur. Si vous sélectionnez l'option Un autre serveur, vous devez fournir vos informations d'identification d'administrateur pour Windows Azure Online Backup.
2. Parcourez les fichiers qui doivent être restaurés ou recherchez-les dans Windows Azure Online Backup.

3. Une fois les fichiers localisés, sélectionnez-les pour la récupération, et sélectionnez un emplacement où les fichiers seront restaurés.
4. Lors de la restauration des fichiers, choisissez l'une des options suivantes :
    - Créer des copies de sorte que le fichier restauré et le fichier original se trouvent dans le même emplacement. Le nom du fichier est au format suivant : *Date de récupération*+**Copie de**+*Nom du fichier d'origine*.
    - Remplacer les versions existantes par la version récupérée.
    - Ne pas récupérer les éléments qui existent déjà dans l'emplacement de destination de la récupération.

Une fois la procédure de restauration terminée, les fichiers sont restaurés sur le serveur Windows Server 2012 au niveau de votre site.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation des fonctionnalités de sauvegarde et de restauration de Windows Server

Scénario

De nombreuses données stockées sur le réseau de l'entreprise A. Datum Corporation sont extrêmement précieuses pour l'organisation. La perte de ces données serait lourde de conséquences pour l'organisation. En outre, plusieurs serveurs qui s'exécutent sur le réseau fournissent des services extrêmement précieux pour l'organisation ; ce qui signifie que la perte de ces serveurs pendant une durée importante aurait également des conséquences négatives pour l'organisation. En raison de l'importance des données et des services, il est crucial qu'ils puissent être restaurés même si un incident se produit.

La société A. Datum envisage de sauvegarder des données essentielles sur un service en cloud. A. Datum considère également ceci comme option pour les petites filiales qui ne disposent pas d'une infrastructure complète de centre de données.

En tant que l'un des administrateurs réseau seniors chez A. Datum, vous êtes chargé de planifier et d'implémenter une solution de récupération d'urgence qui garantit la récupération des données et des services essentiels en cas de défaillance de tout type. Vous devez implémenter un processus de sauvegarde et de restauration qui peut récupérer les données et les services perdus.

Objectifs

- Sauvegarder des données sur un serveur Windows Server 2012
- Restaurer des fichiers à l'aide de la Sauvegarde Windows Server
- Implémenter Windows Azure Online Backup et la restauration

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	**22412B-LON-DC1** **22412B-LON-SVR1** **MSL-TMG1**
Nom d'utilisateur	Adatum\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22412B-LON-DC1** et, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Connexion**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22412B-LON-SVR1**.
6. Répétez l'étape 2 pour **MSL-TMG1**.

Exercice 1 : Sauvegarde de données sur un serveur Windows Server 2012

Scénario

Le serveur LON-SVR1 contient des données financières qui doivent être sauvegardées régulièrement. Ces données sont essentielles pour l'organisation. Vous avez décidé d'utiliser l'utilitaire Sauvegarde Windows Server pour sauvegarder des données essentielles. Vous installerez cette fonctionnalité et configurerez des sauvegardes planifiées.

Les tâches principales de cet exercice sont les suivantes :

1. Installer Sauvegarde Windows Server
2. Configurer une sauvegarde planifiée
3. Terminer une sauvegarde à la demande

▶ Tâche 1 : Installer Sauvegarde Windows Server

1. Basculez vers **LON-SVR1**.
2. Dans le Gestionnaire de serveur, installez la fonctionnalité Sauvegarde Windows Server. Acceptez les valeurs par défaut de l'Assistant Ajout de rôles et de fonctionnalités.

▶ Tâche 2 : Configurer une sauvegarde planifiée

1. Sur LON-SVR1, démarrez la fonctionnalité **Sauvegarde Windows Server**.
2. Configurez la planification de sauvegarde avec les options suivantes :
   - Configuration de la sauvegarde : **serveur complet (recommandé)**
   - Heure de la sauvegarde : **Une fois par jour, à 01h00**
   - Type de destination : **sauvegarder dans un dossier réseau partagé**
   - Dossier partagé distant : \\LON-DC1\Sauvegarde.
     - Enregistrer la planification de sauvegarde : Nom d'utilisateur : **Administrateur**
     - Mot de passe : **Pa$$w0rd**

 **Remarque :** Dans un environnement de production, vous n'enregistrerez pas la sauvegarde dans un contrôleur de domaine. Vous le faites ici uniquement dans le cadre de l'atelier pratique.

▶ Tâche 3 : Terminer une sauvegarde à la demande

1. Sur LON-SVR1, démarrez la fonctionnalité **Sauvegarde Windows Server**.
2. Exécutez l'assistant de Sauvegarde unique pour sauvegarder le dossier **C:\Financial Data** vers le dossier distant, **\\LON-DC1\Backup**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré la fonctionnalité Sauvegarde Windows Server, aurez planifié une tâche de sauvegarde, et aurez effectué une sauvegarde à la demande.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Restauration de fichiers à l'aide des fonctionnalités de sauvegarde de Windows Server

Scénario

Pour vous assurer qu'il est possible de restaurer les données financières, vous devez valider la procédure pour restaurer les données sur un autre emplacement.

Les tâches principales de cet exercice sont les suivantes :

1. Supprimer un fichier du serveur de fichiers
2. Restaurer un fichier à partir de la sauvegarde

▶ Tâche 1 : Supprimer un fichier du serveur de fichiers

- Sur LON-SVR1, ouvrez **Explorateur de fichiers**, puis supprimez le dossier **C:\Financial Data**.

▶ Tâche 2 : Restaurer un fichier à partir de la sauvegarde

1. Dans la console MMC de la Sauvegarde Windows Server, exécutez l'**assistant de récupération** et spécifiez les informations suivantes :
   - Mise en route : **Un autre emplacement**
   - Spécifier un type d'emplacement : **Dossier partagé distant**
   - Spécifier un dossier distant : **\\LON-DC1\Backup**
   - Sélectionner une date de sauvegarde : **Valeur par défaut, Aujourd'hui**
   - Sélectionner le type de récupération : **Valeur par défaut, fichiers et dossiers**
   - Sélectionner les éléments à récupérer : **LON-SVR1\disque local (C:)\Financial Data**
   - Spécifiez les options de récupération : **Autre emplacement (C:)**
2. Ouvrez le lecteur **C**, et vérifiez que le dossier **Financial Data** est restauré.

Résultats : Après avoir effectué cet exercice, vous aurez testé et validé la procédure de restauration d'un fichier à partir d'une sauvegarde.

Exercice 3 : Implémentation de sauvegarde et de restauration Windows Azure Online

Scénario

A. Datum doit protéger des données essentielles dans ses petites filiales. Ces bureaux ne disposent ni du matériel de sauvegarde, ni des infrastructures de centre de données. Par conséquent A. Datum a décidé de sauvegarder les données essentielles des filiales dans un service dans le cloud à l'aide de Windows Azure Online Backup dans Windows Server 2012.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le composant de Windows Azure™ Online Backup
2. Inscrire le serveur à Windows Azure Online Backup

3. Configurer Windows Azure Online Backup et démarrer une sauvegarde.
4. Restaurer des fichiers à l'aide de la Windows Azure Online Backup
5. Désinscrire le serveur à partir de Windows Azure Online Backup

▶ Tâche 1 : Installer le composant de Windows Azure™ Online Backup

1. Sur LON-SVR1, sur le lecteur E, localisez le fichier d'installation de l'agent Windows Azure Online Backup, **OBSInstaller. exe**.
2. Démarrez l'installation de l'agent Windows Azure Online Backup en double-cliquant sur le fichier d'installation.
3. Terminez l'installation en spécifiant les informations suivantes :
   - Dossier d'installation : **C:\Program Files\Agent Windows Azure Online Backup**.
   - Emplacement du cache : **C:\Program Files\Agent Windows Azure Online Backup\Scratch**.
   - Abonnement à Microsoft Update : **Je ne souhaite pas utiliser Microsoft Update**.
4. Vérifiez l'installation et assurez-vous de recevoir le message suivant : **L'installation de l'agent Windows Azure Online Backup s'est achevée avec succès**.
5. Désactivez la case à cocher **Rechercher des mises à jour plus récentes**, puis cliquez sur **Terminer**.
6. Dans le menu **Accueil,** vérifiez l'installation en cliquant sur **Windows Azure Online Backup**, et sur **Interpréteur de commandes de Windows Azure Online Backup**.

▶ Tâche 2 : Inscrire le serveur à Windows Azure Online Backup

Avant que vous inscriviez le serveur, vous devez renommer LON-SVR1 en *NOMDEVOTREVILLE-VOTRENOM*. Par exemple : **PARIS-ALICE**. Cet exercice étant effectué en ligne, les noms des ordinateurs utilisés dans cet atelier pratique doivent être uniques. Si plusieurs stagiaires dans la classe portent le même nom, ajoutez un numéro à la fin du nom de l'ordinateur, tel que **PARIS-ALICE-1**.

Pour renommer LON-SVR1, procédez comme suit :

1. Dans la fenêtre du Gestionnaire de serveurs**,** remplacez le nom de **LON-SVR1** par *NOMDEVOTREVILLE-VOTRENOM*, puis redémarrez *NOMDEVOTREVILLE-VOTRENOM*.
2. Attendez que *NOMDEVOTREVILLE-VOTRENOM* ait redémarré, puis connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour inscrire le serveur à Windows Azure Online Backup, procédez comme suit :

1. Dans la console Windows Azure Online Backup, inscrivez **LON-SVR1** en spécifiant les informations suivantes dans l'assistant Inscrire le serveur :
   - Paramètres de chiffrement :
     - Entrez la phrase secrète : **Pa$$w0rdPa$$w0rd**
     - Confirmez la phrase secrète : **Pa$$w0rdPa$$w0rd**
   - Informations d'identification du compte :
     - Nom d'utilisateur : **MSLTestUser@MSL TestOrg.onmicrosoft.com**
     - Mot de passe : **Pa$$w0rd**

 **Remarque :** en situation réelle, vous saisiriez le nom d'utilisateur et le mot de passe de votre compte d'abonnement à Windows Azure Online Backup.

2. Vérifiez que vous recevez le message suivant : **Windows Azure Online Backup est maintenant disponible pour ce serveur**

▶ Tâche 3 : Configurer Windows Azure Online Backup et démarrer une sauvegarde

1. Basculez vers la console Windows Azure Online Backup.
2. Configurez une sauvegarde en ligne à l'aide des options suivantes :
   - Sélectionner les éléments à sauvegarder : **C:\Financial Data**
   - Spécifiez l'heure de la sauvegarde : **Samedi, 01:00**
   - Spécifiez le paramètre de rétention : Valeurs par défaut
3. Dans la console Windows Azure Online Backup, cliquez sur **Sauvegarder maintenant**.
4. Patientez jusqu'à ce que le message **Sauvegarde réussie** s'affiche, puis fermez la fenêtre du message.

▶ Tâche 4 : Restaurer des fichiers à l'aide de la Windows Azure Online Backup

1. Sur LON-SVR1, ouvrez **Explorateur de fichiers**, puis supprimez le dossier **C:\Financial Data**.
2. Basculez vers la console **Windows Azure Online Backup**.
3. Restaurer des fichiers et dossiers à l'aide de l'option **Récupérer des données**, et spécifiez les informations suivantes :
   - Identifiez le serveur sur lequel la sauvegarde a été initialement créée : **Ce serveur**
   - Sélectionnez le mode de récupération : **Parcourir les fichiers**
   - Sélectionnez le volume et la date : **C:**, et utilisez la date et l'heure auxquelles vous avez effectué la dernière sauvegarde.
   - Sélectionnez les éléments à récupérer : **C:\Financial Data**
   - Spécifiez les options de récupération : **Emplacement d'origine** et **Créer des copies pour avoir les deux versions**.
4. Dans l'Explorateur de fichiers, développez le lecteur **C**, et vérifiez que le dossier **Financial Data** est restauré sur le lecteur C.

▶ Tâche 5 : Désinscrire le serveur à partir de Windows Azure Online Backup

1. Basculez vers la console **Windows Azure Online Backup**.
2. Désinscrivez le serveur à partir de Windows Azure Online Backup à l'aide des informations d'identification suivantes :
   - Nom d'utilisateur : **MSLTestUser@MSLTestOrg.onmicrosoft.com**
   - Mot de passe : **Pa$$w0rd**

Résultats : Après avoir terminé cet exercice, vous aurez installé l'agent Windows Azure Online Backup, inscrit le serveur avec Windows Azure Online Backup, configuré une sauvegarde planifiée, et effectué une restauration à l'aide de Windows Azure Online Backup.

▶ Pour préparer la prochaine application pratique, vous devez effectuer les tâches suivantes :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, et **MSL-TMG1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée :

- Analysez vos ressources en infrastructure importantes et vos données essentielles à l'accomplissement de votre mission et à votre entreprise. En fonction de cette analyse, créez une stratégie de sauvegarde qui protégera les ressources en infrastructure et les données commerciales essentielles de l'entreprise.
- Avec l'aide des directeurs commerciaux de l'organisation, identifiez le temps de récupération minimum pour les données essentielles de l'entreprise. En fonction de ces informations, créez une stratégie de restauration optimale.
- Testez régulièrement les procédures de sauvegarde et de restauration. Réalisez l'essai dans un environnement isolé et non en cours de production.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Des composants du serveur ont rencontré une défaillance importante.	

Questions de contrôle des acquis

Question : Vous souhaitez créer une stratégie pour sauvegarder différentes technologies qui sont utilisées dans votre organisation, telles que DHCP, DNS, AD DS et SQL Server. Que devez-vous faire ?

Question : À quelle fréquence devez-vous effectuer les sauvegardes des données essentielles ?

Problèmes réels et scénarios

Votre organisation a besoin d'informations sur les données à sauvegarder, sur la fréquence des sauvegardes des différents types de données et technologies, sur le lieu de stockage des données sauvegardées (sur site ou sur le cloud), et sur la vitesse à laquelle elle peut restaurer les données sauvegardées. Comment amélioreriez-vous la capacité de votre organisation à restaurer efficacement des données lorsque cela s'avère nécessaire ?

Outils

Outil	Utilisez	Emplacement
Sauvegarde Windows Server	Exécution de sauvegardes à la demande ou planifiées, et restauration des données et des serveurs	Gestionnaire de serveur - Outils
Windows Azure Online Backup	Exécution de sauvegardes à la demande ou planifiées vers le cloud, et restauration de données à partir de la sauvegarde située dans le cloud.	Gestionnaire de serveur - Outils

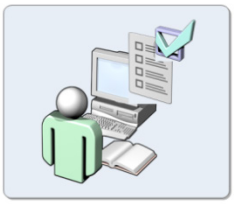
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Évaluation du cours

Votre évaluation de ce cours aidera Microsoft à comprendre la qualité de votre expérience de formation.

Consultez votre formateur pour accéder au formulaire d'évaluation du cours.

Votre évaluation est strictement confidentielle et vos réponses à cette enquête seront utilisées dans le seul but d'améliorer la qualité des prochains cours Microsoft. Vos commentaires ouverts et honnêtes sont très précieux.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1 : Implémentation des services réseau avancés

Atelier pratique : Implémentation des services réseau avancés

Exercice 1 : Configuration des paramètres avancés du protocole DHCP (Dynamic Host Configuration Protocol)

▶ Tâche 1 : Configurer une étendue globale

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **DHCP**.
2. Dans la console DHCP, cliquez sur **lon-dc1.adatum.com**, cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**.
3. Dans l'Assistant Nouvelle étendue, cliquez sur **Suivant**.
4. Dans la page **Nom de l'étendue**, dans la zone **Nom**, saisissez **Etendue1**, puis cliquez sur **Suivant**.
5. Dans la page **Plage d'adresses IP**, dans la zone **Adresse IP de début**, saisissez **192.168.0.50**, puis dans la zone **Adresse IP de fin**, saisissez **192.168.0.100**.
6. Dans la zone **Masque de sous-réseau**, vérifiez que **255.255.255.0** est entré, puis cliquez sur **Suivant**.
7. Dans la page **Ajout d'exclusions et de retard**, cliquez sur **Suivant**.
8. Sur la page **Durée du bail**, cliquez sur **Suivant**.
9. Dans la page **Configuration des paramètres DHCP**, sélectionnez **Oui, je veux configurer ces options maintenant**, puis cliquez sur **Suivant**.
10. Sur la page **Routeur (passerelle par défaut)**, dans la zone **Adresse IP**, tapez **192.168.0.1**, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
11. Sur la page **Nom de domaine et serveurs DNS**, vérifiez que le domaine parent est **Adatum.com**, puis cliquez sur **Suivant**.
12. Sur la page **Serveurs WINS**, cliquez sur **Suivant**.
13. Sur la page **Activer l'étendue**, cliquez sur **Non, j'activerai cette étendue ultérieurement**, puis cliquez sur **Suivant**.
14. Sur la page **Fin de l'Assistant Nouvelle étendue**, cliquez sur **Terminer**.
15. Cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**.
16. Dans l'Assistant Nouvelle étendue, cliquez sur **Suivant**.
17. Dans la page **Nom de l'étendue**, dans la zone **Nom**, saisissez **Etendue2**, puis cliquez sur **Suivant**.
18. Dans la page **Plage d'adresses IP**, dans la zone **Adresse IP de début**, saisissez **192.168.1.50**, puis dans la zone **Adresse IP de fin**, saisissez **192.168.1.100**.
19. Dans la zone **Masque de sous-réseau**, vérifiez que **255.255.255.0** est entré, puis cliquez sur **Suivant**.
20. Dans la page **Ajout d'exclusions et de retard**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

21. Sur la page **Durée du bail**, cliquez sur **Suivant**.
22. Dans la page **Configuration des paramètres DHCP**, sélectionnez **Oui, je veux configurer ces options maintenant**, puis cliquez sur **Suivant**.
23. Sur la page **Routeur (passerelle par défaut)**, dans la zone **Adresse IP**, tapez **192.168.1.1**, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
24. Sur la page **Nom de domaine et serveurs DNS**, vérifiez que le domaine parent est **Adatum.com**, puis cliquez sur **Suivant**.
25. Sur la page **Serveurs WINS**, cliquez sur **Suivant**.
26. Sur la page **Activer l'étendue**, cliquez sur **Non, j'activerai cette étendue ultérieurement**, puis cliquez sur **Suivant**.
27. Sur la page **Fin de l'Assistant Nouvelle étendue**, cliquez sur **Terminer**.
28. Cliquez avec le bouton droit sur le nœud **IPv4**, puis cliquez sur **Nouvelle étendue globale**.
29. Dans l'Assistant Nouvelle super-étendue, cliquez sur **Suivant**.
30. Sur la page **Nom d'étendue globale**, dans la zone **Nom**, saisissez **AdatumSuper**, puis cliquez sur **Suivant**.
31. Sur la page **Choix des étendues**, sélectionnez **Etendue1**, maintenez la touche Ctrl enfoncée, sélectionnez **Etendue2**, puis cliquez sur **Suivant**.
32. Sur la page **Fin de l'Assistant Nouvelle étendue globale**, cliquez sur **Terminer**.
33. Dans la console DHCP, sous IPv4, sélectionnez **Étendue globale Adatum Super** et cliquez dessus avec le bouton droit, puis cliquez sur **Activer**.

▶ Tâche 2 : Configurer la protection de nom DHCP

1. Sur LON-DC1, dans la console DHCP, développez **lon-dc1.adatum.com**.
2. Cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de : IPv4**, cliquez sur l'onglet **DNS**.
4. Dans le volet Nommer la protection, cliquez sur **Configurer**.
5. Activez la case à cocher **Activer la protection des noms**, puis cliquez sur **OK**.
6. Cliquez de nouveau sur **OK**.

▶ Tâche 3 : Configurer et vérifier le basculement DHCP

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **DHCP** dans la liste déroulante. Notez que le serveur est autorisé, mais qu'aucune étendue n'est configurée.
2. Sur LON-DC1, dans la console DHCP, cliquez avec le bouton droit sur le nœud **IPv4**, puis cliquez sur **Configurer un basculement**.
3. Dans l'Assistant Configuration du basculement, cliquez sur **Suivant**.
4. Sur la page **Spécifier le serveur partenaire à utiliser pour le basculement**, dans la zone **Serveur partenaire**, entrez **172.16.0.21**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Sur la page **Créer une relation de basculement**, dans la zone **Nom de la relation**, entrez **Adatum**.
6. Dans le champ **Délai de transition maximal du client (MCLT)**, définissez les heures sur **0**, puis définissez les minutes sur **15**.
7. Assurez-vous que le champ **Mode** est défini sur **Équilibrage de charge**, et que **Pourcentage d'équilibrage de charge** est défini sur **50 %**.
8. Activez la case à cocher **Intervalle de basculement d'état**. Laissez la valeur par défaut de 60 minutes.
9. Dans la zone **Activer le secret d'authentification des messages partagé**, saisissez **Pa$$w0rd**, puis cliquez sur **Suivant**.
10. Cliquez sur **Terminer**, puis sur **Fermer**.
11. Sur LON-SVR1, actualisez le nœud IPv4, puis notez que le nœud IPv4 est actif.
12. Développez le nœud IPv4, développez **Étendue [172.16.0.0] Adatum**, cliquez sur le nœud **Pool d'adresses**, et notez que le pool d'adresses est configuré.
13. Cliquez sur le nœud **Options d'étendue** et notez que les options d'étendue sont configurées.
14. Démarrez **22412B-LON-CL1**, puis ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
15. Dans le menu Accueil, tapez **Panneau de configuration**.
16. Dans la zone **Applications Résultats**, cliquez sur **Panneau de configuration**.
17. Dans le panneau de configuration, cliquez sur **Réseau et Internet**, cliquez sur **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de la carte**, cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
18. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
19. Dans la boîte de dialogue **Propriétés**, sélectionnez la case d'option **Obtenir une adresse IP automatiquement**, cliquez sur **Obtenir les adresses des serveurs DNS automatiquement**, puis cliquez sur **OK**.
20. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, cliquez sur **Fermer**.
21. Pointez au-dessus du coin inférieur droit pour exposer le menu de vol, puis cliquez sur l'icône **Rechercher**.
22. Dans la zone de recherche **Applications**, saisissez **Cmd**, puis appuyez sur **Entrée**.
23. Dans la fenêtre de l'invite de commandes, tapez **ipconfig**, puis appuyez sur Entrée. Enregistrez votre adresse IP.
24. Sur **LON-DC1**, cliquez sur l'icône **Gestionnaire de serveur** dans la barre des tâches.
25. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Services**.
26. Dans la fenêtre Services, cliquez avec le bouton droit sur le service **Serveur DHCP**, puis cliquez sur **Arrêter** pour arrêter le service.
27. Fermez la fenêtre Services, et fermez la console DHCP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

28. Sur **LON-CL1**, dans la fenêtre d'invite de commandes, tapez **ipconfig /release**, puis appuyez sur Entrée.
29. Tapez **ipconfig /renew**, puis appuyez sur Entrée.
30. Tapez **ipconfig**, puis appuyez sur Entrée. Quelle est votre adresse IP ? Les réponses peuvent varier.
31. Arrêtez le serveur LON-SVR1.
32. Sur LON-DC1, dans la console LON-SVR1, démarrez le service de serveur DHCP.
33. Fermez la console Services.

Résultats : À l'issue de cet exercice, vous aurez configuré une étendue globale, une protection de nom DHCP, et configuré et vérifié le basculement DHCP.

Exercice 2 : Configuration des paramètres DNS avancés

▶ Tâche 1 : Configurer DNSSEC

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS** dans la liste déroulante.
2. Développez successivement **LON-DC1** et **Zones de recherché directes**, cliquez sur **Adatum.com**, puis cliquez avec le bouton droit sur **Adatum.com**.
3. Dans le menu, cliquez sur **DNSSEC>Signer la zone**.
4. Dans l'Assistant Signature de zone, cliquez sur **Suivant**.
5. Sur la page **Options de signature**, cliquez sur **Personnalisez les paramètres de signature de zone**, puis cliquez sur **Suivant**.
6. Sur la page **Maître des clés**, assurez-vous que le serveur DNS (Domain Name System) **LON-DC1** est sélectionné comme Maître des clés, puis cliquez sur **Suivant**.
7. Sur la page **Clé KSK**, cliquez sur **Suivant**.
8. Sur la page **Clé KSK**, cliquez sur **Ajouter**.
9. Sur la page **Nouvelle clé KSK**, cliquez sur **OK**.
10. Sur la page **Clé KSK**, cliquez sur **Suivant**.
11. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
12. Sur la page **Clé ZSK**, cliquez sur **Ajouter**.
13. Sur la page **Nouvelle clé ZSK**, cliquez sur **OK**.
14. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
15. Sur la page **Next Secure (NSEC)**, cliquez sur **Suivant**.
16. Sur la page **Ancres d'approbation**, cochez la case **Activer la distribution des ancres d'approbation pour cette zone**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

17. Sur la page **Paramètres de signature et d'interrogation**, cliquez sur **Suivant**.
18. Sur la page **Extensions de sécurité DNS (DNSSEC)**, cliquez sur **Suivant**, puis sur **Terminer**.
19. Dans la console DNS, développez successivement **Points d'approbation** et **com**, puis cliquez sur **Adatum**. Assurez-vous que les enregistrements de ressource de DNSKEY s'affichent, et que leur état est valide.
20. Réduisez le Gestionnaire DNS.
21. Dans le Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante, cliquez sur **Gestion des stratégies de groupe**.
22. Développez **Forêt : Adatum.com**, **Domaines**, **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
23. Dans l'Éditeur de gestion des stratégies de groupe, sous Configuration ordinateur, développez successivement **Stratégies** et **Paramètres Windows**, puis cliquez sur **Stratégie de résolution de noms**.
24. Dans le volet de droite, sous Créer des règles, dans la zone **Suffixe**, saisissez **Adatum.com** pour appliquer la règle au suffixe de l'espace de noms.
25. Activez la case à cocher **Activer DNSSEC dans cette règle** et **Demander aux clients DNS de vérifier que les données de nom et d'adresse ont été validées par le serveur DNS**, puis cliquez sur **Créer**.
26. Fermez les consoles Éditeur de gestion des stratégies de groupe et Gestion des stratégies de groupe.

▶ Tâche 2 : Configurer le pool de sockets DNS

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell®**.
2. Dans la fenêtre Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
Get-DNSServer
```

   Cette commande affiche la taille actuelle du pool de sockets DNS (sur la quatrième ligne de la section ServerSetting). Notez que la taille actuelle est de 2 500.

3. Tapez la commande suivante et appuyez sur Entrée pour modifier la taille du pool de sockets pour 3 000 :

```
dnscmd /config /socketpoolsize 3000
```

4. Tapez la commande suivante et appuyez sur Entrée pour arrêter le serveur DNS :

```
net stop dns
```

5. Tapez la commande suivante et appuyez sur Entrée pour redémarrer le serveur DNS :

```
net start dns
```

6. Tapez la commande suivante et appuyez sur Entrée pour confirmer la nouvelle taille du pool de sockets.

```
Get-DnsServer
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer le verrouillage de cache DNS

1. Dans la fenêtre Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
Get-Dnsserver
```

   Ceci affiche la valeur actuelle du pourcentage du verrouillage de cache DNS. Notez que la valeur actuelle est de 100 %. La valeur s'affiche dans la section ServerCache.

2. Tapez la commande suivante, puis appuyez sur Entrée :

```
Set-DnsServerCache –LockingPercent 75
```

   Ceci modifie la valeur de verrouillage de cache pour 75 pour cent.

3. Tapez la commande suivante et appuyez sur Entrée pour arrêter le serveur DNS :

```
net stop dns
```

4. Tapez la commande suivante et appuyez sur Entrée pour redémarrer le serveur DNS :

```
net start dns
```

5. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-DnsServer
```

   Cette commande affiche la valeur actuelle du pourcentage du verrouillage de cache DNS. Notez que la nouvelle valeur est de 75 %.

6. Laissez la fenêtre d'invite de commandes ouverte pour la tâche suivante.

▶ Tâche 4 : Configurer une zone GlobalNames

1. Créez une zone de recherche directe intégrée à Active Directory nommée **Contoso.com** en exécutant l'applet de commande suivant dans Windows PowerShell :

```
Add-DnsServerPrimaryZone –Name Contoso.com –ReplicationScope Forest
```

2. Dans la fenêtre Windows PowerShell, saisissez la commande suivante, puis appuyez sur Entrée pour activer la prise en charge des zones GlobalName :

```
Set-DnsServerGlobalNameZone –AlwaysQueryServer $true
```

3. Créez une zone de recherche directe intégrée à Active Directory® nommée **GlobalNames** en exécutant la commande suivante :

```
Add-DnsServerPrimaryZone –Name GlobalNames –ReplicationScope Forest
```

4. Réduisez la fenêtre d'invite de commandes.

5. Depuis la barre des tâches, restaurez la console DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la console DNS, cliquez sur **Action**, puis cliquez sur **Actualiser**.
7. Dans la console DNS, développez **Zones de recherché directes**, cliquez sur la zone **Contoso.com**, cliquez avec le bouton droit sur **Contoso.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
8. Dans la boîte de dialogue **Nouvel hôte**, dans la zone **Nom**, tapez **App1**.

Remarque : La zone **Nom** utilise le nom de domaine parent si elle est laissée vierge.

9. Dans la zone **Adresse IP**, tapez **192.168.1.200**, puis cliquez sur **Ajouter un hôte**.
10. Cliquez sur **OK**, puis sur **Terminé**.
11. Sélectionnez **GlobalNames** et cliquez dessus avec le bouton droit, puis cliquez sur **Nouvel alias (CNAME)**.
12. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans la zone **Nom de l'alias**, saisissez **App1**.
13. Dans la zone **Nom de domaine complet (FQDN) pour l'hôte de destination**, saisissez **App1.Contoso.com**, puis cliquez sur **OK**.
14. Fermez le Gestionnaire DNS et fermez l'invite de commandes.

Résultats : À l'issue de cet exercice, vous aurez configuré DNSSEC, le pool de sockets DNS, le verrouillage de cache DNS et la zone GlobalName.

Exercice 3 : Configuration de IPAM

▶ Tâche 1 : Installer la fonctionnalité IPAM

1. Sur LON-SVR2, dans le tableau de bord du Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, activez la case à cocher **Serveur de gestion des adresses IP (IPAM)**.
7. Dans la fenêtre contextuelle **Ajouter les fonctionnalités requises pour le Serveur de gestion des adresses IP (IPAM)**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
8. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Fermez l'Assistant Ajout de rôles et de fonctionnalités une fois l'opération terminée.

▶ Tâche 2 : Configurer des objets de stratégie de groupe en relation avec IPAM

1. Sur LON-SVR2, dans le volet de navigation Gestionnaire de serveur, cliquez sur **IPAM**.
2. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Se connecter au serveur IPAM**, cliquez sur **LON-SVR2.Adatum.com**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez sur **Configurer le serveur IPAM**.
4. Dans l'Assistant Configuration d'IPAM, sur la page **Avant de commencer**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner la méthode d'approvisionnement**, vérifiez que la méthode **Basée sur une stratégie de groupe** est sélectionnée, dans la zone **Préfixe du nom d'objet de stratégie de groupe**, saisissez **IPAM**, puis cliquez sur **Suivant**.
6. Sur la page **Confirmer les paramètres**, cliquez sur **Appliquer**. La configuration prendra quelques instants.
7. Une fois la configuration terminée, cliquez sur **Fermer**.

▶ Tâche 3 : Configurer la découverte de serveurs d'administration d'IP

1. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Configurer la découverte de serveurs**.
2. Dans la boîte de dialogue de paramètres **Configurer la découverte de serveurs**, cliquez sur **Ajouter**, puis cliquez sur **OK**.
3. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Démarrer la découverte de serveurs**. Le processus de découverte peut durer 5 à 10 minutes. La barre jaune indique quand la découverte est terminée.

▶ Tâche 4 : Configurer des serveurs gérés

1. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Sélectionner ou ajouter des serveurs à gérer et vérifier l'accès IPAM**. Notez que l'état de l'accès IPAM est bloqué.
2. Faites défiler l'écran jusqu'au volet Détails et notez le rapport d'état, qui doit indiquer que le serveur IPAM n'a pas encore été autorisé à gérer LON-DC1 via la Stratégie de groupe.
3. Dans la barre des tâches, cliquez avec le bouton droit sur l'icône Windows PowerShell, puis sur **Windows PowerShell** et cliquez sur **Exécuter en tant qu'administrateur**.
4. À l'invite Windows PowerShell, saisissez la commande suivante et cliquez sur Entrée :

```
Invoke-IpamGpoProvisioning –Domain Adatum.com –GpoPrefixName IPAM –IpamServerFqdn
LON-SVR2.adatum.com –DelegatedGpoUser Administrateur
```

5. Quand vous êtes invité à confirmer l'action, saisissez **O**, puis appuyez sur Entrée. Cette commande demande quelques minutes pour s'exécuter.
6. Fermez Windows PowerShell.
7. Dans le Gestionnaire de serveur, dans le volet Détails, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Modifier le serveur**.
8. Dans la boîte de dialogue **Ajouter ou modifier un serveur**, définissez **État de gérabilité** sur **Géré**, puis cliquez sur **OK**.
9. Basculez vers LON-DC1.
10. Dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
11. À l'invite de Windows PowerShell, saisissez **Gpupdate /force** et appuyez sur Entrée.
12. Fermez la fenêtre Windows PowerShell.
13. Basculez vers LON-SVR2.
14. Dans le Gestionnaire de serveur, dans la console IPAM, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Actualiser l'état de l'accès au serveur**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

15. Une fois l'actualisation terminée, cliquez sur le bouton d'actualisation de la console du Gestionnaire de serveur. La modification de l'état peut prendre jusqu'à 10 minutes. Au besoin, répétez les deux tâches d'actualisation comme nécessaire jusqu'à ce qu'une coche verte s'affiche à côté de LON-DC1 et que l'accès à IPAM affiche l'état **Débloqué**.
16. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Récupérer les données des serveurs gérés**. L'exécution de cette action prendra quelques minutes.

▶ Tâche 5 : Configurer et vérifier une nouvelle étendue DHCP avec IPAM

1. Sur LON-SVR2, dans le volet de navigation d'IPAM, sous SURVEILLER ET GÉRER, cliquez sur **serveurs DNS et DHCP**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur l'instance de **LON-DC1.Adatum.com** qui contient le rôle de serveur DHCP, puis cliquer sur **Créer une étendue DHCP**.
3. Dans la boîte de dialogue **Créer une étendue DHCP**, dans la zone **Nom de l'étendue**, saisissez **TestScope**.
4. Dans la zone **Adresse IP de début**, saisissez **10.0.0.50**.
5. Dans la zone **Adresse IP de fin**, saisissez **10.0.0.100**.
6. Vérifiez que le masque de sous-réseau est **255.0.0.0**.
7. Dans le volet Créer une étendue, cliquez sur **Options**.
8. Dans le volet Configurer les options, cliquez sur la flèche de déroulement **Option**, puis sélectionnez **003 Routeur**.
9. Sous **Valeurs**, dans la zone **Adresse IP**, saisissez **10.0.0.1**, cliquez sur **Ajouter à la liste**, puis cliquez sur **OK**.
10. Sur LON-DC1, dans la barre d'outils du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP**.
11. Dans la console DHCP, développez successivement **lon-dc1.adatum.com** et **IPv4**, puis confirmez l'existence de TestScope.
12. Réduisez la console DHCP en icône.

▶ Tâche 6 : Configurer des blocs d'adresses IP, enregistrer des adresses IP et créer des réservations DHCP et des enregistrements DNS

1. Sur LON-SVR2, dans le Gestionnaire de serveur, dans l'arborescence de console IPAM, cliquez sur **Blocs d'adresses IP**.
2. Dans le volet droit, cliquez sur la flèche de déroulement **TÂCHES**, puis cliquez sur **Ajouter un bloc d'adresses IP**.
3. Dans la boîte de dialogue **Ajouter ou modifier un bloc d'adresses IPv4**, renseignez les valeurs suivantes, puis cliquez sur **OK** :
   - ID réseau : **172.16.0.0**
   - Longueur du préfixe : **16**
   - Description : **Siège social**
4. Dans l'arborescence de la console IPAM, cliquez sur **Inventaire d'adresses IP**.
5. Dans le volet droit, cliquez sur la flèche de déroulement **TÂCHES**, puis cliquez sur **Ajouter une adresse IP**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la boîte de dialogue **Ajouter une adresse IP**, sous **Configurations de base**, renseignez les valeurs suivantes, puis cliquez sur **OK** :
   - Adresse IP : **172.16.0.1**
   - Adresse MAC : **112233445566**
   - Type de périphérique : **Routeurs**
   - Description : **Routeur de siège social**
7. Cliquez sur la flèche de déroulement **TÂCHES**, puis cliquez sur **Ajouter une adresse IP**.
8. Dans la boîte de dialogue **Ajouter une adresse IP**, sous **Configuration de base**, renseignez les valeurs suivantes :
   - Adresse IP : **172.16.0.10**
   - Adresse MAC : **223344556677**
   - Type de périphérique : **Hôte**
9. Dans le volet Ajouter une adresse IPv4, cliquez sur **Réservation DHCP**, puis entrez les valeurs suivantes :
   - Nom du serveur de réservations : **LON-DC1.Adatum.com**
   - Nom de réservation : **Webserver**
   - Type de réservation : **Les deux**
10. Dans le volet Ajouter une adresse IPv4, cliquez sur **Enregistrement DNS**, entrez les valeurs suivantes, puis cliquez sur **OK** :
    - Nom de l'unité : **Webserver**
    - Zone de recherche directe : **adatum.com**
    - Serveur principal de recherche directe : **LON-DC1.adatum.com**
11. Dans la zone déroulante **Affichage actuel**, cliquez sur **Adresse IP**.
12. Cliquez avec le bouton droit sur l'entrée avec l'adresse IP 172.16.0.10, puis cliquez sur **Créer une réservation DHCP**.
13. Cliquez de nouveau sur l'entrée avec le bouton droit, puis cliquez sur **Créer un enregistrement d'hôte DNS**.
14. Sur LON-DC1, ouvrez la console DHCP, développez successivement **IPv4** et **Étendue (172.16.0.0) Adatum**, puis cliquez sur **Réservations**. Assurez-vous que la réservation de serveur Web pour 172.16.0.10 s'affiche.
15. Ouvrez la console DNS, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**. Assurez-vous qu'un enregistrement d'hôte s'affiche pour le serveur Web.

Résultats : À l'issue de cet exercice, vous aurez installé IPAM et configuré IPAM avec des objets de stratégie de groupe en relation avec IPAM, la découverte de serveurs d'administration d'IP, des serveurs gérés, une nouvelle étendue DHCP, des blocs d'adresses IP, des adresses IP, des réservations DHCP et des enregistrements DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Pour préparer le module suivant

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-SVR2** et **22412B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2 : Implémentation des services de fichiers avancés

Atelier pratique A : Implémentation des services de fichiers avancés

Exercice 1 : Configuration du stockage iSCSI

▶ Tâche 1 : Installer la fonctionnalité de cible iSCSI

1. Ouvrez une session sur LON-DC1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **Serveur cible iSCSI**, puis cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Une fois l'installation terminée, cliquez sur **Fermer**.

▶ Tâche 2 : Configurer les cibles iSCSI

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**.
2. Dans le volet Services de fichiers et de stockage, cliquez sur **iSCSI**.
3. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
4. Dans l'Assistant Nouveau disque virtuel iSCSI, sur la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur le lecteur **C**, puis sur **Suivant**.
5. Sur la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone de texte **Nom**, saisissez **iSCSIDisk1**, puis cliquez sur **Suivant**.
6. Sur la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone de texte **Taille**, saisissez **5**, assurez-vous que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
7. Sur la page **Affecter la cible iSCSI**, cliquez sur **Nouvelle cible iSCSI**, puis cliquez sur **Suivant**.
8. Sur la page **Indiquer le nom de la cible**, dans la zone **Nom**, saisissez **LON-DC1**, puis cliquez sur **Suivant**.
9. Sur la page **Indiquer les serveurs d'accès**, cliquez sur **Ajouter**.
10. Dans la boîte de dialogue **Sélectionnez une méthode pour identifier l'initiateur**, cliquez sur **Entrer une valeur pour le type sélectionné**, dans la zone de liste déroulante **Type**, cliquez sur **Adresse IP**, dans la zone de texte **Valeur**, saisissez **172.16.0.22**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Sur la page **Indiquer les serveurs d'accès**, cliquez sur **Ajouter**.
12. Dans la boîte de dialogue **Sélectionnez une méthode pour identifier l'initiateur**, cliquez sur **Entrer une valeur pour le type sélectionné**, dans la zone de liste déroulante **Type**, cliquez sur **Adresse IP**, dans la zone de texte **Valeur**, saisissez **131.107.0.2**, puis cliquez sur **OK**.
13. Sur la page **Indiquer les serveurs d'accès**, cliquez sur **Suivant**.
14. Sur la page **Activer l'authentification**, cliquez sur **Suivant**.
15. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
16. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
17. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
18. Dans l'Assistant Nouveau disque virtuel iSCSI, sur la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur le lecteur **C**, puis sur **Suivant**.
19. Sur la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone **Nom**, saisissez **iSCSIDisk2**, puis cliquez sur **Suivant**.
20. Sur la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la case **Taille**, saisissez **5**, assurez-vous que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
21. Sur la page **Affecter la cible iSCSI**, cliquez sur **lon-dc1**, puis cliquez sur **Suivant**.
22. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
23. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
24. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
25. Dans l'Assistant Nouveau disque virtuel iSCSI, sur la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur le lecteur **C**, puis sur **Suivant**.
26. Sur la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone de texte **Nom**, saisissez **iSCSIDisk3**, puis cliquez sur **Suivant**.
27. Sur la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone de texte **Taille**, saisissez **5**, assurez-vous que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
28. Sur la page **Affecter la cible iSCSI**, cliquez sur **lon-dc1**, puis cliquez sur **Suivant**.
29. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
30. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
31. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
32. Dans l'Assistant Nouveau disque virtuel iSCSI, sur la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur le lecteur **C**, puis sur **Suivant**.
33. Sur la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone de texte **Nom**, saisissez **iSCSIDisk4**, puis cliquez sur **Suivant**.
34. Sur la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone de texte **Taille**, saisissez **5**, assurez-vous que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
35. Sur la page **Affecter la cible iSCSI**, cliquez sur **lon-dc1**, puis cliquez sur **Suivant**.
36. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

37. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
38. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
39. Dans l'Assistant Nouveau disque virtuel iSCSI, sur la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur le lecteur **C**, puis sur **Suivant**.
40. Sur la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone de texte **Nom**, saisissez **iSCSIDisk5**, puis cliquez sur **Suivant**.
41. Sur la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone de texte **Taille**, saisissez **5**, assurez-vous que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
42. Sur la page **Affecter la cible iSCSI**, cliquez sur **lon-dc1**, puis cliquez sur **Suivant**.
43. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
44. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

▶ Tâche 3 : Configurer les services MPIO

1. Ouvrez une session sur LON-SVR2 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante **Outils**, cliquez sur **Routage et accès distant**.
3. Attendez que l'**Assistant Activation de DirectAccess** s'affiche.
4. Dans l'Assistant Activation de DirectAccess, cliquez sur **Annuler** puis, dans la boîte de dialogue **Confirmation**, cliquez sur **OK**.
5. Cliquez avec le bouton droit sur **LON-SVR2**, puis cliquez sur **Désactiver le routage et l'accès à distance**. Cliquez sur **Oui**, puis fermez la console Routage et accès distant.

Remarque : Normalement, vous ne désactivez pas Routage et accès distant (RRAS) avant de configurer la fonctionnalité MPIO (Multipath input/output). Vous le faites ici en raison de la configuration requise pour l'atelier pratique.

6. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
7. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
9. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
10. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
11. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **MPIO (Multipath I/O)**, puis sur **Suivant**.
12. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Une fois l'installation terminée, cliquez sur **Fermer**.
14. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante **Outils**, sélectionnez **Initiateur iSCSI**.
15. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.

16. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, dans l'onglet **Cibles**, dans la zone **Cible**, saisissez **LON-DC1**, puis cliquez sur **Connexion rapide**.
17. Dans la zone **Connexion rapide**, cliquez sur **Terminer**.
18. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : Initiateur iSCSI**.
19. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante **Outils**, cliquez sur **MPIO**.
20. Dans la boîte de dialogue **Propriétés de : MPIO**, cliquez sur l'onglet **Découvrir plusieurs chemins**.
21. Sous l'onglet **Découvrir plusieurs chemins**, activez la case à cocher **Ajouter la prise en charge des périphériques iSCSI**, puis cliquez sur **Ajouter**. Lorsque vous êtes invité à redémarrer l'ordinateur, cliquez sur **Oui**.
22. Lorsque l'ordinateur a redémarré, ouvrez une session sur LON-SVR2 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
23. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante **Outils**, cliquez sur **MPIO**.
24. Dans la boîte de dialogue **Propriétés MPIO**, dans l'onglet **Propriétés de : MPIO**, notez que **ID du matériel de périphérique MSFT2005iSCSIBusType_0x9** supplémentaire est ajouté à la liste.
25. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : MPIO**.

▶ Tâche 4 : Se connecter aux cibles iSCSI et les configurer

1. Sur LON-SVR2, dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante **Outils**, cliquez sur **Initiateur iSCSI**.
2. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, dans l'onglet **Cibles**, cliquez sur **Déconnexion**.
3. Dans la boîte de dialogue **Déconnecter toutes les sessions**, cliquez sur **Oui**.
4. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, dans l'onglet **Cibles**, cliquez sur **Connexion**.
5. Dans la fenêtre Connexion à la cible, cliquez sur **Activer la prise en charge de plusieurs chemins d'accès**, vérifiez que la case à cocher **Ajoutez cette connexion à la liste des cibles favorites** est activée, puis cliquez sur le bouton **Avancé**.
6. Dans la boîte de dialogue **Paramètres avancés**, dans l'onglet **Général**, remplacez la valeur **Par défaut** de **Adaptateur local** par **Initiateur Microsoft iSCSI**. Dans la liste déroulante **IP de l'initiateur**, cliquez sur **172.16.0.22** et, dans la liste déroulante **IP du portail cible**, cliquez sur **172.16.0.10 / 3260**.
7. Dans la boîte de dialogue **Paramètres avancés**, cliquez sur **OK**.
8. Dans la fenêtre Connexion à la cible, cliquez sur **OK**.
9. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, dans l'onglet **Cibles**, cliquez sur **Connexion**.
10. Dans la fenêtre Connexion à la cible, cliquez sur **Activer la prise en charge de plusieurs chemins d'accès**, vérifiez que la case à cocher **Ajoutez cette connexion à la liste des cibles favorites** est activée, puis cliquez sur le bouton **Avancé**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la boîte de dialogue **Paramètres avancés**, dans l'onglet **Général**, remplacez la valeur **Par défaut** de **Adaptateur local** par **Initiateur Microsoft iSCSI**. Dans la liste déroulante **IP de l'initiateur**, sélectionnez **131.107.0.2** et, dans la liste déroulante **IP du portail cible**, sélectionnez **131.107.0.1 / 3260**.
12. Dans la boîte de dialogue **Paramètres avancés**, cliquez sur **OK**.
13. Dans la fenêtre Connexion à la cible, cliquez sur **OK**.
14. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, cliquez sur l'onglet **Volumes et périphériques**.
15. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, dans l'onglet **Volumes et périphériques**, cliquez sur **Configuration automatique**.
16. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, cliquez sur l'onglet **Cibles**.
17. Dans la liste **Cibles**, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target**, puis cliquez sur **Périphériques**.
18. Dans la boîte de dialogue **Périphériques**, cliquez sur **MPIO**.
19. Vérifiez que **Répétition alternée** est sélectionné dans **Stratégie d'équilibrage de charge**. Sous **Ce périphérique possède les chemins d'accès suivants**, notez que deux chemins d'accès sont répertoriés. Sélectionnez le premier chemin d'accès, puis cliquez sur **Détails**.
20. Notez l'adresse IP des portails **Source** et **Cible**, puis cliquez sur **OK**.
21. Sélectionnez le second chemin d'accès, puis cliquez sur **Détails**.
22. Vérifiez que l'adresse IP source est celle de la deuxième carte réseau, puis cliquez sur **OK**.
23. Cliquez sur **OK** pour fermer la boîte de dialogue **Détails du périphérique**.
24. Cliquez sur **OK** pour fermer la boîte de dialogue **Périphériques**.
25. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : Initiateur iSCSI**.

Résultats : À la fin de cet exercice, vous aurez configuré les cibles iSCSI et vous serez connecté à ces cibles.

Exercice 2 : Configuration de l'infrastructure de classification des fichiers

▶ Tâche 1 : Créer une propriété de classification pour la documentation d'entreprise

1. Sur LON-SVR1, dans le coin supérieur droit du Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestionnaire de ressources du serveur de fichiers**.
2. Dans la fenêtre du **Gestionnaire de ressources du serveur de fichiers**, développez **Gestion de la classification**, sélectionnez puis cliquez avec le bouton droit sur **Propriétés de classification**, puis cliquez sur **Créer une propriété locale**.
3. Dans la fenêtre Créer la propriété de classification locale, dans la zone de texte **Nom**, saisissez **Corporate Documentation**. Dans la zone de liste déroulante **Type de propriété**, vérifiez que **Oui/Non** est sélectionné, puis cliquez sur **OK**.
4. Laissez le Gestionnaire de ressources du serveur de fichiers ouvert.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer une règle de classification pour la documentation d'entreprise

1. Dans le Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**, cliquez sur **Règles de classification** puis, dans le volet Actions, cliquez sur **Créer une règle de classification**.
2. Dans la fenêtre Créer une règle de classification, sous l'onglet **Général,** dans la zone de texte **Nom de la règle**, saisissez **Corporate Documents Rule**, puis assurez-vous que la case à cocher **Activée** est sélectionnée.
3. Cliquez sur l'onglet **Portée**, puis sur **Ajouter**.
4. Dans la fenêtre Rechercher un dossier, développez **Allfiles (E:)**, développez **Labfiles**, cliquez sur **Corporate Documentation**, puis sur **OK**.
5. Dans la fenêtre Créer une règle de classification, sous l'onglet **Classification,** dans la zone de liste déroulante **Méthode de classification**, cliquez sur **Classificateur de dossiers**. Dans la zone de liste déroulante **Propriété-Choisissez une propriété à attribuer aux fichiers**, cliquez sur **Corporate Documentation** puis, dans la zone de liste déroulante **Propriété-Spécifiez une valeur**, cliquez sur **Oui**.
6. Cliquez sur l'onglet **Type d'évaluation**, cliquez sur **Réévaluer les valeurs de propriété existantes**, assurez-vous que la case d'option **Agréger les valeurs** est sélectionnée, puis cliquez sur **OK**.
7. Dans le Gestionnaire de ressources du serveur de fichiers, dans le volet Actions, cliquez sur **Exécuter la classification avec toutes les règles maintenant**.
8. Dans la fenêtre Exécuter la classification, sélectionnez la case d'option **Attendre la fin de la classification,** puis cliquez sur **OK**.
9. Examinez le Rapport de classification automatique qui s'affiche dans Windows® Internet Explorer® et vérifiez que le rapport affiche le même nombre de fichiers classés que dans le dossier Documentation d'entreprise.
10. Fermez Internet Explorer, mais laissez la console du Gestionnaire de ressources du serveur de fichiers ouverte.

▶ Tâche 3 : Créer une règle de classification s'appliquant à un dossier partagé

1. Dans la console du Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**, cliquez avec le bouton droit sur **Propriétés de classification**, puis cliquez sur **Créer une propriété locale**.
2. Dans la fenêtre Créer la propriété de classification locale**,** dans la zone de texte **Nom**, saisissez **Expiration date**. Dans la zone de liste déroulante **Type de propriété**, assurez-vous que **Date-heure** est sélectionné, puis cliquez sur **OK**.
3. Dans le Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**, cliquez sur **Règles de classification** puis, dans le volet Actions, cliquez sur **Créer une règle de classification**.
4. Dans la fenêtre Créer une règle de classification, sous l'onglet **Général,** dans la zone de texte **Nom de la règle**, saisissez **Expiration Rule** et vérifiez que la case à cocher **Activée** est sélectionnée.
5. Cliquez sur l'onglet **Portée**, puis sur **Ajouter**.
6. Dans la fenêtre Rechercher un dossier, développez **Allfiles (E:)**, développez **Labfiles**, cliquez sur **Corporate Documentation**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Cliquez sur l'onglet **Classification**. Dans la zone de liste déroulante **Méthode de classification,** cliquez sur **Classificateur de dossiers** puis, dans la zone de liste déroulante **Propriété-Choisissez une propriété à attribuer aux fichiers,** cliquez sur **Expiration Date**.
8. Cliquez sur l'onglet **Type d'évaluation** . Cliquez sur **Réévaluer les valeurs de propriété existantes**, vérifiez que la case d'option **Agréger les valeurs** est sélectionnée, puis cliquez sur **OK**.
9. Dans la console du Gestionnaire de ressources du serveur de fichiers, dans le volet Actions, cliquez sur **Exécuter la classification avec toutes les règles maintenant**.
10. Dans la fenêtre Exécuter la classification, sélectionnez la case d'option **Attendre la fin de la classification**, puis cliquez sur **OK**.
11. Examinez le Rapport de classification automatique qui s'affiche dans Windows Internet Explorer et vérifiez que le rapport affiche le même nombre de fichiers classés que dans le dossier Documentation d'entreprise.
12. Fermez Internet Explorer, mais laissez la console du Gestionnaire de ressources du serveur de fichiers ouverte.

▶ Tâche 4 : Créer une tâche de gestion de fichiers pour l'expiration des documents d'entreprise

1. Dans le Gestionnaire de ressources du serveur de fichiers, sélectionnez puis cliquez avec le bouton droit sur **Tâches de gestion de fichiers**, puis cliquez sur **Créer une tâche de gestion de fichiers**.
2. Dans la fenêtre Créer une tâche de gestion de fichiers, sous l'onglet **Général**, dans la zone de texte **Nom de la tâche,** saisissez **Expired Corporate Documents**, puis assurez-vous que la case à cocher **Activer** est sélectionnée.
3. Cliquez sur l'onglet **Portée**, puis sur **Ajouter**.
4. Dans la fenêtre Rechercher un dossier, cliquez sur **E:\Labfiles\Corporate Documentation**, puis cliquez sur **OK**.
5. Dans la fenêtre Créer une tâche de gestion de fichiers, sous l'onglet **Action**, dans la zone de liste déroulante **Type**, assurez-vous que **Expiration de fichier** est sélectionné, puis dans la zone **Répertoire d'expiration**, saisissez **E:\Labfiles\Expired**.
6. Cliquez sur l'onglet **Notification**, puis sur **Ajouter**.
7. Dans la fenêtre Ajouter une notification, sous l'onglet **Journal des événements**, activez la case à cocher **Envoyer un avertissement au journal des événements**, puis cliquez sur **OK**.
8. Cliquez sur l'onglet **Condition**, activez la case à cocher **Nombre de jours depuis la dernière modification au fichier**, puis dans la même ligne, remplacez la valeur par défaut de 0 par **1**.

 **Remarque :** Cette valeur est fournie aux fins de l'atelier pratique uniquement. Dans un scénario réel, la valeur serait de 365 jours ou plus, selon la stratégie de chaque société.

9. Cliquez sur l'onglet **Planification**, vérifiez que la case d'option **Toutes les semaines** est sélectionnée, activez la case à cocher **dimanche**, puis cliquez sur **OK**.
10. Laissez le Gestionnaire de ressources du serveur de fichiers ouvert.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Vérifier que les documents d'entreprise sont expirés

1. Dans le Gestionnaire de ressources du serveur de fichiers, cliquez sur **Tâches de gestion de fichiers**, cliquez avec le bouton droit sur **Documents d'entreprise expirés**, puis cliquez sur **Exécuter maintenant une tâche de gestion de fichiers**.
2. Dans la fenêtre Exécuter une tâche de gestion de fichiers, cliquez sur **Attendre la fin de l'exécution de la tâche**, puis cliquez sur **OK**.
3. Examinez le Rapport de tâche de gestion de fichiers qui s'affiche dans Windows Internet Explorer et vérifiez que le rapport affiche le même nombre de fichiers classés que dans le dossier Documentation d'entreprise.
4. Dans le gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Observateur d'événements**.
5. Dans la console de l'Observateur d'événements, développez **Journaux Windows**, puis cliquez sur **Application**.
6. Examinez les événements portant les numéros **908** et **909**. Notez que 908 – FSRM a démarré une tâche de gestion de fichiers et que 909 – FSRM a terminé une tâche de gestion de fichiers.

Résultats : Après avoir terminé cet exercice, vous aurez configuré une infrastructure de classification des fichiers de sorte que la version la plus récente de la documentation est toujours à la disposition des utilisateurs.

▶ Pour préparer l'atelier suivant

Une fois l'atelier pratique terminé, rétablissez la configuration de 22412B-LON-SVR2. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-SVR2**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.

   Laissez tous les autres ordinateurs virtuels en fonctionnement pour l'atelier suivant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Implémentation de la fonctionnalité BranchCache

Exercice 1 : Configuration des serveurs du siège social pour la fonctionnalité BranchCache

▶ Tâche 1 : Configurer LON-DC1 pour utiliser Windows BranchCache

1. Sur LON-DC1, cliquez sur l'icône Gestionnaire de serveur dans la barre des tâches.
2. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (installés)**, développez **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **BranchCache pour fichiers réseau**, puis cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Cliquez sur **Fermer**, puis fermez le Gestionnaire de serveur.
10. Placez votre pointeur dans le coin inférieur droit de l'écran et cliquez sur **Rechercher**. Dans la zone de texte **Rechercher**, saisissez **gpedit.msc**, puis appuyez sur Entrée.
11. Dans la console de l'Éditeur de stratégie de groupe locale, dans le volet de navigation, sous **Configuration ordinateur**, développez **Modèles d'administration**, développez **Réseau**, puis cliquez sur **Serveur Lanman**.
12. Dans **le** volet des résultats du serveur Lanman, dans la liste **Paramètre**, cliquez avec le bouton droit sur **Publication de hachages pour BranchCache**, puis sur **Modifier**.
13. Dans la boîte de dialogue **Publication de hachages pour BranchCache**, cliquez sur **Activé**. Dans la liste **Actions de la publication de hachages**, activez la case à cocher **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**, puis cliquez sur **OK**.

▶ Tâche 2 : Simuler une liaison lente avec la succursale

1. Dans la console de l'Éditeur de stratégie de groupe locale, dans le volet de navigation, sous **Configuration Ordinateur**, développez **Paramètres Windows**, cliquez avec le bouton droit sur **QoS basée sur la stratégie**, puis cliquez sur **Créer une nouvelle stratégie**.
2. Dans l'Assistant QoS basée sur la stratégie, sur la page **Créer une stratégie de QoS**, dans la zone de texte **Nom de la stratégie**, saisissez **Limiter à 100 Kbits/s** et activez la case à cocher **Spécifier le taux d'accélération en sortie**. Dans la zone de texte **Spécifier le taux d'accélération en sortie**, saisissez **100**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Sur la page **Cette stratégie de QoS s'applique à**, cliquez sur **Suivant**.
4. Sur la page **Spécifiez les adresses IP source et de destination**, cliquez sur **Suivant**.
5. Sur la page **Spécifiez le protocole et les numéros de port**, cliquez sur **Terminer**.
6. Fermez l'Éditeur de stratégie de groupe locale.

▶ Tâche 3 : Activer un partage de fichiers pour BranchCache

1. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
2. Dans l'Explorateur de fichiers, naviguez jusqu'au Disque local (**C:)**.
3. Dans la fenêtre du Disque local (**C:**), dans le menu, cliquez sur l'onglet **Accueil**, puis sur **Nouveau dossier**.
4. Saisissez **Partage** et appuyez sur Entrée.
5. Cliquez avec le bouton droit sur **Partage**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de : Partage**, sous l'onglet **Partage**, cliquez sur **Partage avancé**.
7. Activez la case à cocher **Partager ce dossier**, puis cliquez sur **Mise en cache**.
8. Dans la boîte de dialogue **Paramètres hors connexion**, activez la case à cocher **Activer BranchCache**, puis cliquez sur **OK**.
9. Dans la boîte de dialogue **Partage avancé**, cliquez sur **OK**.
10. Dans la boîte de dialogue **Propriétés de : Partage**, cliquez sur **Fermer**.
11. Placez votre pointeur dans le coin inférieur droit de l'écran et cliquez sur **Rechercher**. Dans la zone de texte **Rechercher**, saisissez **cmd**, puis appuyez sur Entrée.
12. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Copy C:\windows\system32\mspaint.exe c:\partage
```

13. Fermez la fenêtre d'invite de commandes.
14. Fermez l'Explorateur de fichiers.

▶ Tâche 4 : Configurer les règles de pare-feu des clients pour BranchCache

1. Sur LON-DC1, cliquez sur l'icône Gestionnaire de serveur dans la barre des tâches.
2. Dans le Gestionnaire de serveur, dans la barre de menus, cliquez sur **Outils** puis, dans la zone de liste déroulante **Outils**, cliquez sur **Gestion des stratégies de groupe**.
3. Dans Gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
4. Dans l'Éditeur de gestion des stratégies de groupe, dans le volet de navigation, naviguez jusqu'à **Configuration ordinateur**, développez **Stratégies**, développez **Paramètres Windows**, développez **Paramètres de sécurité**, puis développez **Pare-feu Windows avec fonctions avancées de sécurité**.
5. Dans Pare-feu Windows avec fonctions avancées de sécurité, dans le volet de navigation, développez **Pare-feu Windows avec fonctions avancées de sécurité**, puis cliquez sur **Règles de trafic entrant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans l'Éditeur de gestion des stratégies de groupe, dans le menu **Action**, cliquez sur **Nouvelle règle**.
7. Dans l'Assistant Nouvelle règle de trafic entrant, sur la page **Type de règle**, cliquez sur **Prédéfinie**, cliquez sur **BranchCache – Extraction du contenu (utilise HTTP)**, puis cliquez sur **Suivant**.
8. Sur la page **Règles prédéfinies**, cliquez sur **Suivant**.
9. Sur la page **Action**, cliquez sur **Terminer** pour créer la règle de trafic entrant du pare-feu.
10. Dans l'Éditeur de gestion des stratégies de groupe, dans le volet de navigation, cliquez sur **Règles de trafic entrant** puis, toujours dans l'Éditeur de gestion des stratégies de groupe, sur le menu **Action**, cliquez sur **Nouvelle règle**.
11. Sur la page **Type de règle**, cliquez sur **Prédéfinie**, cliquez sur **BranchCache – Découverte d'homologue (utilise WSD)**, puis cliquez sur **Suivant**.
12. Sur la page **Règles prédéfinies**, cliquez sur **Suivant**.
13. Sur la page la page **Action**, cliquez sur **Terminer**.
14. Fermez les consoles Éditeur de gestion des stratégies de groupe et Gestion des stratégies de groupe.

Résultats : À la fin de cet exercice, vous aurez déployé BranchCache, configuré une liaison lente et activé BranchCache sur un partage de fichiers.

Exercice 2 : Configuration des serveurs de succursale pour la fonctionnalité BranchCache

▶ Tâche 1 : Installer la fonctionnalité BranchCache sur LON-SVR1

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, puis activez la case à cocher **BranchCache pour fichiers réseau**.
6. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **BranchCache**, puis cliquez sur **Suivant**.
8. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Cliquez sur Fermer.

▶ Tâche 2 : Mettre en marche le serveur hôte BranchCache

1. Basculez vers LON-DC1.
2. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante **Outils**, cliquez sur **Utilisateurs et ordinateurs Active Directory**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Adatum.com**, placez le pointeur sur **Nouveau** et sélectionnez **Unité d'organisation**.
4. Dans la fenêtre Nouvel Objet - Unité d'organisation, saisissez **BranchCacheHost**, puis cliquez sur **OK**.
5. Développez **Adatum.com**, puis cliquez sur **Computers**.
6. Cliquez sur **LON-SVR1**, puis faites-le glisser dans **BranchCacheHost**.
7. Cliquez sur **Oui** pour fermer l'avertissement concernant le déplacement d'objets.
8. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.
9. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante **Outils**, cliquez sur **Gestion des stratégies de groupe**.
10. Dans Gestion des stratégies de groupe, sous **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **BranchCacheHost** et cliquez sur **Bloquer l'héritage**.
11. Sur LON-DC1, fermez toutes les fenêtres actives.
12. Redémarrez LON-SVR1 et ouvrez une session en tant que **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
13. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
14. Dans la fenêtre Windows PowerShell, saisissez l'applet de commande suivante et appuyez sur Entrée :

```
Enable-BCHostedServer
-RegisterSCP
```

15. Dans la fenêtre Windows PowerShell, saisissez l'applet de commande suivante et appuyez sur Entrée :

```
Get-BCStatus
```

16. Assurez-vous que la fonctionnalité BranchCache est activée et en cours d'exécution.
17. Fermez Windows PowerShell.

Résultats : À la fin de cet exercice, vous aurez activé le serveur BranchCache dans la succursale.

Exercice 3 : Configuration des ordinateurs clients pour la fonctionnalité BranchCache

▶ Tâche 1 : Configurer les ordinateurs client pour utiliser BranchCache en mode de cache hébergé

1. Sur LON-DC1, cliquez sur l'icône Gestionnaire de serveur dans la barre des tâches.
2. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils**, puis dans la liste déroulante **Outils**, sélectionnez **Gestion de stratégies de groupe**.
3. Dans le volet de navigation de la console Gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans le volet de navigation de l'Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez successivement **Stratégies**, **Modèles d'administration** et **Réseau**, puis cliquez sur **BranchCache**.
5. Dans le volet des résultats de BranchCache, dans la liste **Paramètre**, cliquez avec le bouton droit sur **Activer BranchCache**, puis cliquez sur **Modifier**.
6. Dans la boîte de dialogue **Activer BranchCache**, cliquez sur **Activé**, puis sur **OK**.
7. Dans le volet des résultats de BranchCache, dans la liste **Paramètre**, cliquez avec le bouton droit sur **Activer la découverte automatique du cache hébergé par le point de connexion de service**, puis cliquez sur **Modifier**.
8. Dans la boîte de dialogue **Activer la découverte automatique du cache hébergé par le point de connexion de service**, cliquez sur **Activé**, puis sur **OK**.
9. Dans le volet des résultats de BranchCache, dans la liste **Paramètre**, cliquez avec le bouton droit sur **Configurer BranchCache pour les fichiers réseau**, puis cliquez sur **Modifier**.
10. Dans la boîte de dialogue **Configurez BranchCache pour les fichiers réseau**, cliquez sur **Activé**. Dans la zone de texte **Entrer le temps de réponse maximum du réseau aller-retour (millisecondes) avant que la mise en cache ne commence**, saisissez **0**, puis cliquez sur **OK**. Ce paramètre est obligatoire pour simuler l'accès depuis une succursale, mais n'est pas généralement requis.
11. Fermez l'Éditeur de gestion des stratégies de groupe.
12. Fermez la console GPMC.
13. Démarrez **22412B-LON-CL1** et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
14. Sur l'écran Accueil, placez votre pointeur dans le coin inférieur droit de l'écran et cliquez sur **Rechercher**. Dans la zone de texte **Rechercher**, saisissez **cmd**, puis appuyez sur Entrée.
15. Dans la fenêtre d'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

16. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
netsh branchcache show status all
```

17. Vérifiez que BranchCache est **Activé** avec l'état **En cours d'exécution** et que les options de la Stratégie de groupe sont appliquées. Si l'état est défini sur **Arrêté**, répétez les étapes 15 et 16.
18. Démarrez **22412B-LON-CL2**, et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
19. Sur l'écran Accueil, placez votre pointeur dans le coin inférieur droit de l'écran et cliquez sur **Rechercher**. Dans la zone de texte **Rechercher**, saisissez **power**, puis appuyez sur Entrée.
20. Dans la fenêtre Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

21. Dans la fenêtre Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
netsh branchcache show status all
```

22. Vérifiez que BranchCache est **Activé** avec l'état **En cours d'exécution** et que les options de la Stratégie de groupe sont appliquées. Si l'état est défini sur **Arrêté**, répétez les étapes 20 et 21.

Résultats : À la fin de cet exercice, vous aurez configuré les ordinateurs client pour BranchCache.

Exercice 4 : Contrôle de la fonctionnalité BranchCache

▶ Tâche 1 : Configurer l'Analyseur de performances sur LON-SVR1

1. Basculez vers LON-SVR1.
2. Dans la barre de menus du Gestionnaire de serveur, cliquez sur **Outils**, puis dans la zone de liste déroulante **Outils**, cliquez sur **Analyseur de performance**.
3. Dans la console de l'Analyseur de performances, dans le volet de navigation, sous **Outils d'analyse**, cliquez sur **Analyseur de performances**.
4. Dans le volet des résultats de l'Analyseur de performances, cliquez sur l'icône Supprimer (touche de suppression).
5. Dans le volet des résultats de l'Analyseur de performances, cliquez sur l'icône Ajouter (Ctrl+N).
6. Dans la boîte de dialogue **Ajouter des compteurs**, sous **Choisir les compteurs sur**, cliquez sur **BranchCache**, cliquez sur **Ajouter**, puis cliquez sur **OK**.
7. Sur le bouton **Modifier le type de graphique**, sélectionnez **Rapport**.

▶ Tâche 2 : Configurer les statistiques de performances sur LON-CL1

1. Basculez vers LON-CL1.
2. Placez votre pointeur dans le coin inférieur droit de l'écran et cliquez sur **Rechercher**. Dans la zone de texte **Rechercher**, saisissez **perfmon**, puis appuyez sur Entrée.
3. Dans la console de l'Analyseur de performances, dans le volet de navigation, sous **Outils d'analyse**, cliquez sur **Analyseur de performances**.
4. Dans le volet des résultats de l'Analyseur de performances, cliquez sur l'icône Supprimer (touche de suppression).
5. Dans le volet des résultats de l'Analyseur de performances, cliquez sur l'icône Ajouter (Ctrl+N).
6. Dans la boîte de dialogue **Ajouter des compteurs**, sous **Choisir les compteurs sur**, cliquez sur **BranchCache**, cliquez sur **Ajouter**, puis cliquez sur **OK**.
7. Définissez le type de graphique sur **Rapport**. Remarquez que la valeur de toutes les statistiques de performances est zéro.

▶ Tâche 3 : Configurer les statistiques de performances sur LON-CL2

1. Basculez vers LON-CL2.
2. Placez votre pointeur dans le coin inférieur droit de l'écran et cliquez sur **Rechercher**. Dans la zone de texte **Rechercher**, saisissez **perfmon**, puis appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la console de l'Analyseur de performances, dans le volet de navigation, sous **Outils d'analyse**, cliquez sur **Analyseur de performances**.
4. Dans le volet des résultats de l'Analyseur de performances, cliquez sur l'icône Supprimer (touche de suppression).
5. Dans le volet des résultats de l'Analyseur de performances, cliquez sur l'icône Ajouter (Ctrl+N).
6. Dans la boîte de dialogue **Ajouter des compteurs**, sous **Choisir les compteurs sur**, cliquez sur **BranchCache**, cliquez sur **Ajouter**, puis cliquez sur **OK**.
7. Définissez le type de graphique sur **Rapport**. Remarquez que la valeur de toutes les statistiques de performances est zéro.

▶ Tâche 4 : Tester la fonctionnalité BranchCache en mode de cache hébergé

1. Basculez vers LON-CL1.
2. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
3. Dans la barre d'adresse de l'Explorateur de fichiers, saisissez **LON-DC1.adatum.com\Partage**, puis appuyez sur Entrée.
4. Dans la fenêtre Partage, dans la liste **Nom**, cliquez avec le bouton droit sur **mspaint.exe**, puis cliquez sur **Copier**.
5. Dans la fenêtre Partage, cliquez sur **Réduire**.
6. Cliquez avec le bouton droit n'importe où sur le Bureau, puis cliquez sur **Coller**.
7. Lisez les statistiques de performance sur LON-CL1. Ce fichier a été récupéré depuis LON-DC1 (récupération : octets du serveur). Après que le fichier a été mis en cache localement, il a été transféré au cache hébergé. (récupération : octets traités).
8. Basculez vers LON-CL2.
9. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
10. Dans la barre d'adresse de l'Explorateur de fichiers, saisissez **\\LON-DC1.adatum.com\Partage**, puis appuyez sur Entrée.
11. Dans la fenêtre Partage, dans la liste **Nom**, cliquez avec le bouton droit sur **mspaint.exe**, puis cliquez sur **Copier**.
12. Dans la fenêtre **Partage**, cliquez sur **Réduire**.
13. Cliquez avec le bouton droit n'importe où sur le **Bureau**, puis cliquez sur **Coller**.
14. Lisez les statistiques de performance sur **LON**-CL2. Ce fichier a été obtenu à partir du cache hébergé (récupération : octets du cache).
15. Lisez les statistiques de performance sur LON-SVR1. Ce serveur a fourni les données en mémoire cache aux clients (cache hébergé : offres de segments de fichiers effectuées).

Résultats : À la fin de cet exercice, vous aurez vérifié que BranchCache fonctionne comme prévu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-CL1** et **22412B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3 : Implémentation du contrôle d'accès dynamique

Atelier pratique : Implémentation du contrôle d'accès dynamique

Exercice 1 : Planification de l'implémentation du contrôle d'accès dynamique

▶ Tâche 1 : Planifier le déploiement du contrôle d'accès dynamique

Selon le scénario, décrivez comment vous concevrez le Contrôle d'accès dynamique pour remplir les conditions du contrôle d'accès.

Le scénario requiert les éléments suivants :

1. Les dossiers qui appartiennent à l'équipe de recherche doivent être accessibles et modifiables uniquement par les employés appartenant à l'équipe de recherche.
2. Les fichiers désignés par Haut doivent être accessibles uniquement aux gestionnaires.
3. Les gestionnaires doivent accéder aux dossiers confidentiels uniquement à partir des stations de travail appartenant au groupe de sécurité ManagersWKS.

Vous pouvez répondre à ces exigences en implémentant des revendications, des propriétés de ressource et des classifications des fichiers, comme suit :

1. Créez les revendications appropriées pour les utilisateurs et les périphériques. La revendication d'utilisateur utilise le département sécurité comme attribut source ; et la revendication de périphérique utilise la description comme attribut source.
2. Configurez la propriété de ressource pour le service de recherche.
3. Configurez les règles d'accès centralisées et les stratégies d'accès centralisé de manière à protéger les ressources. En même temps, vous devez configurer la classification des fichiers pour les documents confidentiels.
4. Appliquez une stratégie d'accès centralisée aux dossiers dans lesquels les fichiers destinés aux services de recherche et aux gestionnaires sont situés.
5. Pour résoudre le problème des utilisateurs recevant des messages d'erreur, vous devez implémenter l'assistance en cas d'accès refusé.

▶ Tâche 2 : Préparer AD DS pour prendre en charge le contrôle d'accès dynamique

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
3. Dans la boîte de dialogue **Nouvel objet – Unité d'organisation** de la zone **Nom**, saisissez **Test**, puis cliquez sur **OK**.
4. Cliquez sur le conteneur **Computers**.
5. Appuyez et maintenez la touche Ctrl enfoncée, cliquez avec le bouton droit sur les ordinateurs **LON-SVR1**, **LON-CL1**, et **LON-CL2**, puis cliquez sur **Déplacer**.

6. Dans la fenêtre Déplacer, cliquez sur **Test**, puis cliquez sur **OK**.
7. Fermez la console Utilisateurs et ordinateurs Active Directory.
8. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
9. Développez **Forêt : Adatum.com**, puis **Domaines**, puis **Adatum.com**.
10. Cliquez avec le bouton droit sur l'unité d'organisation (UO) **Managers**, puis cliquez sur **Bloquer l'héritage**. Faites cela pour enlever le paramètre d'héritage de bloc utilisé dans un module postérieur du cours.
11. Cliquez sur le conteneur **Objets de stratégie de groupe**.
12. Dans le volet des résultats, cliquez avec le bouton droit sur **Default Domain Controllers Policy**, puis cliquez sur **Modifier**.
13. Dans l'Éditeur de gestion des stratégies de groupe, dans Configuration ordinateur, développez **Stratégies**, **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local**, **Système** et cliquez sur **KDC**.
14. Dans le volet droit, double-cliquez sur **Prise en charge du contrôleur de domaine Kerberos pour les revendications, l'authentification...**.
15. Dans la fenêtre de prise en charge KDC pour les revendications, l'authentification composée et le blindage Kerberos, sélectionnez **Activé**, dans la section **Options**, cliquez sur la liste déroulante, sélectionnez **Pris en charge**, puis cliquez sur **OK**.
16. Fermez la console de l'Éditeur de gestion des stratégies de groupe et la Console de gestion des stratégies de groupe.
17. Dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
18. À l'invite de Windows PowerShell, saisissez **gpupdate /force** et appuyez sur Entrée. Après les mises à jour de la stratégie de groupe, fermez la fenêtre Windows PowerShell.
19. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
20. Développez **Adatum.com**, cliquez avec le bouton droit sur **Users**, cliquez sur **Nouveau**, puis sur **Groupe**.
21. Dans le champ **Nom du groupe**, saisissez **ManagersWKS**, puis cliquez sur **OK**.
22. Cliquez sur l'unité d'organisation **Test**.
23. Cliquez avec le bouton droit sur **LON-CL1**, puis cliquez sur **Propriétés**.
24. Cliquez sur l'onglet **Membre de,** puis sur **Ajouter**.
25. Dans la fenêtre Sélectionner des groupes, saisissez **ManagersWKS**, cliquez sur **Vérifier les noms**, cliquez sur **OK**, puis cliquez de nouveau sur **OK**.
26. Cliquez sur l'unité d'organisation **Managers**.
27. Cliquez avec le bouton droit sur **Aidan Delaney**, puis cliquez sur **Propriétés**.
28. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Organisation**. Vérifiez que le champ **Department** est rempli avec la valeur **Managers**, puis cliquez sur **Annuler**.
29. Cliquez sur l'unité d'organisation **Research**.
30. Cliquez avec le bouton droit sur **Allie Bellew**, puis cliquez sur **Propriétés**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

31. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Organisation**. Vérifiez que le champ **Department** est rempli avec la valeur **Research**, puis cliquez sur **Annuler**.
32. Fermez la console **Utilisateurs et ordinateurs Active Directory**.

Résultats : Après avoir terminé cet exercice, vous aurez organisé le déploiement du contrôle d'accès dynamique et préparé AD DS pour l'implémentation du contrôle d'accès dynamique.

Exercice 2 : Configuration des revendications d'utilisateurs et de périphériques

▶ Tâche 1 : Examiner les types de revendication par défaut

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**.
3. Dans le volet central, double-cliquez sur **Claim Types**.
4. Vérifiez qu'aucune revendication par défaut n'est définie.
5. Dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Resource Properties**.
6. Examinez les propriétés de ressource par défaut. Notez que toutes les propriétés sont désactivées par défaut.
7. Dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Resource Property Lists**.
8. Dans le volet central, cliquez avec le bouton droit sur **Global Resource Property List** puis cliquez sur **Propriétés**.
9. Dans la boîte de dialogue **Global Resource Property List**, dans la section Propriétés de ressources, examinez les propriétés de ressources disponibles, puis cliquez sur **Annuler**.

▶ Tâche 2 : Configurer des revendications pour des utilisateurs

1. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Claim Types**.
2. Dans le conteneur Types de revendication, dans le volet **Tâches**, cliquez sur **Nouveau**, puis sur **Type de revendication**.
3. Dans la fenêtre Créer un type de revendication, dans la section Attribut source, sélectionnez **department**.
4. Dans la zone de texte **Nom complet**, saisissez le **Service de société**.
5. Activez les cases à cocher **Utilisateur** et **Ordinateur**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer des revendications pour des périphériques

1. Dans le Centre d'administration Active Directory, dans le volet Tâches, cliquez sur **Nouveau**, puis sélectionnez **Type de revendication**.
2. Dans la fenêtre Créer un type de revendication, dans la section Attribut de source, cliquez sur **description**.
3. Désactivez la case à cocher **Utilisateur**, activez la case à cocher **Ordinateur**, puis cliquez sur **OK**.

Résultats : Après avoir terminé cet exercice, vous aurez examiné les types de revendication par défaut, configuré les revendications d'utilisateurs et les revendications de périphériques.

Exercice 3 : Configuration des définitions des propriétés de ressource

▶ Tâche 1 : Configurer les définitions des propriétés de ressource

1. Dans le Centre d'administration Active Directory, cliquez sur **Contrôle d'accès dynamique**.
2. Dans le volet central, double-cliquez sur **Resource Properties**.
3. Dans la liste de Propriétés de ressource, cliquez avec le bouton droit sur **Department**, puis cliquez sur **Activer**.
4. Dans la liste de Propriétés de ressource, cliquez avec le bouton droit sur **Confidentiality**, puis cliquez sur **Activer**.
5. Dans la liste des Propriétés de ressource globale, vérifiez que les propriétés **Department** et **Confidentiality** sont activées.
6. Double-cliquez sur **Department**.
7. Allez à la section Valeurs suggérées, puis cliquez sur **Ajouter**.
8. Dans la fenêtre Ajouter une valeur suggérée, dans les zones de texte **Valeur** et **Nom complet**, saisissez **Research**, puis cliquez deux fois sur **OK**.
9. Cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Resource Property Lists**.
10. Dans le volet central, double-cliquez sur **Global Resource Property List**, en veillant à ce que les propriétés **Department** et **Confidentiality** soit affichées, puis cliquez sur **Annuler**. Si elles ne s'affichent pas, cliquez sur **Ajouter**, ajoutez ces deux propriétés, puis cliquez sur **OK**.
11. Fermez le Centre d'administration Active Directory.

▶ Tâche 2 : Classer les fichiers

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
2. Dans la console du Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**.
3. Cliquez avec le bouton droit sur **Propriétés de classification**, puis cliquez sur **Actualiser**.
4. Vérifiez que les propriétés **Confidentiality** et **Department** sont dans la liste.
5. Cliquez sur **Règles de classification**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans le volet Actions, cliquez sur **Créer une règle de classification**.
7. Dans la fenêtre Créer une règle de classification, pour le **Nom de la règle**, saisissez **Définir la confidentialité**.
8. Cliquez sur l'onglet **Portée**, puis sur **Ajouter**.
9. Dans la boîte de dialogue **Rechercher un dossier**, développez **Disque local (C:)**, cliquez sur le dossier **Docs**, puis cliquez sur **OK**.
10. Cliquez sur l'onglet **Classification**.
11. Assurez-vous que les paramètres suivants sont définis, puis cliquez sur **Configurer** :
    - Méthode de classification : **Classifieur de contenus**
    - Propriété : **Confidentiality**
    - Valeur : **High**
12. Dans la boîte de dialogue **Paramètres de classification,** cliquez sur la liste déroulante **Expression régulière,** puis cliquez sur **Chaîne**.
13. Dans le champ **Expression** (à côté du mot Chaîne) saisissez **secret**, puis cliquez sur **OK**.
14. Cliquez sur l'onglet **Type d'évaluation**, sélectionnez **Réévaluer les valeurs de propriété existantes**, cliquez sur **Remplacer la valeur existante**, puis cliquez sur **OK**.
15. Dans le Gestionnaire de ressources du serveur de fichiers, dans le volet Actions, cliquez sur **Exécuter la classification avec toutes les règles maintenant**.
16. Cliquez sur **Attendre la fin de la classification**, puis cliquez sur **OK**.
17. Un rapport s'affiche une fois la classification terminée. Vérifiez que les deux fichiers ont été classés. Vous pouvez le confirmer dans la section Totaux des rapports.
18. Fermez le rapport.
19. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers®.
20. Dans la fenêtre de l'Explorateur de fichiers, développez le lecteur **C**, puis le dossier **Docs**.
21. Dans le dossier Docs, cliquez avec le bouton droit sur **Doc1.txt**, cliquez sur **Propriétés**, puis sur l'onglet **Classification**. Vérifiez que la confidentialité est définie sur **High**.
22. Répétez l'étape 21 sur les fichiers **Doc2.txt** et **Doc3.txt**. Doc2.txt devrait avoir la même confidentialité que Doc1.txt, alors que Doc3.txt ne devrait avoir aucune valeur. C'est parce que seuls Doc1 et Doc2 contiennent le mot secret dans leur contenu.

▶ Tâche 3 : Affecter des propriétés à un dossier

1. Sur LON-SVR1, ouvrez une fenêtre de l'Explorateur de fichiers et accédez au lecteur **C**.
2. Dans le lecteur C, cliquez avec le bouton droit sur le dossier **Research**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Classification**, puis sur **Department**. Dans la section **Valeur**, cliquez sur **Research**, sur **Appliquer**, puis sur **OK**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré des propriétés de ressource pour des fichiers, classifié des fichiers et attribué des propriétés à un dossier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Configuration des règles d'accès central et des stratégies d'accès centralisées

▶ Tâche 1 : Configurer des règles d'accès centralisé

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Central Access Rules**.
3. Dans le volet Tâches, cliquez sur **Nouveau**, puis sur **Règle d'accès central**.
4. Dans la boîte de dialogue **Créer Règle d'accès central**, dans le champ **Nom**, saisissez **Correspondance de service**.
5. Dans la section Ressources cibles, cliquez sur **Modifier**.
6. Dans la boîte de dialogue **Règle d'accès central**, cliquez sur **Ajouter une condition**.
7. Définissez une condition comme suit : **Ressource-Department-Est égal à-Valeur-Research**, puis cliquez sur **OK**.
8. Dans la section **Autorisations**, cliquez sur **Utiliser les autorisations suivantes en tant qu'autorisations actuelles**.
9. Dans la section **Autorisations**, cliquez sur **Modifier**.
10. Enlevez l'autorisation pour **Administrateurs**.
11. Dans les **Paramètres de sécurité avancés pour Autorisations**, cliquez sur **Ajouter**.
12. Dans **Autorisations pour Autorisations**, cliquez sur **Sélectionnez un principal**.
13. Dans la fenêtre Sélectionner les utilisateurs, Ordinateur, Compte de service ou Groupe, saisissez **Utilisateurs authentifiés**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
14. Dans la section **Autorisations de base**, activez les cases à cocher **Modification**, **Lecture et exécution**, **Lecture** et **Écriture**.
15. Cliquez sur **Ajouter une condition**.
16. Cliquez sur la liste déroulante **Groupe**, puis cliquez sur **Service de société**.
17. Cliquez sur la liste déroulante **Valeur**, puis cliquez sur **Ressource**.
18. Dans la dernière liste déroulante, cliquez sur **Department**.

 **Remarque :** Vous devez avoir cette expression comme résultat : **Utilisateur-Service de société-Est égal à-Ressource-Department**.

19. Cliquez trois fois sur **OK**.
20. Dans le volet Tâches, cliquez sur **Nouveau**, puis sur **Règle d'accès central**.
21. Pour le nom de la règle, saisissez **Accéder aux documents confidentiels**.
22. Dans la section Ressources cibles, cliquez sur **Modifier**.
23. Dans la fenêtre Règle d'accès centralisée, cliquez sur **Ajouter une condition**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

24. Dans la dernière liste déroulante, cliquez sur **High**.

Remarque : Vous devez avoir cette expression comme résultat : **Ressource-Confidentiality-Est égal à-Valeur-High**.

25. Cliquez sur **OK**.
26. Dans la section **Autorisations**, cliquez sur **Utiliser les autorisations suivantes en tant qu'autorisations actuelles**.
27. Dans la section Autorisations, cliquez sur **Modifier**.
28. Enlevez l'autorisation pour **Administrateurs**.
29. Dans les Paramètres de sécurité avancés des Autorisations, cliquez sur **Ajouter**.
30. Dans l'Entrée d'autorisation pour les autorisations, cliquez sur **Sélectionnez un principal**.
31. Dans la fenêtre Sélectionner les utilisateurs, Ordinateur, Compte de service ou Groupe, saisissez **Utilisateurs authentifiés**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
32. Dans la section Autorisations de base, activez les cases à cocher **Modification**, **Lecture et exécution**, **Lecture** et **Écriture**.
33. Cliquez sur **Ajouter une condition**.
34. Définissez la première condition à : Utilisateur-Groupe-Membre de chaque-Valeur-Managers, puis cliquez sur Ajouter une condition.

Remarque : Si vous ne trouvez pas Managers dans la dernière liste déroulante, cliquez sur **Ajouter des éléments**. Puis, dans la fenêtre Sélectionner les utilisateurs, Ordinateur, Compte de service ou Groupe, saisissez **Managers**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK** deux fois.

35. Définissez la deuxième condition à : **Périphérique-Groupe-Membre de chaque-Valeur-ManagersWKS**.

Remarque : Si vous ne trouvez pas ManagersWKS dans la dernière liste déroulante, cliquez sur **Ajouter des éléments**. Puis, dans la fenêtre Sélectionner les utilisateurs, Ordinateur, Compte de service ou Groupe, saisissez **ManagersWKS**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.

36. Cliquez trois fois sur **OK**.

▶ Tâche 2 : Créer une stratégie d'accès centralisé

1. Sur LON-DC1, dans le Centre d'administration Active Directory, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Central Access Policies**.
2. Dans le volet des tâches, cliquez sur **Nouveau**, puis sur **Stratégie d'accès central**.
3. Dans le champ **Nom**, saisissez **Protéger les documents confidentiels**, puis cliquez sur **Ajouter**.
4. Cliquez sur la règle **Accéder aux documents confidentiels**, puis sur **>>**. Ensuite, cliquez deux fois sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans le volet des tâches, cliquez sur **Nouveau**, puis cliquez sur **Stratégie d'accès central**.
6. Dans le champ **Nom**, saisissez **Correspondance de service**, puis cliquez sur **Ajouter**.
7. Cliquez sur la règle **Correspondance de service**, cliquez sur **>>**, puis cliquez deux fois sur **OK**.
8. Fermez le Centre d'administration Active Directory.

▶ Tâche 3 : Publier une stratégie d'accès centralisée à l'aide de la stratégie de groupe

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la Console de gestion des stratégies de groupe, sous **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **Test** et cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
3. Saisissez **Stratégie DAC**, puis cliquez sur **OK**.
4. Cliquez avec le bouton droit sur **Stratégie DAC**, puis cliquez sur **Modifier**.
5. Développez **Configuration ordinateur**, développez **Stratégies**, développez **Paramètres Windows**, développez **Paramètres de sécurité**, développez **Système de fichiers**, cliquez avec le bouton droit sur **Stratégie d'accès centralisée**, puis cliquez sur **Gérer les stratégies d'accès centralisées**.
6. Appuyez et maintenez la touche CTRL enfoncée, puis cliquez deux fois sur **Correspondance de service** et sur **Protéger les documents confidentiels**, cliquez sur **Ajouter**, puis sur **OK**.
7. Fermez l'Éditeur de gestion des stratégies de groupe.
8. Fermez la console Gestion de stratégie de groupe.

▶ Tâche 4 : Appliquer la stratégie d'accès centralisée aux ressources

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. À l'invite de Windows PowerShell, saisissez **gpupdate /force** et appuyez sur Entrée.
3. Fermez Windows PowerShell.
4. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
5. Dans l'Explorateur de fichiers, accédez au lecteur **C**, cliquez avec le bouton droit sur le dossier **Docs**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Sécurité**, puis cliquez sur **Avancé**.
7. Dans la fenêtre **Paramètres de sécurité avancés pour Docs**, cliquez sur l'onglet **Stratégie centralisée**, puis cliquez sur **Modifier**.
8. Dans la liste déroulante, sélectionnez **Protéger les documents confidentiels**, puis cliquez deux fois sur **OK**.
9. Cliquez avec le bouton droit sur le dossier **Research**, puiscliquez sur **Propriétés**.
10. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Sécurité**, puis cliquez sur **Avancé**.
11. Dans la fenêtre **Paramètres de sécurité avancés pour Research**, cliquez sur l'onglet **Stratégie centralisée**, puis cliquez sur **Modifier**.
12. Dans la liste déroulante, cliquez sur **Correspondance de service** puis cliquez deux fois sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Configurer les paramètres d'action corrective en cas d'accès refusé

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans le GPMC, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, puis cliquez sur **Objets de stratégie de groupe**.
3. Cliquez avec le bouton droit sur **Stratégie DAC**, puis cliquez sur **Modifier**.
4. Dans le nœud Configuration ordinateur, développez **Stratégies**, développez **Modèles d'administration**, développez **Système**, puis cliquez sur **Assistance en cas d'accès refusé**.
5. Dans le volet droit, double-cliquez sur **Personnaliser le message pour les erreurs d'accès refusé**.
6. Dans la fenêtre Personnaliser le message des erreurs d'accès refusé, cliquez sur **Activé**.
7. Dans la zone de texte **Afficher le message suivant aux utilisateurs auxquels l'accès est refusé**, saisissez **Votre accès est refusé en raison de la stratégie d'autorisation. Veuillez demander un accès**.
8. Activez la case à cocher **Autoriser les utilisateurs à demander de l'assistance**.
9. Examinez d'autres options, mais n'apportez aucune modification, puis cliquez sur **OK**.
10. Dans le volet droit de l'Éditeur de gestion des stratégies de groupe, double-cliquez sur **Activer l'assistance en cas d'accès refusé pour tous les types de fichiers**.
11. Cliquez sur **Activé**, puis cliquez sur **OK**.
12. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.
13. Basculez vers LON-SVR1 et dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
14. Dans l'interface de ligne de commande Windows PowerShell, saisissez **gpupdate /force**, puis appuyez sur Entrée.

Résultats : Après avoir complété cet exercice, vous aurez configuré des règles d'accès centralisées et des stratégies d'accès centralisé pour le contrôle d'accès dynamique.

Exercice 5 : Validation et mise à jour du contrôle d'accès dynamique

▶ Tâche 1 : Valider la fonctionnalité de contrôle d'accès dynamique

1. Démarrez et connectez-vous à LON-CL1 en tant que **Adatum\April** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur la mosaïque du Bureau, puis à partir de la barre des tâches, cliquez sur l'icône Internet Explorer.
3. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\LON-SVR1\Docs**, puis appuyez sur Entrée.
4. Dans le dossier Docs, essayez d'ouvrir **Doc3**. Vous devriez pouvoir ouvrir ce document. Fermez le Bloc-notes.
5. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\LON-SVR1\Research**, puis appuyez sur Entrée. Vous ne devriez pas pouvoir accéder à ce dossier.
6. Cliquez sur **Demander de l'aide**. Examinez les options pour envoyer un message, puis cliquez sur **Fermer**.

7. Déconnectez-vous de LON-CL1.
8. Connectez-vous sur LON-CL1 en tant que **Adatum\Allie** avec le mot de passe **Pa$$w0rd**.
9. Cliquez sur la mosaïque du Bureau, puis à partir de la barre des tâches, cliquez sur l'icône Internet Explorer.
10. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\LON-SVR1\Research**, puis appuyez sur Entrée.
11. Vérifiez que vous pouvez accéder à ce dossier et ouvrir les documents qui s'y trouvent, parce qu'Allie est membre de l'équipe de recherche.
12. Déconnectez-vous de LON-CL1.
13. Connectez-vous sur LON-CL1 en tant que **Adatum\Aidan** avec le mot de passe **Pa$$w0rd**.
14. Cliquez sur la mosaïque du Bureau, puis à partir de la barre des tâches, cliquez sur l'icône Internet Explorer.
15. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\LON-SVR1\Docs**.
16. Vérifiez que vous pouvez accéder à ce dossier et ouvrir tous les fichiers qui s'y trouvent.
17. Déconnectez-vous de LON-CL1.
18. Démarrez et connectez-vous à LON-CL2 en tant que **Adatum\Aidan** avec le mot de passe **Pa$$w0rd**.
19. Cliquez sur la mosaïque du Bureau, puis à partir de la barre des tâches, cliquez sur l'icône Internet Explorer.
20. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\LON-SVR1\Docs**. Vous ne devriez pas pouvoir consulter Doc1 ou Doc2, parce que LON-CL2 n'est pas autorisé à consulter les documents secrets.

Résultats : Après avoir terminé cet exercice, vous aurez validé la fonctionnalité de contrôle d'accès dynamique.

Exercice 6 : Implémentation de nouvelles stratégies de ressource

▶ Tâche 1 : Configurer le transit pour une stratégie d'accès centralisé

1. Sur LON-DC1, ouvrez Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestion de stratégie de groupe**.
2. Dans la console Gestion des stratégies de groupe, développez **Forest:Adatum.com**, développez **Domaines**, développez **Adatum.com**, puis cliquez sur **objet de Stratégie de groupe**.
3. Cliquez avec le bouton droit sur **Stratégie DAC**, puis cliquez sur **Modifier**.
4. Dans l'Éditeur de gestion des stratégies de groupe, développez **Configuration ordinateur**, développez **Stratégies**, développez **Paramètres Windows**, développez **Paramètres de sécurité**, développez **Configuration avancée de la stratégie d'audit**, développez **Stratégies d'audit**, puis cliquez sur **Accès à l'objet**.
5. Double-cliquez sur **Auditer la stratégie d'accès centralisée intermédiaire**, activez les trois cases à cocher, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Double-cliquez sur **Auditer le système de fichiers**, activez les trois cases à cocher, puis cliquez sur **OK**.
7. Fermez l'Éditeur de gestion des stratégies de groupe et la console de Gestion des stratégies de groupe.

▶ Tâche 2 : Configurer des autorisations intermédiaires

1. Sur LON-DC1, ouvrez le Gestionnaire de serveur, cliquez sur Outils, puis cliquez sur Centre d'administration Active Directory.
2. Dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**.
3. Double-cliquez sur **Central Access Rules**.
4. Cliquez avec le bouton droit sur **Correspondance de service**, puis cliquez sur **Propriétés**.
5. Faites défiler l'écran jusqu'à la section **Autorisations proposées**, cliquez sur **Activer la configuration intermédiaire des autorisations**, puis cliquez sur **Modifier**.
6. Cliquez sur **Utilisateurs authentifiés**, puis cliquez sur **Modifier**.
7. Modifiez la condition par : **Utilisateur-Service de société-Est égal à-Valeur-Marketing**, puis cliquez sur **OK**.
8. Cliquez sur **OK** deux fois supplémentaires pour fermer toutes les fenêtres.
9. Basculez vers LON-SVR1.
10. Dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
11. Sur Windows PowerShell, saisissez **gpupdate /force**, puis appuyez sur Entrée.
12. Fermez la fenêtre Windows PowerShell.

▶ Tâche 3 : Vérifier le transit

1. Connectez-vous sur LON-CL1 en tant que **Adatum\Adam** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur la mosaïque du Bureau, puis à partir de la barre des tâches, cliquez sur l'icône Internet Explorer.
3. Dans la barre d'adresses de l'Explorateur de fichiers, cliquez sur l'icône jaune, puis saisissez **\\LON-SVR1\Research**.
4. Essayez d'ouvrir le dossier Research et les fichiers qu'il contient. Vous ne pourrez pas l'ouvrir.
5. Basculez vers LON-SVR1.
6. Ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Observateur d'événements**.
7. Développez **Journaux Windows**, puis accédez à **Sécurité**.
8. Recherchez les événements avec l'ID **4818**.
9. Lisez le contenu de ces journaux.

▶ Tâche 4 : Utiliser des autorisations effectives pour tester le contrôle d'accès dynamique

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
2. Dans la fenêtre de l'Explorateur de fichiers, accédez à **C:\Research**, cliquez avec le bouton droit sur **Research**, puis cliquez sur **Propriétés**.

3. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Sécurité**, cliquez sur **Avancé**, puis cliquez sur **Accès effectif**.
4. Cliquez sur **Sélectionner un utilisateur**.
5. Dans la fenêtre Sélectionner des utilisateurs, Ordinateur, Compte de service ou Groupe**,** saisissez **April**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
6. Cliquez sur **Afficher l'accès effectif**.
7. Vérifiez les résultats. L'utilisateur April ne devrait pas avoir accès à ce dossier.
8. Cliquez sur **Inclure une revendication utilisateur**.
9. Dans la liste déroulante, cliquez sur **Service de société**.
10. Dans la zone de texte **Valeur**, saisissez **Research**.
11. Cliquez sur **Afficher l'accès effectif**. April devrait maintenant y avoir accès.
12. Fermez toutes les fenêtres.

Résultats : À la fin de cet exercice, vous aurez implémenté de nouvelles stratégies de ressource.

▶ Pour préparer le module suivant

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-CL1** et **22412B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4 : Implémentation des déploiements de services de domaine Active Directory distribués

Atelier pratique : Implémentation des déploiements AD DS distribués

Exercice 1 : Implémenter des domaines enfants dans AD DS

▶ Tâche 1 : Configurer le DNS (Domain Name System) pour la délégation de domaine

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le Gestionnaire DNS, développez **LON-DC1**, et **Zones de recherche directes**, cliquez puis cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvelle délégation**.
3. Dans l'Assistant de nouvelle délégation, cliquez sur **Suivant**, dans la zone de texte **Domaine délégué** texte**,** saisissez **N/A**, puis cliquez sur **Suivant**.
4. Dans la zone **Serveurs de noms,** cliquez sur **Ajouter**.
5. Dans la zone de texte **Nom de domaine complet (FQDN) du serveur**, saisissez **TOR-DC1.adatum.com**, effacez **<Cliquer ici pour ajouter une adresse IP>**, et saisissez **172.16.0.25**, puis cliquez sur **OK**.
6. Dans la fenêtre Nommer les serveurs**,** cliquez sur **Suivant**.
7. Dans la fenêtre L'Assistant de Nouvelle délégation est terminé, cliquez sur **Terminer**.

▶ Tâche 2 : Installer un contrôleur de domaine dans un domaine enfant

1. Sur TOR-DC1, dans le Gestionnaire de serveurs, cliquez sur **Gérer**, et dans la zone de liste déroulante, cliquez sur **Ajouter des rôles et fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, confirmez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination** vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné et que **TOR-DC1.Adatum.com** est mis en surbrillance, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**cliquez sur **Services AD DS**.
6. Sur la page **Ajouter les fonctionnalités requises pour Services AD DS ?,** cliquez sur **Ajouter des fonctionnalités**.
7. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Services de domaine Active Directory** cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**. (Cette opération peut prendre quelques minutes.)
11. Quand les binaires des services de domaine Active Directory® (AD DS) sont installés, cliquez sur le lien bleu **Promouvoir ce serveur en contrôleur de domaine**.
12. Dans la fenêtre de configuration de déploiement, cliquez sur **Ajouter un nouveau domaine à une forêt existante**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

13. Vérifiez que **Sélectionnez le type du domaine** est défini en tant que **Domaine enfant**, et que **Nom du domaine parent** est défini en tant que **Adatum.com**. Dans la zone de texte **Nouveau nom de domaine**, saisissez **NA**.
14. Confirmez que **Fournir les informations d'identification pour effectuer cette opération** sont listés est défini à **ADATUM\Administrateur (utilisateur actuel)**, puis cliquez sur **Suivant**.

Remarque : Si ce n'est pas le cas, utilisez le bouton **Modifier** pour saisir les informations d'identification **Adatum\administrateur**, et le mot de passe **Pa$$w0rd**.

15. Dans la fenêtre d'options de contrôleur de domaine, assurez-vous que **Niveau fonctionnel du domaine** est défini sur **Windows Server 2012**.
16. Assurez-vous que les cases à cocher **Serveur DNS (Domain Name System)** et **Catalogue global (GC)** sont sélectionnées.
17. Confirmez que **Nom du site :** est défini comme **Default-First-Site-Name**.
18. Sous **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**, saisissez **Pa$$w0rd** dans les deux zones de texte, puis cliquez sur **Suivant**.
19. Sur la page **Options DNS**, cliquez sur **Suivant**.
20. Sur la page **Options supplémentaires**, cliquez sur **Suivant**.
21. Sur la page **Chemins d'accès**, cliquez sur **Suivant**.
22. Sur la page **Examiner les options**, cliquez sur **Suivant**.
23. Sur la page **Vérification de la configuration requise**, confirmez qu'il n'y a aucun problème, puis cliquez sur **Installer**.

▶ Tâche 3 : Vérifier la configuration d'approbation par défaut

1. Ouvrez une session TOR-DC1 en tant que **NA\Administrateur** à l'aide du mot de passe **Pa$$w0rd**.
2. Quand le Gestionnaire de serveurs s'ouvre, cliquez sur **Serveur local**.
3. Vérifiez que le **Pare-feu Windows** indique **Domaine : Actif**. Si ce n'est pas le cas, à côté de **Connexion au réseau local**, cliquez sur **172.16.0.25, Compatible IPv6**. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Désactiver**. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Activer**. La connexion au réseau local devrait à présent indiquer **Adatum.com**.
4. Dans le Gestionnaire de serveurs, dans le menu **Outils**, cliquez sur **Domaines et approbations Active Directory**.
5. Dans la console Domaines et approbations Active Directory, développez **Adatum.com**, cliquez avec le bouton droit sur **NA.Adatum.com**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de : NA.Adatum.com** cliquez sur l'onglet **Approbations**, dans la case **Domaine approuvé par ce domaine (approbations sortantes),** cliquez sur **Adatum.com**, puis sur **Propriétés**.
7. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur **Valider**, puis sur **Oui, valider l'approbation entrante**.
8. Dans la zone de texte **Nom d'utilisateur,** saisissez **administrateur**, et dans la zone de texte **Mot de passe** saisissez **Pa$$w0rd**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Quand le message **La relation d'approbation a été validée. Elle est en place et activée** s'affiche, cliquez sur **OK**.

Remarque : Si vous recevez un message disant que l'approbation ne peut pas être validée, ou que la vérification de canal sécurisé (SC) a échoué, assurez-vous que vous avez terminé l'étape 2, et attendez au moins 10 à 15 minutes avant de réessayer. Vous pouvez continuer les travaux pratiques et revenir ultérieurement à cette étape.

10. Cliquez deux fois sur **OK** pour fermer la boîte de dialogue **Propriétés de : Adatum.com**.

Résultats : À la fin de cet exercice, vous aurez implémenté des domaines enfants dans AD DS.

Exercice 2 : Implémenter des approbations de forêt

▶ Tâche 1 : Configurer les zones de stub pour la résolution de nom DNS

1. Dans le Gestionnaire de serveurs, sur LON-DC1, cliquez sur le menu **Outils** puis dans le menu déroulant, cliquez sur **DNS**.
2. Dans le volet d'arborescence de DNS, développez **LON-DC1**, sélectionnez **Zones de recherche directe** et cliquez dessus avec le bouton droit, puis cliquez sur **Nouvelle zone**.
3. Dans l'Assistant de nouvelle zone, cliquez sur **Suivant**.
4. Sur la page **Type de zone** cliquez sur **Zone de stub**, puis sur **Suivant**.
5. Dans la page **Étendue de la zone de réplication de Active Directory**, cliquez sur **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : Adatum.com**, puis cliquez sur **Suivant**.
6. Dans la zone de texte **Nom de la zone :** saisissez **treyresearch.net**, puis cliquez sur **Suivant**.
7. Sur la page **Serveurs DNS maîtres,** cliquez sur **<Cliquez ici pour ajouter une adresse IP ou un nom DNS>**, saisissez **172.16.10.10**, cliquez sur l'espace libre, puis sur **Suivant**.
8. Sur la page **Fin de l'Assistant Nouvelle Zone** cliquez sur **Suivant**, puis sur **Terminer**.
9. Sélectionnez puis cliquez avec le bouton droit sur la nouvelle zone de stub **treyresearch.net**, puis cliquez sur **Transfert à partir du maître**.
10. Cliquez avec le bouton droit sur **treyresearch.net**, puis cliquez sur **Actualiser**.
11. Confirmez que la zone de stub de treyresearch.net contient des enregistrements.
12. Basculez vers MUN-DC1.
13. Dans le Gestionnaire de serveurs, cliquez sur le menu **Outils** et dans le menu déroulant, cliquez sur **DNS**.
14. Dans le volet d'arborescence, développez **MUN-DC1.TreyResearch.net si nécessaire**, sélectionnez puis cliquez avec le bouton droit sur **Zones de recherche directes**, puis cliquez sur **Nouvelle zone**.
15. Dans l'Assistant de nouvelle zone, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Sur la page **Type de zone** cliquez sur **Zone de stub**, puis sur **Suivant**.
17. Dans la page **Étendue de la zone de réplication de Active Directory**, cliquez sur **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : TreyResearch.net**, puis cliquez sur **Suivant**.
18. Dans la zone de texte **Nom de la zone :** saisissez **adatum.com**, puis cliquez sur **Suivant**.
19. Sur la page **Serveurs DNS maîtres,** effacez le champ **<Cliquez ici pour ajouter une adresse IP ou un nom DNS>**, et saisissez **172.16.0.10**, cliquez sur l'espace libre, puis sur **Suivant**.
20. Sur la page **Fin de l'Assistant Nouvelle Zone** cliquez sur **Suivant**, puis sur **Terminer**.
21. Sélectionnez puis cliquez avec le bouton droit sur la nouvelle zone de stub **adatum.com**, puis cliquez sur **Transfert à partir du maître**.
22. Cliquez avec le bouton droit sur **adatum.com**, puis cliquez sur **Actualiser**.
23. Confirmez que la zone de stub de adatum.com contient des enregistrements.
24. Fermez le Gestionnaire DNS.

▶ Tâche 2 : Configurer une approbation de forêt avec authentification sélective

1. Sur LON-DC1, dans le menu **Outils** cliquez sur **Domaines et approbations Active Directory**.
2. Dans la fenêtre de la console de gestion **Domaines et approbations Active Directory** cliquez avec le bouton droit sur **Adatum.com**, puis sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de : Adatum.com** cliquez sur l'onglet **Approbations** puis cliquez sur **Nouvelle approbation**.
4. Sur la page **Assistant Nouvelle approbation**, cliquez sur **Suivant**.
5. Dans la zone de texte **Nom** saisissez **treyresearch.net**, puis cliquez sur **Suivant**.
6. Sur la page **Type d'approbation** cliquez sur **Approbation de forêt**, puis cliquez sur **Suivant**.
7. Sur la page **Direction de l'approbation** cliquez sur **Sens unique : en sortie**, puis cliquez sur **Suivant**.
8. Sur la page **Sens de l'approbation** cliquez sur **Ce domaine et le domaine spécifié**, puis cliquez sur **Suivant**.
9. Sur la page **Nom d'utilisateur**, saisissez le nom d'utilisateur **Administrateur** et le mot de passe **Pa$$w0rd** dans les cases appropriées, puis cliquez sur **Suivant**.
10. Sur la page **Niveau d'authentification d'approbations sortantes - Forêt locale**, cliquez sur **Authentification sélective**, puis cliquez sur **Suivant**.
11. Sur la page **Fin de la sélection des approbations**, cliquez sur **Suivant**.
12. Sur la page **Fin de la création de l'approbation**, cliquez sur **Suivant**.
13. Sur la page **Confirmer l'approbation sortante**, cliquez sur **Suivant**.
14. Cliquez sur **Terminer**.
15. Dans la boîte de dialogue **Propriétés de : Adatum.com,** cliquez sur l'onglet **Approbations**.
16. Sur l'onglet **Approbations,** sous **Domaines approuvés par ce domaine (approbations sortantes)**, cliquez sur **TreyResearch.net** puis sur **Propriétés**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

17. Dans la boîte de dialogue **Propriétés de : TreyResearch.net,** cliquez sur **Valider**.
18. Examinez le message qui s'affiche : **La relation d'approbation a été validée. Elle est en place et activée**.
19. Cliquez sur **OK**, puis sur **Non** lorsque vous y êtes invité.
20. Cliquez sur **OK** à deux reprises.
21. Fermez la fenêtre Domaines et approbations Active Directory.

▶ Tâche 3 : Configurer un serveur pour l'authentification sélective.

1. Sur LON-DC1,dans le Gestionnaire de serveurs, dans le menu **Outils** cliquez sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans la console Utilisateurs et ordinateurs Active Directory, dans le menu **Affichage** cliquez sur **Fonctionnalités avancées**.
3. Développez **Adatum.com**, puis cliquez sur **Computers**.
4. Cliquez avec le bouton droit sur **LON-SVR1**, puis sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de : LON-SVR1** cliquez sur **Sécurité** puis sur **Ajouter**.
6. Sur la page **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, cliquez sur **Emplacements**.
7. Cliquez sur **TreyResearch.net**, puis sur **OK**.
8. Dans la zone de texte **Entrez les noms des objets à sélectionner (exemples),** saisissez **IT (TREYRESEARCH\IT)**, puis cliquez sur **Vérifier les noms**. Si vous êtes invité à entrer les informations d'identification, saisissez **treyresearch\administrateur** avec le mot de passe **Pa$$w0rd**, puis cliquez sur **OK**.
9. Sur la page **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes** cliquez sur **OK.**
10. Dans la fenêtre **Propriétés de : LON-SVR1**, vérifiez que **IT (TREYRESEARCH\IT)** est mis en surbrillance, sélectionnez la case à cocher **Autoriser** sur la même ligne que **Autorisation d'authentifier** puis cliquez sur **OK**.
11. Basculez vers LON-SVR1.
12. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers®.
13. Dans l'Explorateur de fichiers, cliquez sur **Disque local (C)**.
14. Cliquez avec le bouton droit dans le volet d'informations, cliquez sur **Nouveau**, puis sur **Dossier**.
15. Dans la zone de texte **Nom**, saisissez **Données IT**, et appuyez sur la touche Entrée.
16. Cliquez avec le bouton droit sur **Données IT**, pointez sur **Partager avec**, puis cliquez sur **Des personnes spécifiques**.
17. Dans la boîte de dialogue **Partage de fichiers** saisissez **IT (TREYRESEARCH\IT)**, puis cliquez sur **Ajouter**.
18. Cliquez sur **Lecture**, puis sur **Lecture/écriture**. Cliquez sur **Partager**, puis sur **Terminé**.
19. Déconnectez-vous de MUN-DC1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

20. Ouvrez une session sur **MUN-DC1** en tant que **TREYRESEARCH\Alice** à l'aide du mot de passe **Pa$$w0rd**.
21. Placez votre curseur dans l'angle inférieur droit du Bureau, et quand le volet Windows s'affiche, cliquez sur **Rechercher**.
22. Dans la zone de texte **Recherche** saisissez **Données II**, puis appuyez sur la touche Entrée. Le dossier s'ouvre.

Résultats : À la fin de cet exercice, vous aurez implémenté des approbations de forêt.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-TOR-DC1**, **22412B-MUN-DC1**, et **22412B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5 : Implémentation des sites et de la réplication Active Directory Domain Services (AD DS)

Atelier pratique : Implémentation des sites et de la réplication AD DS

Exercice 1 : Modification du site par défaut

▶ Tâche 1 : Installer le contrôleur de domaine de Toronto

1. Sur TOR-DC1, dans le Gestionnaire de serveurs, cliquez sur **Gérer**, et dans la zone de liste déroulante, cliquez sur **Ajouter des rôles et fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, confirmez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné et que **TOR-DC1.Adatum.com** est mis en surbrillance, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Services AD DS**.
6. Sur la page **Ajouter les fonctionnalités requises pour Services AD DS ?** cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Services de domaine Active Directory** cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**. (Cette opération peut prendre quelques minutes.)
10. Quand les binaires AD DS sont installés, cliquez sur le lien bleu **Promouvoir ce serveur en contrôleur de domaine**.
11. Dans la fenêtre de configuration de déploiement, cliquez sur **Ajouter un contrôleur de domaine à un domaine existant**, puis cliquez sur **Suivant**.
12. Dans la fenêtre d'options du contrôleur de domaine, assurez-vous que les cases à cocher **Serveur DNS (Domain Name System)** et **Catalogue global (GC)** sont sélectionnées.
13. Confirmez que **Nom du site :** est défini en tant que **Default-First-Site-Name**, puis dans **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**, saisir **Pa$$w0rd** dans les cases **Mot de passe** et **Confirmer le mot de passe**. Cliquez sur **Suivant**.
14. Sur la page **Options DNS**, cliquez sur **Suivant**.
15. Sur la page **Options supplémentaires**, cliquez sur **Suivant**.
16. Dans la fenêtre chemins d'accès, cliquez sur **Suivant**.
17. Dans la fenêtre **Examiner les options**, cliquez sur **Suivant**.
18. Dans la fenêtre **Vérification de la configuration requise**, confirmez qu'il n'y a aucun problème, puis cliquez sur **Installer**. Le serveur redémarrera automatiquement.
19. Après le redémarrage de TOR-DC1, connectez-vous en tant qu' **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Renommer le site par défaut

1. Si nécessaire, sur LON-DC1, ouvrez la console du gestionnaire de serveur.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
3. Dans Sites et les services Active Directory, dans le volet de navigation, développez **Sites**.
4. Cliquez avec le bouton droit sur **Default-First-Site-Name**, puis cliquez sur **Renommer**.
5. Tapez **LondonHQ**, puis appuyez sur Entrer.
6. Développez **LondonHQ**, développez le dossier **Servers**, puis vérifiez que chacun des deux sites **LON-DC1** et **TOR-DC1** appartiennent à **LondonHQ**.

▶ Tâche 3 : Configurez les sous-réseaux IP associés au site par défaut

1. S'il y a lieu, sur LON-DC1, ouvrez la console du Gestionnaire de serveur, puis ouvrez **Site et services Active Directory**.
2. Dans la console Sites et services Active Directory, dans le volet de navigation, développez **Sites**, puis cliquez sur le dossier **Subnets**.
3. Cliquez avec le bouton droit sur **Subnets**, puis cliquez sur **Nouveau sous-réseau**.
4. Dans la boîte de dialogue **Nouvel objet – Sous-réseau** dans **Préfixe**, tapez **172.16.0.0/24**.
5. Dans la catégorie **Sélectionnez un objet du site pour ce préfixe**, cliquez sur **LondonHQ**, puis cliquez sur **OK**.

Résultats : Après avoir complété cet exercice, vous aurez reconfiguré le site par défaut et assigné les sous-réseaux IP au site.

Exercice 2 : Création de sites et de sous-réseaux supplémentaires

▶ Tâche 1 : Créez les sites AS DS pour Toronto

1. Si nécessaire, sur LON-DC1, ouvrez la console du Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Sites et les services Active Directory**.
2. Dans la console Sites et services Active Directory, dans le volet de navigation, cliquez avec le bouton droit sur **Sites**, puis cliquez sur **Nouveau site**.
3. Dans la boîte de dialogue **Nouvel objet - Site**, à côté de **Nom**, tapez **Toronto**.
4. Dans **Sélectionnez un objet lien de sites pour ce site**, sélectionnez **DEFAULTIPSITELINK**, puis cliquez sur **OK**.
5. Dans la **boîte de dialogue AD DS** cliquez sur **OK**. Le site de Toronto s'affiche dans le volet de navigation.
6. Dans la console Sites et services Active Directory, dans le volet de navigation, cliquez avec le bouton droit sur **Sites**, puis cliquez sur **Nouveau site**.
7. Dans la boîte de dialogue **Nouvel objet - Site**, à côté de **Nom**, tapez **TestSite**.
8. Dans **Sélectionnez un objet lien de sites pour ce site**, sélectionnez **DEFAULTIPSITELINK**, puis cliquez sur **OK**. Le TestSite s'affiche dans le volet de navigation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créez les sous-réseaux IP associés avec les sites de Toronto

1. Si nécessaire, sur LON-DC1, ouvrez la console du Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Sites et les services Active Directory**.
2. Dans la console Sites et services Active Directory, dans le volet de navigation, développez **Sites**, puis cliquez sur le dossier **Subnets**.
3. Cliquez avec le bouton droit sur **Subnets**, puis cliquez sur **Nouveau sous-réseau**.
4. Dans la boîte de dialogue **Nouvel objet – Sous-réseau** dans **Préfixe**, tapez **172.16.1.0/24**.
5. Dans la catégorie **Sélectionnez un objet du site pour ce préfixe**, cliquez sur **Toronto**, puis cliquez sur **OK**.
6. Cliquez avec le bouton droit sur **Subnets**, puis cliquez sur **Nouveau sous-réseau**.
7. Dans la boîte de dialogue **Nouvel objet – Sous-réseau** dans **Préfixe**, tapez **172.16.100.0/24**.
8. Dans la catégorie **Sélectionnez un objet du site pour ce préfixe**, cliquez sur **TestSite**, puis cliquez sur **OK**.
9. Dans le volet de navigation, cliquez sur le dossier **Sous-réseau**. Vérifiez dans le volet d'informations que les trois sous-réseaux sont créés et associés avec leur site approprié.

Résultats : À la fin de cet exercice, vous aurez créé deux sites supplémentaires représentant les adresses IP de sous-réseau situées à Toronto.

Exercice 3 : Configuration de la réplication AD DS

▶ Tâche 1 : Configurez les liens de sites entre les sites Active Directory DS

1. Si nécessaire, sur LON-DC1, ouvrez la console du Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Sites et les services Active Directory**.
2. Dans la console Sites et services Active Directory, dans le volet de navigation, développez **Sites**, développez **Inter-Site Transports**, et cliquez sur le dossier **IP**.
3. Cliquez avec le bouton droit sur **IP**, puis cliquez sur **Lien vers un nouveau site**.
4. Dans la boîte de dialogue **Nouvel objet - Lien du site**, à côté de **Nom**, tapez **TOR-TEST**.
5. Sous **Sites absents de ce lien de sites**, appuyez sur CTRL de votre clavier et cliquez sur **Toronto**, puis cliquez sur **TestSite**,, puis cliquez sur **Ajouter**, et enfin cliquez sur **OK**.
6. Cliquez avec le bouton droit sur **TOR-TEST**, puis cliquez sur **Propriétés**.
7. Dans la boîte de dialogue **Propriétés de : TOR-TEST**, cliquez sur **Modifier la planification**.
8. Dans la boîte de dialogue **Planification pour TOR-TEST**, mettez en surbrillance la plage entre **lundi 9h et au vendredi 15h**.
9. Cliquez sur **Réplication non disponible**, puis cliquez sur **OK**.
10. Cliquez sur **OK** pour fermer **Propriétés de : TOR-TEST**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Cliquez avec le bouton droit sur **DEFAULTIPSITELINK**, puis cliquez sur **Renommer**.
12. Tapez **LON-TOR** puis appuyez sur Entrer.
13. Cliquez avec le bouton droit sur LON-TOR, puis cliquez sur **Propriétés**.
14. Dans la section **Sites présents dans ce lien de sites**, cliquez sur **TestSite**, puis cliquez sur **Supprimer**.
15. À côté de **Réplication toutes les**, modifiez la valeur en indiquant **60** minutes, puis cliquez sur **OK**.

▶ Tâche 2 : Déplacez TOR-DC1 au site de Toronto

1. Si nécessaire, dans LON-DC1, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans la console Sites et services Active Directory, dans le volet de navigation, développez **Sites**, développez **LondonHQ**, puis développez le dossier **Serveurs**.
3. Cliquez avec le bouton droit sur **TOR-DC1**, puis cliquez sur **Déplacer**.
4. Dans la boîte de dialogue **Déplacer un serveur**, cliquez sur **Toronto**, puis cliquez sur **OK**.
5. Dans le volet de navigation, développez le site de **Toronto**, développez **Servers**, puis cliquez sur **TOR-DC1**.

▶ Tâche 3 : Surveillez la réplication de site AD DS

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
2. À l'invite de commandes Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
Repadmin /kcc
```

   Cette commande recalcule la topologie de réplication entrante pour le serveur.

3. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
Repadmin /showrepl
```

4. Vérifie que la dernière réplication avec TOR-DC1 a été réussie.
5. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
Repadmin /bridgeheads
```

   Cette commande affiche les serveurs tête de pont pour la topologie du site.

6. À l'invite de commandes Windows PowerShell, tapez l'instruction suivante et appuyez sur Entrée :

```
Repadmin /replsummary
```

   Cette commande affiche un résumé des tâches de réplication. Vérifiez qu'aucune erreur n'apparaît.

7. À l'invite de commandes Windows PowerShell, tapez l'instruction suivante et appuyez sur Entrée :

```
DCDiag /test:replications
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Vérifie que tous les tests de connectivité et de réplication ont eu lieu avec succès.
9. Basculez vers TOR-DC1, puis répétez les étapes 1 à 8 pour afficher les informations depuis le point de vue de TOR-DC1. Pour l'étape 4, vérifiez que la dernière réplication avec LON-DC1 a été réussie.

Résultats : À la fin de cet exercice, vous aurez configuré les liens de sites et surveillé la réplication.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-TOR-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6 : Implémentation des services de certificats Active Directory

Atelier pratique A : Déploiement et configuration de la hiérarchie d'autorités de certification

Exercice 1 : Déploiement d'une AC racine autonome

▶ Tâche 1 : Installez le rôle serveur Active Directory® Certificate Services (AD CS) sur un serveur non joint au domaine

1. Connectez-vous à LON-CA1 en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la console Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, sélectionnez **Services de certificats Active Directory**. Lorsque l'Assistant Ajouter des rôles et des fonctionnalités s'affiche, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
9. Sur la page **Sélectionner des services de rôle**, vérifiez que l'option **Autorité de certification** est sélectionnée, puis cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Sur la page **Progression de l'installation**, après l'installation, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
12. Dans l'Assistant de configuration AD CS, sur la page **Informations d'identification**, cliquez sur **Suivant**.
13. Sur la page **Services de rôle**, sélectionnez **Autorité de certification**, puis cliquez sur **Suivant**.
14. Sur la page **Type d'installation**, sélectionnez **Autorité de certification autonome**, puis cliquez sur **Suivant**.
15. Sur la page **Type d'autorité de certification**, vérifiez que l'option **Autorité de certification racine** est sélectionnée, puis cliquez sur **Suivant**.
16. Sur la page **Clé privée**, vérifiez que l'option **Créer une clé privée** est sélectionnée, puis cliquez sur **Suivant**.
17. Sur la page **Chiffrement pour l'autorité de certification**, conservez les sélections par défaut pour CSP et l'algorithme de hachage, mais définissez la **Longueur de la clé** sur **4 096**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Sur la page **Nom de l'autorité de certification**, dans la zone **Nom commun de cette AC**, tapez **AdatumRootCA**, puis cliquez sur **Suivant**.
19. Sur la page **Période de validité**, cliquez sur **Suivant**.
20. Sur la page **Base de données de l'autorité de certification**, cliquez sur **Suivant**.
21. Sur la page **Confirmation**, cliquez sur **Configurer**.
22. Sur la page **Résultats**, cliquez sur **Fermer**.
23. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.

▶ Tâche 2 : Configuration d'un nouvel emplacement de révocation de certificat

1. Sur LON-CA1, dans la console du **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console **certsrv – [Autorité de certification (Local)]**, cliquez avec le bouton droit sur **AdatumRootCA**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de : AdatumRootCA**, cliquez sur l'onglet **Extensions**.
4. Sous l'onglet **Extensions**, dans la liste déroulante **Sélectionner l'extension**, cliquez sur **Points de distribution de liste de révocation des certificats (CDP)**, puis sur le bouton **Ajouter**.
5. Dans la zone de texte **Emplacement**, tapez **http://lon-svr1.adatum.com/CertData/**, dans la zone de liste déroulante **Variable**, cliquez sur **NomAutoritéCertification**, puis sur **Insérer**.
6. Dans la zone de liste déroulante **Variable**, cliquez sur **<SuffixeNomListeRévocationCertificats>**, puis sur **Insérer**.
7. Dans la zone de liste déroulante **Variable**, cliquez sur **ListeRévocationCertificatsDeltaAutorisée**, puis sur **Insérer**.
8. Dans la zone de texte **Emplacement**, placez le curseur à la fin de l'URL, tapez **.crl** et cliquez sur **OK**.
9. Sélectionnez les options suivantes, puis cliquez sur **Appliquer** :
   - **Inclure dans l'extension CDP des certificats émis**
   - **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta**
10. Dans la fenêtre contextuelle Autorité de certification, cliquez sur **Non**.
11. Dans la zone de liste déroulante **Sélectionner l'extension**, cliquez sur **Accès aux informations de l'autorité (AIA)**, puis sur **Ajouter**.
12. Dans la zone de texte **Emplacement**, tapez **http://lon-svr1.adatum.com/CertData/**, dans la zone déroulante **Variable**, cliquez sur **Nom du serveur DNS**, puis sur **Insérer**.
13. Dans la zone de texte **Emplacement**, tapez un caractère de soulignement (_), dans la zone de liste déroulante Variable, cliquez sur **NomAutoritéCertification**, puis sur **Insérer**. Placez le curseur à la fin de l'URL.
14. Dans la zone de liste déroulante Variable, cliquez sur **NomCertificat**, puis sur **Insérer**.
15. Dans la zone de texte **Emplacement**, placez le curseur à la fin de l'URL, tapez **.crt**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**, puis cliquez sur **OK**.
17. Cliquez sur **Oui** pour redémarrer le service d'autorité de certification.
18. Dans la console **Autorité de certification (Local)**, développez **AdatumRootCA**, cliquez avec le bouton droit sur **Certificats révoqués**, pointez sur **Toutes les tâches**, puis cliquez sur **Publier**.
19. Dans la fenêtre Publier la liste de révocation des certificats, cliquez sur **OK**.
20. Cliquez avec le bouton droit sur **AdatumRootCA**, puis cliquez sur **Propriétés**.
21. Dans la boîte de dialogue **Propriétés de : AdatumRootCA**, cliquez sur **Afficher le certificat**.
22. Dans la boîte de dialogue Certificat, cliquez sur l'onglet **Détails**.
23. Sous l'onglet **Détails**, cliquez sur **Copier dans un fichier**.
24. Dans l'Assistant Exportation de certificat, sur la page **Bienvenue dans l'Assistant Exportation du certificat**, cliquez sur **Suivant**.
25. Sur la page **Format du fichier d'exportation**, sélectionnez **X.509 binaire encodé DER (*.cer)**, puis cliquez sur **Suivant**.
26. Sur la page **Fichier à exporter**, cliquez sur **Parcourir**. Dans la zone de texte **Nom du fichier**, tapez **\\lon-svr1\C$** et appuyez sur Entrée.
27. Dans la zone de texte **Nom du fichier**, tapez **RootCA**, cliquez sur **Enregistrer**, puis sur **Suivant**.
28. Cliquez sur **Terminer**, puis sur **OK** à trois reprises.
29. Ouvrez une fenêtre Explorateur Windows® et accédez à **C:\Windows\System32\CertSrv\CertEnroll**.
30. Dans le dossier Cert Enroll, cliquez sur les deux fichiers, cliquez avec le bouton droit sur les fichiers en surbrillance et cliquez sur **Copier**.
31. Dans la barre d'adresses de l'Explorateur Windows, tapez **\\lon-svr1\C$**, puis appuyez sur Entrée.
32. Cliquez avec le bouton droit sur l'espace vide, puis cliquez sur **Coller**.
33. Fermez l'Explorateur Windows.

▶ Tâche 3 : Création d'un enregistrement d'hôte DNS pour LON-CA1 et configuration du partage

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
2. Dans la console de **Gestionnaire DNS**, développez **LON-DC1** et **Zones de recherche directes**, puis cliquez sur **Adatum.com** et cliquez avec le bouton droit sur **Adatum.com** et cliquez sur **Nouvel hôte (A ou AAAA)**
3. Dans la fenêtre **Nouvel hôte**, dans la zone **Nom**, tapez **LON-CA1**
4. Dans la fenêtre Adresse IP, tapez **172.16.0.40**.
5. Cliquez sur **Ajouter un hôte**, puis sur **OK**.
6. Cliquez sur **Terminé**.
7. Fermez le **Gestionnaire DNS**.
8. Basculez vers LON-CA1.
9. Dans le menu**Accueil**, cliquez sur **Panneau de configuration**
10. Dans la fenêtre **Panneau de configuration**, cliquez sur **Afficher l'état et la gestion du réseau**

11. Dans la fenêtre **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de partage avancés**.
12. Sous **Invité ou public (profil actuel)**, sélectionnez l'option **Activer le partage de fichiers et d'imprimantes**.
13. Cliquez sur **Enregistrer les modifications**.

Résultats : À la fin de cet exercice, vous aurez déployé une AC autonome racine.

Exercice 2 : Déploiement d'une AC secondaire d'entreprise

▶ Tâche 1 : Installation et configuration d'AD CS sur LON-SVR1

1. Ouvrez une session sur LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, sélectionnez **Services de certificats Active Directory**.
7. Lorsque l'Assistant Ajouter des rôles et des fonctionnalités s'affiche, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
10. Sur la page **Sélectionner des services de rôle**, vérifiez que l'option **Autorité de certification** est déjà sélectionnée, et sélectionnez **Inscription de l'autorité de certification via le Web**.
11. Lorsque l'Assistant Ajouter des rôles et des fonctionnalités s'affiche, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
12. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Sur la page **Progression de l'installation**, après l'installation, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
14. Dans l'Assistant de configuration AD CS, sur la page **Informations d'identification**, cliquez sur **Suivant**.
15. Sur la page **Services de rôle**, sélectionnez **Autorité de certification** et **Inscription de l'autorité de certification via le Web**, puis cliquez sur **Suivant**.
16. Sur la page **Type d'installation**, sélectionnez **Autorité de certification d'entreprise**, puis cliquez sur **Suivant**.
17. Sur la page **Type d'autorité de certification**, cliquez sur **Autorité de certification secondaire**, puis sur **Suivant**.
18. Sur la page **Clé privée**, vérifiez que l'option **Créer une clé privée** est sélectionnée, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

19. Sur la page **Chiffrement pour l'autorité de certification**, conservez les sélections par défaut, puis cliquez sur **Suivant**.
20. Sur la page **Nom de l'autorité de certification**, dans la zone de texte **Nom commun de cette AC**, tapez **Adatum-IssuingCA**, puis cliquez sur **Suivant**.
21. Sur la page **Demande de certificat**, vérifiez que l'option **Enregistrer une demande de certificat dans un fichier de l'ordinateur cible** est sélectionnée, puis cliquez sur **Suivant**.
22. Sur la page **Base de données de l'autorité de certification**, cliquez sur **Suivant**.
23. Sur la page **Confirmation**, cliquez sur **Configurer**.
24. Sur la page **Résultats**, cliquez sur **Fermer**.
25. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.

▶ Tâche 2 : Installation d'un certificat d'autorité de certification secondaire

1. Sur LON-SVR1, ouvrez une fenêtre de l'Explorateur Windows et accédez au **Disque local (C:)**.
2. Cliquez avec le bouton droit sur **RootCA.cer**, puis cliquez sur **Installer le certificat**.
3. Dans l'Assistant Importation de certificat, cliquez sur **Ordinateur local**, puis sur **Suivant**.
4. Sur la page **Magasin de certificats**, cliquez sur **Placer tous les certificats dans le magasin suivant**, puis sur **Parcourir**.
5. Sélectionnez **Autorités de certification racines de confiance**, et cliquez sur **OK**.
6. Cliquez sur **Suivant**, puis sur **Terminer**.
7. Lorsque la fenêtre contextuelle **Assistant Importation du certificat** s'affiche, cliquez sur **OK**.
8. Dans la fenêtre de l'Explorateur Windows, sélectionnez les fichiers **AdatumRootCA.crl** et **LON-CA1_AdatumRootCA.crt**, cliquez avec le bouton droit sur les fichiers et cliquez sur **Copier**.
9. Double-cliquez sur **inetpub**.
10. Double-cliquez sur **wwwroot**.
11. Créez un nouveau dossier et appelez-le **CertData**.
12. Collez les deux fichiers copiés dans ce dossier.
13. Passez au **Disque local (C:)**.
14. Cliquez avec le bouton droit sur le fichier **LON-SVR1.Adatum.com_Adatum- IssuingCA.req**, puis cliquez sur **Copier**.
15. Dans la barre d'adresses de l'Explorateur Windows, tapez **\\LON-CA1\C$**, puis appuyez sur Entrée.
16. Dans la fenêtre de l'Explorateur Windows, cliquez avec le bouton droit sur un espace vide, puis cliquez sur **Coller**. Vérifiez que le fichier de demande est copié sur LON-CA1.
17. Passez au serveur LON-CA1.
18. Dans la console Autorité de certification, cliquez avec le bouton droit sur **AdatumRootCA**, pointez sur **Toutes les tâches**, puis cliquez sur **Soumettre une nouvelle demande**.
19. Dans la fenêtre Ouvrir un fichier de demande, accédez au **Disque local (C:)**, cliquez sur le fichier **LON-SVR1.Adatum.com_Adatum- IssuingCA.req**, puis sur **Ouvrir**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

20. Dans la console Autorité de certification, cliquez sur le conteneur **Demandes en attente**. Cliquez avec le bouton droit sur **Demandes en attente**, puis cliquez sur **Actualiser**.
21. Dans le volet de droite, cliquez avec le bouton droit sur la demande (avec ID 2), pointez sur **Toutes les tâches** et cliquez sur **Délivrer**.
22. Cliquez sur le conteneur **Certificats délivrés**.
23. Dans le volet de droite, double-cliquez sur le certificat, puis cliquez sur l'onglet **Détails**.
24. Cliquez sur **Copier dans un fichier**.
25. Dans l'Assistant Exportation de certificat, sur la page **Accueil**, cliquez sur **Suivant**.
26. Sur la page **Format Du fichier d'exportation**, cliquez sur **Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)**, sur **Inclure tous les certificats dans le chemin d'accès de certification si possible** et sur **Suivant**.
27. Sur la page **Fichier à exporter**, cliquez sur **Parcourir**.
28. Dans la zone de texte **Nom du fichier**, tapez **\\lon-svr1\C$**, et appuyez sur Entrée.
29. Dans la zone de texte **Nom du fichier**, tapez **SubCA**, cliquez sur **Enregistrer**, puis sur **Suivant**.
30. Cliquez sur **Terminer**, puis sur **OK** à deux reprises.
31. Basculez vers **LON-SVR1**.
32. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.
33. Dans la console Autorité de certification, cliquez avec le bouton droit sur **Adatum-IssuingCA**, pointez sur **Toutes les tâches**, puis cliquez sur **Installer un certificat d'autorité de certification**.
34. Accédez au **Disque local (C:)**, cliquez sur le fichier **SubCA.p7b**, puis sur **Ouvrir**.
35. Attendez 15 à 20 secondes, puis, dans la barre d'outils, cliquez sur l'icône verte pour démarrer le service de l'autorité de certification.
36. Vérifiez que l'AC démarre correctement.

▶ Tâche 3 : Publication du certificat d'AC racine via la stratégie de groupe

1. Sur LON-DC1, cliquez sur l'icône Gestionnaire de serveur dans la barre des tâches.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
3. Dans la console Gestion des stratégies de groupe, développez **Forêt:Adatum.com**, **Domaines**, **Adatum.com**, puis cliquez avec le bouton droit sur **Default Domain Policy**, et cliquez sur **Modifier**.
4. Dans le nœud **Configuration ordinateur**, développez **Stratégies**,**Paramètres Windows**, **Paramètres de sécurité**, **Stratégies de clé publique**, puis cliquez avec le bouton droit sur **Autorités de certification racines de confiance**, et cliquez sur **Importer**.
5. Cliquez sur **Suivant**.
6. Sur la page **Fichier à importer**, cliquez sur **Parcourir**.
7. Dans le champ de texte **Nom du fichier**, tapez **\\lon-svr1\C$**, et appuyez sur Entrée.
8. Cliquez sur le fichier **RootCA.cer**, puis sur **Ouvrir**.
9. Cliquez à deux reprises sur **Suivant**, puis cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Lorsque la fenêtre contextuelle Assistant Importation de certificat s'affiche, cliquez sur **OK.**
11. Fermez l'Éditeur de gestion des stratégies de groupe.
12. Fermez la console GPMC.

Résultats : Après avoir terminé cet exercice, vous aurez déployé et configuré une AC secondaire d'entreprise.

▶ Pour préparer l'atelier suivant

- Laisser tous les ordinateurs virtuels en fonctionnement pour l'atelier suivant. N'éteignez aucun ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Déploiement et gestion de certificats

Exercice 1 : Configuration de modèles de certificats

▶ Tâche 1 : Créer un nouveau modèle basé sur le modèle de serveur Web

1. Sur LON-SVR1, dans la console Autorité de certification, développez **Adatum-IssuingCA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis sélectionnez **Gérer**.
2. Dans la console Modèles de certificats, recherchez le modèle **Serveur Web** dans la liste, cliquez avec le bouton droit, puis cliquez sur **Dupliquer le modèle**.
3. Cliquez sur l'onglet **Général**.
4. Dans le champ **Nom complet du modèle**, tapez **Serveur Web d'Adatum** et définissez la **Période de validité** sur **3 années**
5. Cliquez sur l'onglet **Traitement de la demande**, sélectionnez **Autoriser l'exportation de la clé privée**, et cliquez sur **OK**.

▶ Tâche 2 : Créer un modèle de certificat pour les utilisateurs avec inscription de cartes à puce

1. Dans la console Modèles de certificats, cliquez avec le bouton droit sur le modèle de certificat **Utilisateur**, puis cliquez sur **Dupliquer le modèle**.
2. Dans la boîte de dialogue **Propriétés du nouveau modèle**, cliquez sur l'onglet **Général**, et dans la zone de texte **Nom complet du modèle**, tapez **Utilisateur de carte à puce Adatum**.
3. Sous l'onglet **Nom du sujet**, désactivez les cases à cocher **Inclure le nom de compte de messagerie dans le nom du sujet** et **Nom de messagerie électronique**.
4. Sous l'onglet **Extensions**, cliquez sur **Stratégies d'application**, puis sur **Modifier**.
5. Dans la boîte de dialogue **Modifier l'extension des stratégies d'application**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Ajouter une stratégie d'application**, sélectionnez **Ouverture de session par carte à puce**, puis cliquez sur **OK** à deux reprises.
7. Cliquez sur l'onglet **Modèles obsolètes**, puis sur **Ajouter**.
8. Cliquez sur le modèle **Utilisateur**, puis sur **OK**.
9. Sous l'onglet **Sécurité**, cliquez sur **Utilisateurs authentifiés**. Sous **Autorisations pour Utilisateurs authentifiés**, activez la case à cocher **Autoriser** pour **Lecture**, **Inscrire**, et **Inscrire automatique**, puis cliquez sur **OK**.
10. Fermez la console Modèles de certificats.

▶ Tâche 3 : Configurez les modèles pour qu'ils puissent être publiés

1. Sur LON-SVR1, dans la console Autorité de certification, cliquez avec le bouton droit sur **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
2. Dans la fenêtre Activer les modèles de certificat, sélectionnez **Utilisateur de carte à puce Adatum** et **Serveur Web d'Adatum**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Mettez à jour le certificat de serveur Web sur le serveur Web LON-SVR2

1. Ouvrez une session sur LON-SVR2 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
3. À l'invite de Windows PowerShell, tapez **gpupdate /force**, et appuyez sur Entrée.
4. À l'invite, redémarrez le serveur et ouvrez une session en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
5. Dans la barre des tâches, cliquez sur l'icône du Gestionnaire de serveur.
6. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire des services Internet (IIS)**.
7. Dans la console IIS, cliquez sur LON-SVR2, à l'invite du **Gestionnaire des services Internet (IIS)**, cliquez sur **Non**, et dans le volet central, double-cliquez sur **Certificats de serveur**.
8. Dans le volet Actions, cliquez sur **Créer un certificat de domaine**.
9. Sur la page **Propriétés du nom unique**, complétez les champs suivants, puis cliquez sur **Suivant** :
   - Nom commun : **lon-svr2.adatum.com**
   - Organisation : **Adatum**
   - Unité d'organisation : **Informatique**
   - Ville : **Seattle**
   - Department/région : **WA**
   - Pays/région : **US**
10. Sur la page **Autorité de certification en ligne**, cliquez sur **Sélectionner**.
11. Cliquez sur **Adatum-IssuingCA**, puis sur **OK**.
12. Dans la zone de texte **Nom convivial**, tapez **lon-svr2**, puis cliquez sur **Terminer**.
13. Vérifiez que le certificat s'affiche dans la console Certificats de serveur.
14. Dans la console IIS, développez **LON-SVR2** et **Sites**, puis cliquez sur **Default Web Site**.
15. Dans le volet Actions, cliquez sur **Liaisons**.
16. Dans la fenêtre Liaisons de sites, cliquez sur **Ajouter**.
17. Dans la zone de liste déroulante **Type**, cliquez sur **https**.
18. Dans la zone de liste déroulante **Certificat SSL**, cliquez sur **lon-svr2**, sur **OK** et sur **Fermer**.
19. Fermez la console IIS.

Résultats : Après avoir terminé cet exercice, vous aurez créé et publié de nouveaux modèles de certificats.

Exercice 2 : Configuration de l'inscription de certificats

▶ Tâche 1 : Configurer une inscription automatique pour des utilisateurs

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Développez la **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
3. Développez **Configuration utilisateur**, **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, puis cliquez pour mettre en surbrillance **Stratégies de clé publique**.
4. Dans le volet de droite, double-cliquez sur **Client des services de certificats - Inscription automatique**.
5. Dans la zone de liste déroulante **Modèle de configuration**, cliquez sur **Activé**.
6. Sélectionnez l'option **Renouveler les certificats expirés**, **mettre à jour les certificats en attente et supprimer les certificats révoqués**.
7. Sélectionnez l'option **Mettre à jour les certificats qui utilisent les modèles de certificats**.
8. Cliquez sur **OK** pour fermer la fenêtre des propriétés.
9. Dans le volet de droite, double-cliquez sur l'objet **Client des services de certificats - Stratégie d'inscription des certificats**.
10. Sous l'onglet **Stratégie d'inscription**, définissez le **Modèle de configuration** sur **Activé**, et vérifiez que la liste de stratégie d'inscription de certificat affiche la **Stratégie d'inscription à Active Directory** (une coche doit s'afficher à côté de celle-ci, et afficher l'état **Activé**).
11. Cliquez sur **OK** pour fermer la fenêtre.
12. Fermez l'Éditeur de gestion des stratégies de groupe et la console GPMC.

▶ Tâche 2 : Vérifiez l'inscription automatique

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône de Windows PowerShell.
2. À l'invite de Windows PowerShell, saisissez **gpupdate /force** et appuyez sur Entrée.
3. Après l'actualisation de la stratégie, tapez **mmc.exe**, et appuyez sur Entrée.
4. Dans la Console1, cliquez sur **Fichier**, puis dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
5. Cliquez sur **Certificats**, puis sur **Ajouter**.
6. Cliquez sur **Terminer**, puis sur **OK**.
7. Développez **Certificats - Utilisateur actuel**, **Personnel**, puis cliquez sur **Certificats**.
8. Vérifiez que le certificat basé sur le modèle **Utilisateur de carte à puce Adatum** est émis pour l'administrateur.
9. Fermez Console1. Cliquez sur **Non**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurez l'agent d'inscription pour des certificats de carte à puce

1. Sur LON-SVR1, dans la console Gestionnaire de serveur, cliquez sur **Outils**, puis ouvrez **Autorité de certification**.
2. Dans la console certsrv, développez **Adatum-IssuingCA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis cliquez sur **Gérer**.
3. Dans la console Modèles de certificats, double-cliquez sur **Agent d'inscription**.
4. Cliquez sur l'onglet **Sécurité**, puis cliquez sur **Ajouter**.
5. Dans la fenêtre Sélectionner les utilisateurs, ordinateurs, comptes de service ou groupes, tapez **Allie**, cliquez sur **Vérifier les noms**, puis sur **OK**.
6. Sous l'onglet **Sécurité**, cliquez sur **Allie Bellew (Allie@adatum.com)**, sélectionnez **Autoriser** pour les autorisations **Lecture** et **Inscrire**, puis cliquez sur **OK**.
7. Fermez la console Modèles de certificats.
8. Dans la console certsrv, cliquez avec le bouton droit sur **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
9. Dans la liste de modèles, cliquez sur **Agent d'inscription**, puis sur **OK**.
10. Basculez vers LON-CL1, puis ouvrez une session avec le nom d'utilisateur **Adatum\Allie** et le mot de passe **Pa$$w0rd**.
11. Ouvrez une fenêtre d'invite de commandes, à l'invite de commandes, tapez **mmc.exe**, et appuyez sur Entrée.
12. Dans Console1, cliquez sur **Fichier**, et sur **Ajouter/Supprimer un composant logiciel enfichable**.
13. Cliquez sur **Certificats**, sur **Ajouter**, puis sur **OK**.
14. Développez **Certificats – Utilisateur actuel**, **Personnel**, cliquez sur **Certificats**, cliquez avec le bouton droit sur **Certificats**, pointez sur **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
15. Dans l'Assistant Inscription de certificat, sur la page **Avant de commencer**, cliquez sur **Suivant**.
16. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Suivant**.
17. Sur la page **Demander des certificats**, sélectionnez **Agent d'inscription**, puis cliquez sur **Inscription**.
18. Cliquez sur **Terminer**.
19. Basculez vers **LON-SVR1**.
20. Dans la console **Autorité de certification**, cliquez avec le bouton droit sur **Adatum-IssuingCA**, puis cliquez sur **Propriétés**.
21. Cliquez sur l'onglet **Agents d'inscription**.
22. Cliquez sur **Restreindre les agents d'inscription**.
23. Sur la fenêtre contextuelle qui s'affiche, cliquez sur **OK**.
24. Dans la section **Agents d'inscription**, cliquez sur **Ajouter**.
25. Dans le champ **Sélectionnez un utilisateur, un ordinateur ou un groupe**, tapez **Allie**, cliquez sur **Vérifier les noms**, puis sur **OK**.

26. Cliquez sur **Tout le monde**, puis sur **Supprimer**.
27. Dans la section **Modèles de certificats**, cliquez sur **Ajouter**.
28. Dans la liste de modèles, sélectionnez **Utilisateur de carte à puce Adatum**, et cliquez sur **OK**.
29. Dans la section **Modèles de certificats**, cliquez sur **<Tous>**, puis cliquez sur **Supprimer**.
30. Dans la section **Autorisation**, cliquez sur **Ajouter**.
31. Dans le champ **Sélectionnez un utilisateur, un ordinateur ou un groupe**, tapez **Marketing**, cliquez sur **Vérifier les noms**, puis sur **OK**.
32. Dans la section Autorisation, cliquez sur **Tout le monde**, puis sur **Supprimer**.
33. Cliquez sur **OK**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré et vérifié l'inscription automatique pour des utilisateurs, et configuré un agent d'inscription pour des cartes à puce.

Exercice 3 : Configuration de la révocation de certificats

▶ Tâche 1 : Configuration de la distribution de la liste de révocation de certificats

1. Sous LON-SVR1, dans la console Autorité de certification, cliquez avec le bouton droit sur **Certificats révoqués**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : Certificats révoqués**, définissez l'**Intervalle de publication de la liste de révocation des certificats** sur **1 Jours**, et l'intervalle pour **Publier la liste de révocation des certificats delta** sur **1 Heures**, puis cliquez sur **OK**.
3. Cliquez avec le bouton droit sur **Adatum-IssuingCA**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de : Adatum-IssuingCA**, cliquez sur l'onglet **Extensions**, et examinez les valeurs pour **CDP**.
5. Cliquez sur **Annuler**.

▶ Tâche 2 : Installation et configuration d'un répondeur en ligne

1. Sur LON-SVR1, cliquez sur l'icône du Gestionnaire de serveur dans la barre des tâches.
2. Dans Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Cliquez sur **Suivant** à trois reprises.
4. Sur la page **Sélectionner des rôles de serveurs**, développez **Services de certificats Active Directory (Installé)**, puis cliquez sur **Répondeur en ligne**.
5. Cliquez sur **Ajouter des fonctionnalités**.
6. Cliquez sur **Suivant** à deux reprises, puis cliquez sur **Installer**.
7. Lorsque le message affiche que l'installation a réussi, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
8. Dans l'Assistant Configuration AD CS, cliquez sur **Suivant**.
9. Cliquez sur **Répondeur en ligne**, puis cliquez sur **Suivant**.
10. Cliquez sur **Configurer**, puis cliquez à deux reprises sur **Fermer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Sur LON-SVR1, ouvrez la console Autorité de certification.
12. Dans la console Autorité de certification, cliquez avec le bouton droit sur **Adatum-IssuingCA**, puis cliquez sur **Propriétés**.
13. Dans la boîte de dialogue **Propriétés de : Adatum-IssuingCA**, sous l'onglet **Extensions**, dans la liste **Sélectionner l'extension**, cliquez sur **Accès aux informations de l'Autorité (AIA**), puis sur **Ajouter**.
14. Dans la boîte de dialogue **Ajouter un emplacement**, tapez **http://LON-SVR1/ocsp**, puis cliquez sur **OK**.
15. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**.
16. Activez la case à cocher **Inclure dans l'extension OCSP (Online Certificate Status Protocol)**, puis cliquez sur **OK**.
17. Dans la boîte de dialogue **Autorité de certification**, redémarrez AD CS en cliquant sur **Oui**.
18. Dans la console certsrv, développez **Adatum-IssuingCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
19. Dans la console **Modèles de certificats**, double-cliquez sur le modèle **Signature de réponse OCSP**.
20. Dans la boîte de dialogue **Propriétés de : Signature de réponse OCSP**, cliquez sur l'onglet **Sécurité**, sous **Autorisations pour Utilisateurs authentifiés**, sélectionnez **Autoriser** pour la case à cocher **Inscrire**, puis cliquez sur **OK**.
21. Fermez la console Modèles de certificats.
22. Dans la console Autorité de certification, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
23. Dans la boîte de dialogue **Activer les modèles de certificat**, sélectionnez le modèle **Signature de réponse OCSP**, puis cliquez sur **OK**.
24. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des répondeurs en ligne**.
25. Dans la console Gestion OCSP, cliquez avec le bouton droit sur **Configuration de révocation**, puis cliquez sur **Ajouter une configuration de révocation**.
26. Dans l'Assistant Ajouter une configuration de révocation, cliquez sur **Suivant**.
27. Sur la page **Nom de la configuration de révocation**, dans la zone **Nom**, tapez **Répondeur en ligne AdatumCA**, puis cliquez sur **Suivant**.
28. Sur la page **Sélectionner un emplacement de certificat d'autorité de certification**, cliquez sur **Suivant**.
29. Sur la page **Choisir un certificat d'autorité de certification**, cliquez sur **Parcourir**, sur le certificat **Adatum-IssuingCA**, sur **OK**, puis sur **Suivant**.
30. Sur la page **Sélectionner le certificat utilisé pour la signature**, vérifiez que les options **Sélectionner automatiquement un certificat de signature** et **Inscription automatique pour un certificat de signature OCSP** sont sélectionnées, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

31. Sur la page **Fournisseur de révocation**, cliquez sur **Terminer**. L'état de la configuration de révocation est **En cours de calcul**.
32. Fermez la console Répondeur en ligne.

Résultats : Après avoir terminé cet exercice, vous aurez configuré des paramètres de révocation de certificat.

Exercice 4 : Configuration de la récupération de clé

▶ Tâche 1 : Configuration de l'autorité de certification pour délivrer des certificats d'agent de récupération de clé

1. Sur LON-SVR1, ouvrez la console Autorité de certification.
2. Dans la console Autorité de certification, développez le nœud **Adatum-IssuingCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
3. Dans le volet Détails, cliquez avec le bouton droit sur le certificat **Agent de récupération de clé**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de : Agent de récupération de clé**, cliquez sur l'onglet **Conditions d'émission**.
5. Désactivez la case à cocher **Approbation du gestionnaire de certificat de l'autorité de certification**.
6. Cliquez sur l'onglet **Sécurité**. Notez que les Admins du domaine et les administrateurs de l'entreprise sont les seuls groupes qui ont l'autorisation Inscription, puis cliquez sur **OK**.
7. Fermez la console Modèles de certificats.
8. Dans la console Autorité de certification, cliquez avec le bouton droit sur **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
9. Dans la boîte de dialogue **Activer les modèles de certificat**, cliquez sur le modèle **Agent de récupération de clé**, puis sur **OK**.
10. Fermez la console Autorité de certification.

▶ Tâche 2 : Acquisition du certificat KRA

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. À l'invite de commandes Windows PowerShell, tapez **MMC.exe** et appuyez sur Entrée.
3. Dans la console Console1-[Console Root], cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Certificats**, puis sur **Ajouter**.
5. Dans la boîte de dialogue **Composant logiciel enfichable Certificats**, sélectionnez **Mon compte d'utilisateur**, cliquez sur **Terminer**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Développez le nœud**Certificats - Utilisateur actuel**, cliquez avec le bouton droit sur **Personnel**, pointez sur **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
7. Dans l'Assistant Inscription de certificat, sur la page **Avant de commencer**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Suivant**.
9. Sur la page **Demander des certificats**, activez la case à cocher **Agent de récupération de clé**, cliquez sur **Inscription**, puis sur **Terminer**.
10. Actualisez la console et affichez le KRA dans le magasin personnel ; faites défiler les propriétés de certificat et vérifiez que l'agent de récupération de clé de modèle de certificat est présent.
11. Fermez Console1 sans enregistrer les modifications.

▶ Tâche 3 : Configuration de l'autorité de certification pour permettre la récupération de clé

1. Sous LON-SVR1, dans la console Autorité de certification, cliquez avec le bouton droit sur **Adatum-IssuingCA**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : Adatum-IssuingCA**, cliquez sur l'onglet **Agents de récupération**, puis sélectionnez **Archiver la clé**.
3. Sous **Certificats de l'agent de récupération de clé**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Sélection de l'agent de récupération de clé**, cliquez sur le certificat pour l'agent de récupération de clé (très probablement le dernier de la liste), puis cliquez sur **OK** à deux reprises.
5. Lorsque vous êtes invité à redémarrer l'AC, cliquez sur **Oui**.

▶ Tâche 4 : Configuration d'un modèle personnalisé pour l'archivage de clé

1. Sur LON-SVR1, dans la console Autorité de certification, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
2. Dans la console Modèles de certificats, cliquez avec le bouton droit sur le modèle de certificat **Utilisateur**, puis cliquez sur **Dupliquer le modèle**.
3. Dans la boîte de dialogue **Propriétés du nouveau modèle**, sous l'onglet **Général**, dans la zone **Nom complet du modèle**, tapez **Archiver l'utilisateur**.
4. Sous l'onglet **Traitement de la demande**, activez la case à cocher **Archive la clé privée de chiffrement du sujet**.
5. Si une fenêtre contextuelle s'affiche, cliquez sur **OK**.
6. Cliquez sur l'onglet **Nom du sujet**, désactivez les cases à cocher **Nom de messagerie électronique** et **Inclure le nom de compte de messagerie dans le nom du sujet**, puis cliquez sur **OK**.
7. Fermez la console Modèles de certificats.
8. Dans la console Autorité de certification, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
9. Dans la boîte de dialogue **Activer les modèles de certificat**, cliquez sur le modèle **Archiver l'utilisateur**, puis sur **OK**.
10. Fermez la console Autorité de certification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Vérification de la fonctionnalité d'archivage de clé

1. Ouvrez une session sur LON-CL1 en tant qu'**Adatum\Aidan**, en utilisant le mot de passe **Pa$$w0rd**.
2. Dans l'écran Accueil, tapez **mmc.exe** et appuyez sur Entrée.
3. Dans la console Console1-[Console Root], cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Certificats**, sur **Ajouter** et sur OK.
5. Développez le nœud **Certificats - Utilisateur actuel**, cliquez avec le bouton droit sur Personnel, cliquez sur **Toutes les tâches**, puis sur **Demander un nouveau certificat**.
6. Dans l'Assistant Inscription de certificat, sur la page **Avant de commencer**, cliquez sur **Suivant**.
7. Cliquez sur **Suivant**.
8. Sur la page **Demander des certificats**, activez la case à cocher **Archiver l'utilisateur**, cliquez sur **Inscription**, puis sur **Terminer**.
9. Actualisez la console et affichez le fait qu'un certificat est publié pour Aidan, selon le modèle de certificat **Archiver l'utilisateur**.
10. Simulez la perte d'une clé privée en supprimant le certificat. Dans le volet central, cliquez avec le bouton droit sur le certificat que vous venez d'inscrire, sélectionnez **Supprimer**, puis cliquez sur **Oui** pour confirmer.
11. Basculez vers LON-SVR1.
12. Ouvrez la console Autorité de certification, développez **Adatum-IssuingCA**, puis cliquez sur le magasin de **Certificats délivrés**.
13. Dans le volet Détails, double-cliquez sur un certificat avec le nom de demandeur **Adatum\Aidan** et le nom de modèle de certificat **Archiver l'utilisateur**.
14. Cliquez sur l'onglet **Détails**, copiez le **Numéro de série**, puis cliquez sur **OK**. [Vous pouvez copier le numéro dans le Bloc-notes (sélectionnez-le et appuyez sur CTRL+C) ou l'écrire sur un document papier.]
15. Dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
16. À l'invite de Windows PowerShell, tapez la commande suivante (où *<numéro de série>* est le numéro de série que vous avez copié), et appuyez sur Entrée :

```
Certutil –getkey <numéro de série> outputblob
```

 **Remarque :** Si vous collez le numéro de série depuis le Bloc-notes, supprimez les espaces entre les numéros.

17. Vérifiez que le fichier **outputblob** s'affiche désormais dans le dossier **C:\Utilisateurs\Administrateur.Adatum**.
18. Pour convertir le fichier **outputblob** en fichier .pfx, à l'invite de commandes de Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Certutil –recoverkey outputblob aidan.pfx
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

19. Lorsque vous êtes invité à entrer le nouveau mot de passe, tapez **Pa$$w0rd**, puis confirmez le mot de passe.
20. Après l'exécution de la commande, fermez Windows PowerShell.
21. Accédez à **C:\Utilisateurs\Administrateur.ADATUM** et vérifiez que **aidan.pfx**, la clé récupérée, est créée.
22. Basculez vers l'ordinateur LON-CL1
23. Dans le menu Accueil, cliquez sur Panneau de configuration.
24. Dans la fenêtre du Panneau de configuration, cliquez sur Afficher l'état et la gestion du réseau.
25. Dans la fenêtre Centre Réseau et partage, cliquez sur Modifier les paramètres de partage avancés.
26. Sous Invité ou public (profil actuel), sélectionnez l'option Activer le partage de fichiers et d'imprimantes.
27. Cliquez sur Enregistrer les modifications.
28. Lorsque vous êtes invité à entrer les informations d'identification, utilisez **Adatum\administrateur** comme nom d'utilisateur et **Pa$$w0rd** comme mot de passe.
29. Rebasculez vers l'ordinateur LON-SVR1.
30. Copiez le fichier **aidan.pfx** dans **\\lon-cl1\C$**.
31. Basculez vers **LON-CL1** et vérifiez que vous êtes toujours connecté comme Aidan.
32. Accédez au lecteur **C**, et double-cliquez sur le fichier **aidan.pfx**.
33. Sur la page **Bienvenue dans l'Assistant Importation du certificat**, cliquez sur **Suivant**.
34. Sur la page **Fichier à importer**, cliquez sur **Suivant**.
35. Sur la page **Mot de passe**, entrez **Pa$$w0rd** comme mot de passe et cliquez sur **Suivant**.
36. Sur la page **Magasin de certificats**, cliquez sur **Suivant**, sur **Terminer**, puis sur **OK**.
37. Développez le nœud **Certificats - Utilisateur actuel**, **Personnel**, puis cliquez sur **Certificats**.
38. Actualisez la console et vérifiez que le certificat pour **Aidan** est restauré.

Résultats : Après avoir terminé cet exercice, vous aurez implémenté l'archivage de clé et testé la récupération de clé privée.

▶ Pour préparer le module suivant :

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-CL1**, **22412B-LON-SVR1**, **22412B-LON-CA1** et **22412B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR ICT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7 : Implémentation des services AD RMS (Active Directory Rights Management Services)

Atelier pratique : Implémentation AD RMS

Exercice 1 : Installation et configuration AD RMS

▶ Tâche 1 : Configurer le DNS (Domain Name System) et le compte de service Active Directory® Rights Management Services (AD RMS)

1. Connectez-vous à LON-DC1 à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
3. Sélectionnez puis cliquez avec le bouton droit sur **Adatum (local)**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
4. Dans la boîte de dialogue **Créer Unité d'organisation**, dans le champ **Nom**, saisissez **Comptes de service**, puis cliquez sur **OK**.
5. Cliquez avec le bouton droit sur l'unité d'organisation (OU) **Comptes de service**, cliquez sur **Nouveau**, puis sur **Utilisateur**.
6. Dans la boîte de dialogue **Créer Utilisateur**, entrez les détails suivants (Il se peut que vous deviez sélectionnez **Autres options de mot de passe**), puis cliquez sur **OK** :
   - Prénom : **ADRMSSVC**
   - Ouverture de session UPN l'utilisateur : **ADRMSSVC**
   - Mot de passe : **Pa$$w0rd**
   - Confirmation : **Pa$$w0rd**
   - Le mot de passe n'expire jamais : **Activé**
   - L'utilisateur ne peut pas changer de mot de passe : **Activé**
7. Cliquez avec le bouton droit sur le conteneur **Users**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
8. Dans la boîte de dialogue **Créer Groupe**, entrez les détails suivants, puis cliquez sur **OK** :
   - Nom du groupe : **ADRMS_SuperUsers**
   - Adresse de messagerie : **ADRMS_SuperUsers@adatum.com**
9. Cliquez avec le bouton droit sur le conteneur **Users**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
10. Dans la boîte de dialogue **Créer Groupe**, entrez les détails suivants, puis cliquez sur **OK**.
    - Nom du groupe : **Cadres**
    - Adresse de messagerie : **executives@adatum.com**
11. Double-cliquez sur l'unité d'organisation **Managers**.
12. Maintenez la touche Ctrl enfoncée et cliquez sur les utilisateurs suivants :
    - **Aidan Delaney**
    - **Bill Malone**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

13. Dans le volet Tâches, cliquez sur **Ajouter au groupe**.
14. Dans la boîte de dialogue **Sélectionnez des groupes**, saisissez **Cadres**, puis cliquez sur **OK**.
15. Fermez le Centre d'administration Active Directory.
16. Dans le Gestionnaire de serveurs, cliquez sur **Outils**, puis sur **DNS**.
17. Dans le Gestionnaire DNS, développez successivement **LON-DC1**, et **Zones de recherche directes**.
18. Sélectionnez **Adatum.com**, puis cliquez dessus avec le bouton droit et cliquez sur **Nouvel hôte (A ou AAAA)**.
19. Dans la boîte de dialogue **Nouvel hôte**, entrez les informations suivantes, puis cliquez sur **Ajouter un hôte**:
    - Nom : **adrms**
    - Adresse IP : **172.16.0.21**
20. Cliquez sur **OK**, puis sur **Terminé**.
21. Fermez la console du Gestionnaire DNS.

▶ Tâche 2 : Installer et configurer le rôle de serveur AD RMS

1. Connectez-vous à LON-SVR1 à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez trois fois sur **Suivant**.
4. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Services AD RMS (Active Directory Rights Management Services)**.
5. Dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez quatre fois sur **Suivant**.
6. Cliquez sur **Installer**, puis cliquez sur **Fermer**.
7. Dans le Gestionnaire de serveur, cliquez sur le nœud **AD RMS**.
8. À côté de Configuration requise pour Active Directory Rights Management Services au niveau de LON-SVR1, cliquez sur **Autres**.
9. Sur la page **Détails et notifications de la tâche Tous les serveurs**, cliquez sur **Effectuer une configuration supplémentaire**.
10. Dans la boîte de dialogue **Configuration AD RMS : LON-SVR1.Adatum.com**, cliquez sur **Suivant**.
11. Sur la page **Cluster AD RMS**, cliquez sur **Créer un nouveau cluster racine AD RMS**, puis cliquez sur **Suivant**.
12. Sur la page **Base de données de configuration**, cliquez sur **Utiliser la base de données interne de Windows sur ce serveur**, puis cliquez sur **Suivant**.
13. Dans la page **Compte de service**, cliquez sur **Spécifier**.
14. Dans la boîte de dialogue **Sécurité de Windows**, entrez les détails suivants, cliquez sur **OK** puis sur **Suivant** :
    - Nom d'utilisateur : **ADRMSSVC**
    - Mot de passe : **Pa$$w0rd**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

15. Sur la page **Mode de chiffrement**, cliquez sur **Mode de chiffrement 2**, puis cliquez sur **Suivant**.
16. Sur la page **Stockage de clé de cluster**, cliquez sur **Utiliser le stockage de clé AD RMS géré de manière centralisée**, puis cliquez sur **Suivant**.
17. Sur la page **Mot de passe de clé de cluster**, entrez le mot de passe **Pa$$w0rd** deux fois, puis cliquez sur **Suivant**.
18. Dans la page **Site Web de cluster**, vérifiez que **Default Web Site** est sélectionné, puis cliquez sur **Suivant**.
19. Sur la page **Adresse du cluster**, fournissez les informations suivantes, puis cliquez sur **Suivant**:
    - Type de connexion : **Utiliser une connexion non chiffrée (http://)**
    - Nom de domaine complet : **adrms.adatum.com**
    - Port : **80**
20. Sur la page **Certificat de licence**, saisissez **Adatum AD RMS**, puis cliquez sur **Suivant**.
21. Dans la page **Inscription du SCP**, cliquez sur **Enregistrer le point de connexion de service maintenant**, puis cliquez sur **Suivant**.
22. Cliquez sur **Installer**, puis cliquez sur **Fermer**.
23. Dans le Gestionnaire de serveur, cliquez sur **Outils** et cliquez sur **Gestionnaire des services Internet (IIS)**.
24. Dans le Gestionnaire des services Internet (IIS), développez **LON-SVR1**, développez **Sites**, développez **Default Web Site** et cliquez sur **_wmcs**.
25. Sous l'accueil /_wmcs, double-cliquez sur **Authentification**, cliquez sur **Authentification anonyme** et dans le volet Actions, cliquez sur **Activer**.
26. Dans le volet Connexions, développez **_wmcs** et cliquez sur **licensing**.
27. Sous l'accueil /_wmcs/licensing, double-cliquez sur **Authentification**, cliquez sur **Authentification anonyme** et dans le volet Actions, cliquez sur **Activer**.
28. Dans l'écran Accueil, cliquez sur **Administrateur**, puis cliquez sur **Se déconnecter**.

Remarque : Vous devez vous déconnecter avant de pouvoir gérer AD RMS.

▶ Tâche 3 : Configurer le groupe de super utilisateurs des services AD RMS

1. Connectez-vous à LON-SVR1 à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**.
3. Dans la console AD RMS, développez le nœud **lon-svr1**, puis cliquez sur **Stratégies de sécurité**.
4. Dans la zone Stratégies de sécurité, sous Super utilisateurs, cliquez sur **Modifier les paramètres de super utilisateur**.
5. Dans le volet Actions, cliquez sur **Activer les super utilisateurs**.

6. Dans la zone Super utilisateurs, cliquez sur **Modifier le groupe des super utilisateurs**.
7. Dans la boîte de dialogue **Super utilisateurs**, dans la zone de texte **Groupe de super utilisateurs**, saisissez **ADRMS_SuperUsers@adatum.com**, puis cliquez sur **OK**.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré les services AD RMS.

Exercice 2 : Configuration des modèles AD RMS

▶ Tâche 1 : Configurer un nouveau modèle de stratégie de droits

1. Vérifiez que vous avez ouvert une session sur LON-SVR1.
2. Dans la console Active Directory Rights Management Services, cliquez sur le nœud **lon-svr1\Modèles de stratégie de droits**.
3. Dans le volet Actions, cliquez sur **Créer un modèle de stratégie de droits distribué**.
4. Dans l'Assistant Créer un modèle de stratégie de droits distribué., sur la page **Ajouter des informations d'identification du modèle**, cliquez sur **Ajouter**.
5. Sur la page **Ajouter des informations d'identification du modèle**, entrez les informations suivantes, puis cliquez sur **Ajouter** :
   - Langue : **français (France)**
   - Nom : **ReadOnly**
   - Description : **Accès en lecture seule. Aucune copie ou impression**
6. Cliquez sur **Suivant**.
7. Dans la page **Ajouter des droits d'utilisateur**, cliquez sur **Ajouter**.
8. Sur la page **Ajouter un utilisateur ou un groupe**, saisissez **executives@adatum.com**, puis cliquez sur **OK**.
9. Quand executives@adatum.com est sélectionné, sous **Droits**, cliquez sur **Afficher**. Vérifiez que l'option **Octroyer le contrôle total au propriétaire (auteur) sans date d'expiration** est sélectionnée, puis cliquez sur **Suivant**.
10. Dans la page **Spécifier la stratégie d'expiration**, choisissez les paramètres suivants, puis cliquez sur **Suivant** :
    - Expiration du contenu : Expire après (jours) : **7**
    - Expiration de la licence d'utilisation : Expire après (jours) : **7**
11. Sur la page **Spécifier la stratégie étendue**, cliquez sur **Demander une nouvelle licence d'utilisation à chaque accès au contenu (désactiver la mise en cache côté client)**, cliquez sur **Suivant**, puis cliquez sur **Terminer**.

▶ Tâche 2 : Configurer la distribution des modèles de stratégie de droits

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
2. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
New-Item c:\rmstemplates -ItemType Directory
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
New-SmbShare -Name RMSTEMPLATES -Path c:\rmstemplates -FullAccess ADATUM\ADRMSSVC
```

4. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
New-Item c:\docshare -ItemType Directory
```

5. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
New-SmbShare -Name docshare -Path c:\docshare -FullAccess "tout le monde"
```

6. Pour quitter Windows PowerShell, saisissez **exit**.
7. Basculez sur la console AD RMS.
8. Cliquez sur le nœud **Modèles de stratégies de droits**, et dans la zone Modèles de stratégies de droits distribués, cliquez sur **Modifier l'emplacement du fichier de modèles de stratégies de droits distribués**.
9. Dans la boîte de dialogue **Modèles de stratégies de droits**, cliquez sur **Activer l'exportation**.
10. Dans la zone Spécifiez un emplacement de fichier pour les modèles (UNC), saisissez **\\LON-SVR1\RMSTEMPLATES**, puis cliquez sur **OK**.
11. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers®.
12. Naviguez jusqu'au dossier C:\rmstemplates et vérifiez que **ReadOnly.xml** est présent.
13. Fermez la fenêtre de l'Explorateur de fichiers.

▶ Tâche 3 : Configurer une stratégie d'exclusion

1. Basculez sur la console AD RMS.
2. Cliquez sur le nœud **Stratégies d'exclusion**, puis cliquez sur **Gérer la liste d'exclusions d'applications**.
3. Dans le volet Actions, cliquez sur **Activer l'exclusion d'applications**.
4. Dans le volet Actions, cliquez sur **Exclure l'application**.
5. Dans la boîte de dialogue **Exclure l'application**, saisissez les informations suivantes, puis cliquez sur **Terminer** :
   - Nom de fichier d'application : **Powerpnt.exe**
   - Version minimale : **14.0.0.0**
   - Version maximale : **16.0.0.0**

Résultats : Après avoir terminé cet exercice, vous aurez configuré les modèles AD RMS.

Exercice 3 : Implémentation des stratégies d'approbation AD RMS

▶ Tâche 1 : Exporter la stratégie des domaines d'utilisateurs approuvés

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
New-Item c:\export -ItemType Directory
```

3. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
New-SmbShare -Name Export -Path c:\export -FullAccess “tout le monde”
```

4. Fermez la fenêtre Windows PowerShell.
5. Dans la console AD RMS, développez le nœud **Stratégies d'approbation**, puis cliquez sur le nœud **Domaines d'utilisateurs approuvés**.
6. Dans le volet Actions, cliquez sur **Exporter le domaine d'utilisateur approuvé**.
7. Dans la boîte de dialogue **Exporter les domaines d'utilisateurs approuvé en tant que**, naviguez jusqu'à **\\LON-SVR1\Export**, définissez le nom de fichier sur **ADATUM-TUD.bin**, puis cliquez sur **Enregistrer**.
8. Connectez-vous à MUN-DC1 à l'aide du compte **TREYRESEARCH\Administrateur** et du mot de passe **Pa$$w0rd**.
9. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**.
10. Dans la console AD RMS, développez **mun-dc1**, développez le nœud **Stratégies d'approbation**, puis cliquez sur le nœud **Domaines d'utilisateurs approuvés**.
11. Dans le volet Actions, cliquez sur **Exporter le domaine d'utilisateur approuvé**.
12. Dans la boîte de dialogue **Exporter le domaine d'utilisateur approuvé en tant que**, naviguez jusqu'à **\\LON-SVR1\Export**, définissez le nom de fichier sur **TREYRESEARCH-TUD.bin**, puis cliquez sur **Enregistrer**.
13. Sur MUN-DC1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
14. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
Add-DnsServerConditionalForwarderZone -MasterServers 172.16.0.10 -Name adatum.com
```

15. Fermez la fenêtre Windows PowerShell.

▶ Tâche 2 : Exporter la stratégie des domaines de publication approuvés

1. Basculez vers LON-SVR1.
2. Dans la console AD RMS, sous le nœud **Stratégies d'approbation**, cliquez sur le nœud **Domaines de publication approuvés**.
3. Dans le volet Actions, cliquez sur **Exporter le domaine de publication approuvé**.
4. Dans la boîte de dialogue **Exporter le domaine de publication approuvé.**, cliquez sur **Enregistrer sous**.
5. Dans la boîte de dialogue **Exporter le fichier de domaine de publication approuvé en tant que**, naviguez jusqu'à **\\LON-SVR1\Export**, définissez le nom du fichier sur **ADATUM-TPD.xml**, puis cliquez sur **Enregistrer**.
6. Dans la boîte de dialogue **Exporter le domaine de publication approuvé**, entrez le mot de passe **Pa$$w0rd** deux fois, puis cliquez sur **Terminer**.
7. Basculez vers MUN-DC1.
8. Dans la console AD RMS, sous le nœud **Stratégies d'approbation**, cliquez sur le nœud **Domaines de publication approuvés**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans le volet Actions, cliquez sur **Exporter le domaine de publication approuvé**.
10. Dans la boîte de dialogue **Exporter le domaine de publication approuvé**, cliquez sur **Enregistrer sous**.
11. Dans la boîte de dialogue **Exporter le fichier du domaine de publication approuvé sous**, naviguez jusqu'à **\\LON-SVR1\Export**, définissez le nom du fichier sur **TREYRESEARCH-TPD.xml**, puis cliquez sur **Enregistrer**.
12. Dans la boîte de dialogue **Exporter le domaine de publication approuvé**, entrez le mot de passe **Pa$$w0rd** deux fois, puis cliquez sur **Terminer**.

▶ Tâche 3 : Importer la stratégie de domaine d'utilisateur approuvé à partir du domaine partenaire

1. Basculez vers LON-SVR1.
2. Dans la console AD RMS, sous le nœud **Stratégies d'approbation**, cliquez sur le nœud **Domaines d'utilisateurs approuvés**.
3. Dans le volet Actions, cliquez sur **Importer le domaine d'utilisateur approuvé**.
4. Dans la boîte de dialogue **Importer le domaine d'utilisateurs approuvé**, entrez les détails suivants, puis cliquez sur **Terminer** :
   - Fichier du domaine d'utilisateurs approuvés : **\\LON-SVR1\Export\TREYRESEARCH-TUD.bin**
   - Nom complet : **Trey Research**
5. Basculez vers MUN-DC1.
6. Dans la console AD RMS, sous le nœud **Stratégies d'approbation**, cliquez sur le nœud **Domaines d'utilisateurs approuvés**.
7. Dans le volet Actions, cliquez sur **Importer le domaine d'utilisateur approuvé**.
8. Dans la boîte de dialogue **Importer le domaine d'utilisateurs approuvé**, entrez les détails suivants, puis cliquez sur **Terminer** :
   - Fichier du domaine d'utilisateurs approuvés : **\\LON-SVR1\Export\ADATUM-TUD.bin**
   - Nom complet : **Adatum**

▶ Tâche 4 : Importer la stratégie des domaines de publication approuvés à partir du domaine partenaire

1. Basculez vers LON-SVR1.
2. Dans la console AD RMS, sous le nœud **Stratégies d'approbation**, cliquez sur le nœud **Domaines de publication approuvé**.
3. Dans le volet Actions, cliquez sur **Importer le domaine de publication approuvé**.
4. Dans la boîte de dialogue **Importer le domaine de publication approuvé**, entrez les informations suivantes, puis cliquez sur **Terminer** :
   - Fichier du domaine de publication approuvé : **\\LON-SVR1\Export\ TREYRESEARCH-TPD.xml**
   - Mot de passe : **Pa$$w0rd**
   - Nom complet : **Trey Research**
5. Basculez vers MUN-DC1.

6. Dans la console AD RMS, sous le nœud **Stratégies d'approbation**, cliquez sur le nœud **Domaines de publication approuvé**.
7. Dans le volet Actions, cliquez sur **Importer le domaine de publication approuvé**.
8. Dans la boîte de dialogue **Importer le domaine de publication approuvé**, fournissez les informations suivantes, puis cliquez sur **Terminer** :
   - Fichier du domaine de publication approuvé : **\\LON-SVR1\Export\adatum-tpd.xml**
   - Mot de passe : **Pa$$w0rd**
   - Nom complet : **Adatum**

Résultats : À la fin de cet exercice, vous aurez implémenté des stratégies d'approbation AD RMS.

Exercice 4 : Vérification du déploiement AD RMS

▶ Tâche 1 : Créer un document protégé par des droits

1. Ouvrez une session sur LON-CL1 en tant qu'**Adatum\Aidan** en utilisant le mot de passe **Pa$$w0rd**.
2. Sur l'écran d'accueil, saisissez **Word**. Dans la zone Résultats, cliquez sur **Microsoft Word 2010**.
3. Dans la boîte de dialogue **Nom d'utilisateur**, cliquez sur **OK**.
4. Dans la boîte de dialogue Bienvenue dans **Microsoft Office 2010**, cliquez sur **Ne pas apporter de modifications**, puis cliquez sur **OK**.
5. Dans le document Microsoft® Word 2010, saisissez le texte suivant :

   Ce document est pour les cadres seulement, il ne doit pas être modifié.
6. Cliquez sur **Fichier**, cliquez sur **Protéger le document**, cliquez sur **Restreindre l'autorisation par les personnes**, puis cliquez sur **Gérer les informations d'identification**.
7. Dans la boîte de dialogue **Sécurité de Windows**, saisissez les informations d'identification suivantes.
   - Nom d'utilisateur : **Aidan**
   - Mot de passe : **Pa$$w0rd**
8. Activez **Mémoriser ces informations**, puis cliquez sur **OK**.
9. Dans la boîte de dialogue **Sélectionner l'utilisateur**, cliquez sur **OK**.
10. Dans la boîte de dialogue **Autorisation**, activez **Restreindre l'autorisation à : document**.
11. Dans la zone de texte **Lire**, saisissez **bill@adatum.com**, puis cliquez sur **OK**.
12. Cliquez sur **Enregistrer**.
13. Dans la boîte de dialogue **Enregistrer sous**, enregistrer le document à l'emplacement **\\lon-svr1\docshare** avec le nom **Cadres seulement.docx**.
14. Fermez Microsoft Word.
15. Dans l'écran Accueil, cliquez sur l'icône **Aidan Delaney**, puis cliquez sur **Se déconnecter**.

▶ Tâche 2 : Vérifier l'accès interne au contenu protégé

1. Ouvrez une session sur LON-CL1 en tant qu'**Adatum\Bill** en utilisant le mot de passe **Pa$$w0rd**.
2. Dans l'écran **Accueil**, cliquez sur **Bureau**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
4. Dans la fenêtre de l'Explorateur de fichiers, naviguez jusqu'à **\\lon-svr1\docshare**.
5. Dans le dossier docshare, double-cliquez sur le document **Cadres seulement**.
6. Dans la boîte de dialogue **Nom d'utilisateur**, cliquez sur **OK**.
7. Dans la boîte de dialogue **Microsoft Word**, cliquez sur **Oui**.
8. Dans la boîte de dialogue **Sécurité de Windows**, saisissez les informations d'identification suivantes, activez la case à cocher **Mémoriser ces informations**, puis cliquez sur **OK**.
   - Nom d'utilisateur : **Bill**
   - Mot de passe : **Pa$$w0rd**
9. Dans la boîte de dialogue **Microsoft Word**, cliquez sur **Oui**.
10. Dans la boîte de dialogue **Sélectionner l'utilisateur**, cliquez sur **bill@adatum.com (Adatum AD RMS)** et cliquez sur **OK**.
11. Dans la boîte de dialogue **Microsoft Office**, cliquez sur **OK**.
12. Dans la boîte de dialogue **Bienvenue dans Microsoft Office 2010**, cliquez sur **Ne pas apporter de modifications**, puis cliquez sur **OK**.
13. Quand le document s'ouvre, vérifiez que vous ne pouvez pas modifier ni enregistrer le document.
14. Sélectionnez une ligne de texte dans le document.
15. Cliquez avec le bouton droit sur le texte et vérifiez que vous ne pouvez pas apporter de modifications.
16. Cliquez sur **Afficher l'autorisation**, examinez les autorisations, puis cliquez sur **OK**.
17. Fermez Microsoft Word.
18. Dans l'écran Accueil, cliquez sur l'icône **Bill Malone**, puis cliquez sur **Se déconnecter**.

▶ Tâche 3 : Ouvrir le document protégé par des droits en tant qu'utilisateur non autorisé

1. Ouvrez une session sur LON-CL1 en tant qu'**Adatum\Carol** en utilisant le mot de passe **Pa$$w0rd**.
2. Dans le menu Accueil, cliquez sur **Bureau**.
3. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
4. Dans la fenêtre de l'Explorateur de fichiers, naviguez jusqu'à **lon-svr1****docshare**.
5. Dans le dossier docshare, double-cliquez sur le document **Cadres seulement**.
6. Cliquez sur **OK** à l'invite Nom d'utilisateur.
7. Dans la boîte de dialogue **Microsoft Word**, cliquez sur **Oui**.
8. Dans la fenêtre Sécurité de Windows, dans le champ **Nom d'utilisateur**, saisissez **Carol**, dans le champ **Mot de passe**, saisissez **Pa$$w0rd**, puis cliquez sur **OK**.
9. Dans la boîte de dialogue **Microsoft Word**, cliquez sur **Oui**.
10. Dans la boîte de dialogue **Sélectionner l'utilisateur**, cliquez sur **carol@adatum.com (Adatum AD RMS)** et cliquez sur **OK**.

11. Cliquez sur **OK** dans la fenêtre d'invite Microsoft Office.
12. Vérifiez que Carol ne peut pas ouvrir le document. Vous recevrez un message avec l'option Modifier l'utilisateur ou Demander l'accès.
13. Cliquez sur **Non**.
14. Sélectionnez **Ne pas apporter de modifications** et cliquez sur **OK**.
15. Fermez Microsoft Word.
16. Dans l'écran Accueil, cliquez sur l'icône **Carol Troup**, puis cliquez sur **Se déconnecter**.

▶ Tâche 4 : Ouvrir et modifier le document protégé par des droits en tant qu'utilisateur autorisé au sein de Trey Research

1. Ouvrez une session sur LON-CL1 en tant qu'**Adatum\Aidan** en utilisant le mot de passe **Pa$$w0rd**.
2. Sur l'écran d'accueil, saisissez **Word**. Dans la zone Résultats, cliquez sur **Microsoft Word 2010**.
3. Dans le document Microsoft Word, saisissez le texte suivant :

   Ce document est pour Trey Research seulement, il ne doit pas être modifié.
4. Cliquez sur **Fichier**, cliquez sur **Protéger le document**, cliquez sur **Restreindre l'autorisation par les personnes**, puis cliquez sur **Gérer les informations d'identification**.
5. Dans la boîte de dialogue **Sélectionner l'utilisateur**, cliquez sur **OK**.
6. Dans la boîte de dialogue **Autorisation**, activez **Restreindre l'autorisation à : document**.
7. Dans la zone de texte **Lire**, saisissez **april@treyresearch.net**, cliquez sur **OK**, puis cliquez sur **Enregistrer**.
8. Dans la boîte de dialogue **Enregistrer sous**, enregistrer le document à l'emplacement **\\lon-svr1\docshare** avec le nom **TreyResearch-Confidential.docx**.
9. Dans l'écran Accueil, cliquez sur l'icône **Aidan Delaney**, puis cliquez sur **Se déconnecter**.
10. Connectez-vous à MUN-CL1 en tant que **TREYRESEARCH\APRIL** avec le mot de passe **Pa$$w0rd**.
11. Dans l'écran Accueil, cliquez sur **Bureau**.
12. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
13. Dans la fenêtre de l'Explorateur de fichiers, naviguez jusqu'à **lon-svr1****docshare**.
14. Dans la boîte de dialogue **Sécurité de Windows**, entrez les informations d'identification suivantes, puis cliquez sur **OK**:
    - Nom d'utilisateur : **Adatum\Administrateur**
    - Mot de passe : **Pa$$w0rd**
15. Copiez le fichier **TreyResearch-Confidential.docx** sur le bureau.
16. Double-cliquez sur le fichier.
17. Dans la boîte de dialogue **Nom d'utilisateur**, cliquez sur **OK**.
18. Dans la boîte de dialogue **Microsoft Word**, cliquez sur **Oui**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

19. Dans la boîte de dialogue **Sécurité de Windows**, saisissez les informations d'identification suivantes, cochez la case **Mémoriser ces informations**, puis cliquez sur **OK** :
    - Nom d'utilisateur : **April**
    - Mot de passe : **Pa$$w0rd**
20. Dans la boîte de dialogue **Microsoft Word**, cliquez sur **Oui**.
21. Dans la boîte de dialogue **Sélectionner un utilisateur**, assurez-vous qu'**april@treyresearch.com** est sélectionné, puis cliquez sur **OK**.
22. Dans la boîte de dialogue **Microsoft Office**, cliquez sur **OK**.
23. Dans la boîte de dialogue **Microsoft Word**, cliquez sur **Oui**.
24. Dans la boîte de dialogue **Bienvenue dans Microsoft Office 2010**, cliquez sur **Ne pas apporter de modifications**, puis cliquez sur **OK**.
25. Quand le document s'ouvre, vérifiez que vous ne pouvez pas modifier ni enregistrer le document.
26. Sélectionnez une ligne de texte dans le document et vérifier.
27. Cliquez avec le bouton droit sur le texte et vérifiez que vous ne pouvez pas apporter de modifications.
28. Cliquez sur **Afficher l'autorisation**, examinez les autorisations, puis cliquez sur **OK**.

Résultats : Après avoir terminé cet exercice, vous aurez vérifié que le déploiement des services AD RMS est réussi.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-MUN-DC1**, **22412B-LON-CL1** et **22412B-MUN-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8 : Implémentation des services AD FS (Active Directory Federation Services)

Atelier pratique : Implémentation des services AD FS (Active Directory Federation Services)

Exercice 1 : Configuration des conditions préalables des services AD FS (Active Directory Federation Services)

▶ Tâche 1 : Configurer les redirecteurs DNS (Domain Name System)

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Développez **LON-DC1**, puis cliquez sur **Redirecteurs conditionnels**.
3. Cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
4. Dans la boîte de dialogue **Domaine DNS**, saisissez **TreyResearch.net**.
5. Cliquez dans la colonne **Adresse IP** et saisissez **172.16.10.10**. Appuyez sur Entrée, plus cliquez sur **OK**.
6. Fermez le Gestionnaire DNS.
7. Sur MUN-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
8. Développez **MUN-DC1.TreyResearch.net**, puis cliquez sur **Redirecteurs conditionnels**.
9. Cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
10. Dans la zone **Domaine DNS**, saisissez **Adatum.com**.
11. Cliquez dans la colonne **Adresse IP** et saisissez **172.16.0.10**. Appuyez sur Entrée, plus cliquez sur **OK**.
12. Fermez le Gestionnaire DNS.

▶ Tâche 2 : Échanger les certificats racines pour activer des approbations de certificat

1. Sur LON-DC1, accédez à la page **Rechercher**.
2. Dans la zone **Rechercher**, saisissez **\\MUN-DC1.treyresearch.net\certenroll** et appuyez sur Entrée.
3. Dans la fenêtre certenroll, cliquez avec le bouton droit sur le fichier **MUN-DC1.TreyResearch.net_TreyResearch-MUN-DC1-CA.crt**, puis cliquez sur **Copier**.
4. Dans le volet gauche, cliquez sur **Documents**, puis collez le fichier dans le dossier **Documents**.
5. Ouvrez une invite de commandes Windows PowerShell®, saisissez **MMC**, et appuyez sur Entrée.
6. Dans la fenêtre Console1, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
7. Cliquez sur **Éditeur de gestion des stratégies de groupe**, puis sur **Ajouter**.
8. Dans **Objet de stratégie de groupe**, cliquez sur **Parcourir**.
9. Cliquez sur **Default Domain Policy**, puis sur **OK**.
10. Cliquez sur **Terminer**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Double-cliquez sur **Stratégie Default Domain Policy [LON-DC1.Adatum.com]**. Dans l'arborescence de la console, développez **Configuration ordinateur**, **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité** et **Stratégies de clé publique**, puis cliquez sur **Autorités de certification racines de confiance**.
12. Cliquez avec le bouton droit sur **Autorités de certification racines de confiance**, puis cliquez sur **Importer**.
13. Sur la page **Bienvenue dans l'Assistant Importation du certificat**, cliquez sur **Suivant**.
14. Sur la page **Fichier à importer**, cliquez sur **Parcourir**.
15. Dans la fenêtre Ouvrir, cliquez sur **MUN-DC1.TreyResearch.net_TreyResearch-MUN-DC1-CA.crt**, cliquez sur **Ouvrir**, puis sur **Suivant**.
16. Sur la page **Magasin de certificats**, vérifiez que **Placer tous les certificats dans le magasin suivant** est sélectionné, vérifiez que le magasin **Autorités de certification racines de confiance** est répertorié, puis cliquez sur **Suivant**.
17. Sur la page **Fin de l'Assistant Importation du certificat**, cliquez sur **Terminer**, puis sur **OK**.
18. Fermez l'Éditeur de gestion des stratégies de groupe sans enregistrer les modifications.
19. Sur MUN-DC1, accédez à la page **Rechercher**.
20. Dans la zone **Rechercher**, saisissez **\\LON-DC1.adatum.com\certenroll**, puis appuyez sur Entrée.
21. Dans la fenêtre CertEnroll, cliquez avec le bouton droit sur le fichier **MUN-DC1.TreyResearch.net_TreyResearch-MUN-DC1-CA.crt**, puis cliquez sur **Copier**.
22. Dans le volet gauche, développez **Bibliothèques**, cliquez sur **Documents**, puis collez le fichier dans le dossier **Documents**.
23. Ouvrez une invite de commandes Windows PowerShell, saisissez **MMC**, et appuyez sur Entrée.
24. Dans la fenêtre Console1, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
25. Cliquez sur **Certificats**, puis sur **Ajouter**.
26. Cliquez sur **Un compte d'ordinateur**, puis sur **Suivant**.
27. Vérifiez que **L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)** est sélectionné, cliquez sur **Terminer**, puis sur **OK**.
28. Développez **Certificats**, puis cliquez sur **Autorités de certification racines de confiance**.
29. Cliquez avec lebouton droit sur **Autorités de certification racines de confiance**, pointez sur **Toutes les tâches**, puis cliquez sur **Importer**.
30. Sur la page **Bienvenue dans l'Assistant Importation du certificat**, cliquez sur **Suivant**.
31. Sur la page **Fichier à importer**, cliquez sur **Parcourir**.
32. Dans la fenêtre Ouvrir, cliquez sur **MUN-DC1.TreyResearch.net_TreyResearch-MUN-DC1-CA.crt**, cliquez sur **Ouvrir**, puis sur **Suivant**.
33. Sur la page **Magasin de certificats**, vérifiez que **Placer tous les certificats dans le magasin suivant** est sélectionné, vérifiez que le magasin **Autorités de certification racines de confiance** est répertorié, puis cliquez sur **Suivant**.
34. Sur la page **Fin de l'Assistant Importation du certificat**, cliquez sur **Terminer**, puis sur **OK**.
35. Fermez Console1 sans enregistrer les modifications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Demander et installer un certificat pour le serveur Web

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire des services Internet (IIS)**.
2. Dans l'arborescence de la console, cliquez sur **LON-SVR1 (Adatum\Administrateur)**.
3. Dans le volet central, double-cliquez sur **Certificats de serveur**.
4. Dans le volet **Actions**, cliquez sur **Créer un certificat de domaine**.
5. Sur la page **Propriétés du nom unique**, saisissez les paramètres comme indiqué ci-dessous, puis cliquez sur **Suivant** :
   - Nom commun : **LON-SVR1.adatum.com**
   - Organisation : **A. Datum**
   - Unité d'organisation : **Informatique**
   - Ville : **London**
   - Department/région : **Angleterre**
   - Pays/région : **GB**
6. Sur la page **Autorité de certification en ligne**, dans **Indiquer une autorité de certification en ligne**, cliquez sur **Sélectionner** pour rechercher un serveur d'autorité de certification dans le domaine.
7. Sélectionnez **Adatum-LON-DC1-CA**, puis cliquez sur **OK**.
8. Dans le champ **Nom convivial**, saisissez **LON-SVR1.adatum.com**, puis cliquez sur **Terminer**.

▶ Tâche 4 : Lier le certificat à l'application prenant en charge les revendications sur le serveur Web et vérifier l'accès à l'application

1. Sur LON-SVR1, dans le Gestionnaire des services Internet (IIS), développez **Sites**, cliquez sur **Default Web Site**, puis dans le volet Actions, cliquez sur **Liaisons**.
2. Dans la boîte de dialogue **Liaisons de sites**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter la liaison de site**, sous **Type**, sélectionnez **https** et sous **Port**, vérifiez que **443** est sélectionné. Dans la liste déroulante **Certificat SSL**, cliquez sur **LON-SVR1.adatum.com**, puis sur **OK**.
4. Cliquez sur **Fermer**, puis fermez le **Gestionnaire des services Internet (IIS)**.
5. Sur LON-DC1, ouvrez Windows® Internet Explorer®.
6. Connectez-vous à https://lon-svr1.adatum.com/adatumtestapp. Cliquez sur **OK**.
7. Vérifiez que vous pouvez vous connecter au site, mais que vous recevez une erreur d'accès refusé 401. Cela est normal, car vous n'avez pas encore configuré AD FS pour l'authentification.
8. Fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous devez avoir configuré le transfert DNS pour activer la résolution de noms entre A. Datum et Trey Research et échangé des certificats racines entre les deux organisations. Vous devez avoir également installé et configuré un certificat Web sur le serveur d'applications.

Exercice 2 : Installation et configuration d'AD FS

▶ Tâche 1 : Installer et configurer AD FS

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services AD FS (Active Directory Federation Services)**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Services AD FS (Active Directory Federation Services)**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer** et patientez jusqu'à la fin de l'installation. Ne fermez pas la fenêtre.

▶ Tâche 2 : Créer un serveur de fédération autonome à l'aide de l'Assistant Configuration du serveur de fédération AD FS

1. Sur la page **Progression de l'installation**, cliquez sur **Exécuter le composant logiciel enfichable Gestion AD FS**.
2. Dans le volet Vue d'ensemble, cliquez sur le lien **Assistant Configuration du serveur de fédération AD FS**.
3. Sur la page **Bienvenue**, vérifiez que l'option **Créer un service de fédération** est sélectionnée, puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner un déploiement autonome ou de batterie**, cliquez sur **Serveur de fédération autonome**, puis cliquez sur **Suivant**.
5. Sur la page **Spécifier le nom du service de fédération**, vérifiez que le **Certificate SSL** sélectionné est **LON-DC1.Adatum.com**, le **port** est **443** et que le **Nom du service de fédération** est **LON-DC1.Adatum.com**, puis cliquez sur **Suivant**.
6. Sur la page **Prêt à appliquer les paramètres**, vérifiez que les paramètres de configuration corrects sont répertoriés, puis cliquez sur **Suivant**.
7. Patientez jusqu'à la fin de la configuration, puis cliquez sur **Fermer**.

▶ Tâche 3 : Vérifier que le fichier FederationMetaData.xml est présent et contient des données valides

1. Connectez-vous à l'ordinateur virtuel LON-CL1 en tant que **Adatum\Brad** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur Internet Explorer dans la barre des tâches.
3. Cliquez sur l'icône **Outils** dans le coin supérieur droit, puis cliquez sur **Options Internet**.
4. Sous l'onglet **Sécurité**, cliquez sur **Intranet local**.
5. Cliquez sur **Sites** et désactivez la case à cocher **Détecter automatiquement le réseau Intranet**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Cliquez sur **Avancé** et dans la zone **Ajouter ce site Web à la zone,** saisissez **https://lon-dc1.adatum.com**, puis cliquez sur **Ajouter**.
7. Saisissez **https://lon-svr1.adatum.com**, cliquez sur **Ajouter**, puis sur **Fermer**.
8. Cliquez sur **OK** à deux reprises.
9. Connectez-vous à https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml.
10. Vérifiez que le fichier xml s'ouvre avec succès, puis parcourez son contenu.
11. Fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous aurez installé et configuré le rôle serveur AD FS et vérifié la réussite de l'installation en affichant le contenu du fichier FederationMetaData.xml.

Exercice 3 : Configuration d'AD FS pour une seule organisation

▶ Tâche 1 : Configurer un certificat de signature de jetons pour LON-DC1.Adatum.com

1. Sur l'ordinateur virtuel LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Windows PowerShell**.
2. À l'invite Windows PowerShell, saisissez **set-ADFSProperties –AutoCertificateRollover $False**, puis appuyez sur Entrée. Cette étape est indispensable afin de pouvoir modifier les certificats qu'utilise AD FS.
3. Fermez la fenêtre Windows PowerShell.
4. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion AD FS**.
5. Dans la console AD FS, dans le volet gauche, développez **Service**, puis cliquez sur **Certificats**.
6. Cliquez avec le bouton droit sur **Certificats**, puis cliquez sur **Ajouter un certificat de signature de jetons**.
7. Dans la boîte de dialogue **Sélectionner un certificat de signature de jetons**, cliquez sur le premier certificat nommé **LON-DC1.Adatum.com**, puis cliquez sur **Cliquez ici pour afficher les propriétés du certificat**.
8. Vérifiez que les rôles du certificat incluent **Garantit votre identité auprès d'un ordinateur distant** et **Garantit l'identité d'un ordinateur distant**, puis cliquez sur **OK**. Le certificat peut également avoir d'autres rôles, mais ces deux-là sont obligatoires. Si le certificat n'a pas les rôles nécessaires, affichez les propriétés des autres certificats jusqu'à ce que vous en trouviez un avec les rôles prévus, puis cliquez sur **OK**.
9. Quand la boîte de dialogue d'avertissement Gestion AD FS s'affiche, cliquez sur **OK**.

 **Remarque :** Vérifiez que le certificat a l'objet **CN=LON-DC1.Adatum.com**. Si aucun nom ne s'affiche sous l'objet lorsque vous ajoutez le certificat, supprimez le certificat et ajoutez le certificat suivant dans la liste.

10. Cliquez avec le bouton droit sur le certificat ajouté récemment, puis cliquez sur **Définir en tant que certificate principal**. Lisez le message d'avertissement, puis cliquez sur **Oui**.
11. Sélectionnez le certificat qui vient d'être remplacé, cliquez avec le bouton droit sur le certificat, puis cliquez sur **Supprimer**. Cliquez sur **Oui** pour confirmer la suppression.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer l'approbation de fournisseur de revendications Active Directory

1. Sur LON-DC1, dans la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de fournisseur de revendications**.
2. Dans le volet central, cliquez avec le bouton droit sur **Active Directory**, puis cliquez sur **Modifier les règles de revendication**.
3. Dans la boîte de dialogue **Modifier les règles de revendication pour Active Directory**, sur l'onglet **Règles de transformation d'approbation**, cliquez sur **Ajouter une règle**.
4. Dans l'Assistant Ajouter une règle de revendication de transformation, sur la page **Sélectionner un modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Envoyer les attributs LDAP en tant que revendications**, puis cliquez sur **Suivant**.
5. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Règle d'attributs LDAP sortants**.
6. Dans la liste déroulante **Magasin d'attributs**, sélectionnez **Active Directory**.
7. Dans la section **Mappage des attributs LDAP aux types de revendications sortantes**, sélectionnez les valeurs suivantes pour l'attribut LDAP et le type de revendication sortante :
   - Adresses de messagerie = **E-Mail-Addresses**
   - User-Principal-Name = **UPN**
   - Display-Name = **Nom**
8. Cliquez sur **Terminer**, puis sur **OK**.

▶ Tâche 3 : Configurer l'application de revendications pour approuver les revendications entrantes en exécutant l'Utilitaire de fédération Windows Identity Foundation

1. Sur LON-SVR1, cliquez sur l'écran d'**accueil**, puis cliquez sur **Windows Identity Foundation Federation Utility**.
2. Sur la page **Welcome to the Federation Utility wizard**, dans **Application configuration location**, saisissez **C:\inetpub\wwwroot\AdatumTestApp\web.config** pour l'emplacement du fichier web.config de l'exemple d'application Windows Identity Foundation.
3. Dans **Application URI**, saisissez **https://lon-svr1.adatum.com/AdatumTestApp/** pour indiquer le chemin d'accès à l'exemple d'application qui approuvera les revendications entrantes du serveur de fédération. Cliquez sur **Next** pour continuer.
4. Sur la page **Security Token Service**, sélectionnez l'option **Use an existing STS**, saisissez **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml** pour l'emplacement du document de métadonnées WS-Federation du STS, puis cliquez sur **Next** pour continuer.
5. Sur la page Security Token Service, sélectionnez l'option **No encryption**, puis cliquez sur **Next**.
6. Sur la page **Offered claims**, vérifiez les revendications qui seront offertes par le serveur de fédération, puis cliquez sur **Next**.
7. Sur la page **Summary**, vérifiez les modifications qui seront apportées à l'exemple d'application par l'Assistant Utilitaire de fédération, faites défiler les éléments pour comprendre ce que fait chaque élément, puis cliquez sur **Finish**.
8. Cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer une approbation de partie de confiance pour l'application prenant en charge les revendications

1. Sur LON-DC1, dans la console AD FS, cliquez sur **AD FS**.
2. Dans le volet central, cliquez sur **Requis : ajouter une partie de confiance approuvée**.
3. Dans l'Assistant Ajouter une approbation de partie de confiance, sur la page **Bienvenue**, cliquez sur **Démarrer**.
4. Sur la page **Sélectionner une sources de données**, sélectionnez l'option **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confience**, puis saisissez **https://lon-svr1.adatum.com/adatumtestapp**.
5. Cliquez sur **Suivant** pour continuer. Cette action invite l'Assistant à vérifier les métadonnées de l'application que le rôle serveur Web héberge.
6. Sur la page **Entrer le nom complet**, dans la zone **Nom complet**, saisissez **ADatum Test App**, puis cliquez sur **Suivant**.
7. Sur la page **Choisir les règles d'autorisation d'émission**, vérifiez que l'option **Authoriser l'accés de tous les utilisateurs à cette partie de confiance** est sélectionnée, puis cliquez sur **Suivant**.
8. Sur la page **Prêt à ajouter l'approbation**, vérifiez les paramètres d'approbation de partie de confiance, puis cliquez sur **Suivant**.
9. Sur la page **Terminer**, cliquez sur **Fermer**. La boîte de dialogue **Modifier les règles de revendication pour ADatum Test App** s'ouvre.

▶ Tâche 5 : Configurer les règles de revendication pour l'approbation de partie de confiance

1. Dans la boîte de dialogue **Modifier les règles de revendication pour Adatum Test App**, sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
2. Dans l'Assistant Ajouter une règle de revendication de transformation, sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**. Cette action passe une revendication entrante à l'utilisateur à l'aide de l'authentification Windows intégrée.
3. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Passer la règle du nom de compte Windows**. Dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom de compte Windows**, puis cliquez sur **Terminer**.
4. Cliquez sur **Ajouter une règle**.
5. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**.
6. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Passer la règle d'adresse de messagerie**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Adresse de messagerie**, puis cliquez sur **Terminer**.
7. Cliquez sur **Ajouter une règle**.
8. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**.
9. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication,** saisissez **Passer la règle du nom d'utilisateur principal**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **UPN**, puis cliquez sur **Terminer**.

10. Cliquez sur **Ajouter une règle**.
11. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**.
12. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Passer la règle du nom**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom**, puis cliquez sur **Terminer**.
13. Cliquez sur **Appliquer**, puis sur **OK**.

▶ Tâche 6 : Tester l'accès à l'application prenant en charge les revendications

1. Sur LON-CL1, démarrez Internet Explorer.
2. Connectez-vous à **https://lon-svr1.adatum.com/AdatumTestApp/**.

Remarque : Vérifiez que vous saisissez bien la barre oblique (/) à la fin de l'adresse.

3. Si vous êtes invité à indiquer vos informations d'identification, saisissez **Adatum\Brad** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. La page s'affiche et vous voyez les revendications qui ont été traitées pour permettre l'accès au site Web.

Résultats : À la fin de cet exercice, vous aurez configuré les services AD FS pour une seule organisation. Pour ce faire, vous devez avoir configuré un certificat de signature de jetons ainsi qu'une approbation de fournisseur de revendications pour Adatum.com. Vous devez également avoir configuré l'exemple d'application pour approuver les revendications entrantes et configuré une approbation de partie de confiance et les règles de revendication associées. Vous devez également avoir testé l'accès à l'exemple d'application Windows Identity Foundation dans un seul scénario d'organisation.

Exercice 4 : Configuration d'AD FS pour des partenaires commerciaux fédérés

▶ Tâche 1 : Ajouter une approbation de fournisseur de revendications pour le serveur AD FS de TreyResearch.net

1. Sur LON-DC1, le cas échéant, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion AD FS**.
2. Dans la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de fournisseur de revendications**.
3. Dans le volet **Actions**, cliquez sur **Ajouter une approbation de fournisseur de revendications**.
4. Sur la page **Bienvenue**, cliquez sur **Démarrer**.
5. Sur la page **Sélectionner une source de données**, sélectionnez **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confience**, saisissez **https://mun-dc1.treyresearch.net**, puis cliquez sur **Suivant**.
6. Sur la page **Entrer le nom complet**, cliquez sur **Suivant**.
7. Sur la page **Prêt à ajouter l'approbation**, examinez les paramètres d'approbation de fournisseur de revendications, puis cliquez sur **Suivant** pour enregistrer la configuration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Sur la page **Terminer**, cliquez sur **Fermer**.
9. Dans la boîte de dialogue **Modifier les règles de revendication pour mun-dc1.treyresearch.net Propriétés**, sur l'onglet **Règles de transformation d'acceptation**, cliquez sur **Ajouter une règle**.
10. Dans la liste **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**.
11. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passer la règle du nom de compte Windows**.
12. Dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom de compte Windows**.
13. Sélectionnez **Passer toutes les valeurs de revendication**, puis cliquez sur **Terminer**. Cliquez sur **Oui**.
14. Cliquez sur **OK**, puis fermez la console AD FS.
15. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Windows PowerShell**.
16. À l'invite Windows PowerShell, saisissez la commande suivante et appuyez sur Entrée :

```
Set-ADFSClaimsProviderTrust –TargetName “mun-dc1.treyresearch.net” –
SigningCertificateRevocationCheck None
```

17. Fermez Windows PowerShell.

▶ Tâche 2 : Configurer une approbation de partie de confiance sur MUN-DC1 pour l'application prenant en charge les revendications A. Datum

1. Sur MUN-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestion AD FS**.
2. Dans la console AD FS, sur la page **Vue d'ensemble**, cliquez sur **Requis : ajouter une partie de confiance approuvée**.
3. Sur la page **Bienvenue**, cliquez sur **Démarrer**.
4. Sur la page **Sélectionner une source de données**, sélectionnez l'option **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confience**, saisissez **https://lon-dc1.adatum.com**, puis cliquez sur **Suivant**.
5. Sur la page **Entrer le nom complet**, dans la zone de texte **Nom complet**, saisissez **Adatum TestApp**, puis cliquez sur **Suivant**.
6. Sur la page **Choisir les règles d'autorisation d'émission**, sélectionnez l'option **Autoriser l'accès de tous les utilisateurs à cette partie de confiance**, puis cliquez sur **Suivant**.
7. Sur la page **Prêt à ajouter l'approbation**, examinez les paramètres d'approbation de la partie de confiance, puis cliquez sur **Suivant** pour enregistrer la configuration.
8. Sur la page **Terminer**, cliquez sur **Fermer**. La boîte de dialogue Modifier les règles de revendication pour Adatum TestApp s'ouvre.
9. Dans la boîte de dialogue Modifier les règles de revendication pour Adatum TestApp, sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
10. Dans la liste **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la zone **Nom de la règle de revendication**, saisissez **Passer la règle du nom de compte Windows**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom de compte Windows**.
12. Sélectionnez **Passer toutes les valeurs de revendication**, puis cliquez sur **Terminer**.
13. Cliquez sur **OK**, puis fermez la console AD FS.

▶ Tâche 3 : Vérifier l'accès à l'application de test A. Datum pour les utilisateurs de Trey Research

1. Sur MUN-DC1, ouvrez Internet Explorer et connectez-vous à **https://lon-svr1.adatum.com/adatumtestapp/**.

Remarque : Le processus de connexion a changé et vous devez désormais sélectionner une autorité qui peut autoriser et valider la demande d'accès. La page de découverte du domaine d'accueil (la page Se connecter) s'affiche et vous devez sélectionner une autorité.

2. Sur la page **Connexion**, sélectionnez **mun-dc1.treyresearch.net**, puis cliquez sur **Continuer la connexion**.
3. Si vous êtes invité à indiquer vos informations d'identification, saisissez **TreyResearch\April** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée.
4. Vérifiez que vous avez accès à l'application.
5. Fermez Internet Explorer.
6. Ouvrez Internet Explorer et connectez-vous à nouveau à **https://lon-svr1.adatum.com/adatumtestapp/**.
7. Si vous êtes invité à indiquer vos informations d'identification, saisissez **TreyResearch\April** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. Vous devez pouvoir accéder à l'application.

Remarque : À nouveau, vous n'êtes pas invité à sélectionner un domaine d'accueil. Une fois que les utilisateurs ont sélectionné un domaine d'accueil et ont été authentifiés par une autorité du domaine, ils reçoivent un cookie _LSRealm du serveur de fédération de la partie de confiance. La durée de vie par défaut pour le cookie est de 30 jours. Par conséquent, pour se connecter à plusieurs reprises, vous devez supprimer ce cookie après chaque tentative de connexion pour revenir un état propre.

8. Fermez Internet Explorer.

▶ Tâche 4 : Configurer les règles de revendication pour que l'approbation de fournisseur de revendications et l'approbation de partie de confiance autorisent l'accès à un seul groupe

1. Sur MUN-DC1, ouvrez la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de partie de confiance**.
2. Sélectionnez **Adatum TestApp** et dans le volet Actions, cliquez sur **Modifier les règles de revendication**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue Modifier les règles de revendication pour Adatum TestApp, sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
4. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Envoyer l'appartenance à un groupe en tant que revendication**, puis cliquez sur **Suivant**.
5. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Autoriser la règle du groupe Production**.
6. En regard de **Groupe d'utilisateurs**, cliquez sur **Parcourir**, saisissez **Production**, puis cliquez sur **OK**.
7. Sous **Type de revendication sortante**, cliquez sur **Groupe**.
8. Sous **Valeur de revendication sortante**, saisissez **Production**, puis cliquez sur **Terminer**. Cliquez sur **OK**.
9. Sur LON-DC1, si nécessaire, ouvrez la console AD FS.
10. Dans la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de fournisseur de revendications**.
11. Sélectionnez **mun-dc1.treyresearch.net** et dans le volet Actions, cliquez sur **Modifier les règles de revendication**.
12. Sur l'onglet **Règles de transformation d'acceptation**, cliquez sur **Ajouter une règle**.
13. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**.
14. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Envoyer la règle du groupe Production**.
15. Dans la liste déroulante **Type de revendication entrante**, cliquez sur **Groupe**, puis sur **Terminer**. Cliquez sur **Oui**, puis sur **OK**.
16. Dans la console AD FS, sous **Relations d'approbation**, cliquez sur **Approbations de la partie de confiance**.
17. Sélectionnez **ADatum Test App** et dans le volet Actions, cliquez sur **Modifier les règles de revendication**.
18. Sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
19. Sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
20. Dans la zone **Nom de la règle de revendication**, saisissez **Envoyer la règle du nom de groupe TreyResearch**.
21. Dans la liste déroulante **Type de revendication entrante**, cliquez sur **Groupe**, puis sur **Terminer**.
22. Dans la boîte de dialogue **Modifier les règles de revendication pour ADatum Test App**, sur l'onglet **Règles d'autorisation d'émission**, sélectionnez la règle nommée **Autoriser l'accès à tous les utilisateurs**, puis cliquez sur **Supprimer la règle**. Cliquez sur **Oui** pour confirmer. Sans règle, l'accès est refusé aux utilisateurs.
23. Sur l'onglet **Règles d'autorisation d'émission,** cliquez sur **Ajouter une règle**.
24. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Autoriser ou refuser l'accès des utilisateurs en fonction d'une revendication entrante**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

25. Sur la page **Configurer la règle**, dans la boîte **Nom de la règle de revendication**, saisissez **Autoriser la règle du groupe Production TreyResearch**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Groupe**, dans **Valeur de revendication entrante**, saisissez **Production**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.
26. Sur l'onglet **Règles d'autorisation d'émission,** cliquez sur **Ajouter une règle**.
27. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Autoriser ou refuser l'accès des utilisateurs en fonction d'une revendication entrante**, puis cliquez sur **Suivant**.
28. Sur la page **Configurez la règle**, dans la boîte **Nom de la règle de revendication**, saisissez **Temp**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **UPN**, dans le champ **Valeur de revendication entrante**, saisissez **@adatum.com**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.
29. Cliquez sur la règle **Temp**, puis cliquez sur **Modifier une règle**.
30. Dans la boîte de dialogue **Modifier la règle – Temp**, cliquez sur **Afficher le langage de règles**.
31. Appuyez sur **Ctrl + C** pour copier le langage des règles dans le presse-papiers, puis cliquez sur **OK**.
32. Cliquez sur **Annuler**.
33. Cliquez sur la règle **Temp**, sur **Supprimer la règle**, puis sur **Oui**.
34. Sur l'onglet **Règles d'autorisation d'émission,** cliquez sur **Ajouter une règle**.
35. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Envoyer les revendications en utilisant une règle personnalisée**, puis cliquez sur **Suivant**.
36. Sur la page **Configurer la règle**, dans la boîte **Nom de la règle de revendication**, saisissez **Règle d'accès utilisateur ADatum**.
37. Cliquez dans la zone **Règle personnalisée** et appuyez sur les touches Crtl + V pour coller le contenu du presse-papiers dans la zone. Modifiez la première URL afin qu'elle corresponde au texte suivant, puis cliquez sur **Terminer**.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", Value =~
"^(?i).+@adatum\.com$"]=> issue(Type =
“http://schemas.microsoft.com/authorization/claims/permit”, Value =
“PermitUsersWithClaim”);
```



Remarque : Cette règle permet l'accès à toute personne qui présente une revendication dont le Nom d'utilisateur principal (UPN) est @adatum.com. La ligne Valeur de la première URL définit l'attribut qui peut être mis en correspondance dans la revendication. Dans cette ligne, ^ indique le début de la chaîne à faire correspondre, (?i) signifie que le texte n'est pas sensible à la casse, .+ signifie qu'un ou plusieurs caractères seront ajoutés et $ signifie la fin de la chaîne.

38. Cliquez sur **OK** pour fermer la page de propriétés et sauvegardez les modifications apportées à l'approbation de partie de confiance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Vérifier les restrictions et l'accessibilité à l'application prenant en charge les revendications

1. Sur MUN-DC1, ouvrez Internet Explorer et connectez-vous à **https://lon-svr1.adatum.com/adatumtestapp/**.
2. Si vous êtes invité à indiquer vos informations d'identification, saisissez **TreyResearch\April** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. April n'est pas membre du groupe Production, elle ne doit donc pas avoir accès à l'application.
3. Fermez Internet Explorer.
4. Rouvrez Internet Explorer, cliquez sur l'icône **Outils** dans le coin supérieur droit, puis cliquez sur **Options Internet**.
5. Sous **Historique de navigation**, cliquez sur **Supprimer**, cliquez à nouveau sur **Supprimer**, puis sur **OK**.
6. Connectez-vous à **https://lon-svr1.adatum.com/adatumtestapp/**.
7. Sur la page **Se connecter**, cliquez sur **mun-dc1.treyresearch.net**, puis sur **Continuer la connexion**.
8. Si vous êtes invité à indiquer vos informations d'identification, saisissez **TreyResearch\Morgan** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. Morgan est membre du groupe Production et doit pouvoir accéder à l'application.
9. Fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous aurez configuré une approbation de fournisseur de revendications pour Trey Research sur Adatum.com et une approbation de partie de confiance pour Adatum sur TreyResearch.net. Vous avez vérifié l'accès à l'application A. Datum prenant en charge les revendications. Vous avez configuré ensuite l'application pour limiter l'accès à partir de TreyResearch aux groupes spécifiques et vous avez vérifié l'accès approprié.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-MUN-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-CL1**, **22412B-LON-SVR1** et **22412B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9 : Implémentation de l'équilibrage de la charge réseau

Atelier pratique : Implémentation de l'équilibrage de la charge réseau

Exercice 1 : Implémentation d'un cluster d'équilibrage de la charge réseau

▶ Tâche 1 : Vérifier la fonctionnalité de site Web pour les serveurs autonomes

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
2. Naviguez vers le dossier **c:\inetpub\wwwroot**.
3. Double-cliquez sur le fichier **iis-8**. Cette opération permettra d'ouvrir le fichier dans Microsoft® Paint.
4. Assurez-vous que l'outil **Pinceaux** est sélectionné, puis dans la palette, cliquez sur la couleur **Rouge**.
5. Utilisez la souris pour différencier le logo IIS à l'aide de la couleur rouge.
6. Enregistrez les modifications effectuées dans le fichier **iis-8**, puis fermez Microsoft Paint.
7. Fermez l'Explorateur de fichiers.
8. Basculez vers LON-DC1.
9. Cliquez sur l'écran d'accueil.
10. Sur le bureau, cliquez sur l'icône de Windows® Internet Explorer®.
11. Dans la barre d'adresses d'Internet Explorer, tapez l'adresse **http://LON-SVR1**,, puis appuyez sur Entrée. Vérifiez que la page Web affiche le logo IIS avec la marque de différenciation de couleur rouge que vous avez ajoutée.
12. Dans la barre d'adresses d'Internet Explorer, entrez l'adresse **http://LON-SVR2**,, puis appuyez sur Entrée. Vérifiez que la page Web n'affiche pas le logo IIS marqué.
13. Fermez Internet Explorer.

▶ Tâche 2 : Installer l'équilibrage de la charge réseau (NLB)

1. Basculez vers LON-SVR1.
2. Sur le bureau, cliquez sur l'icône du Gestionnaire de serveur.
3. Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Windows PowerShell ISE**.
4. Dans la fenêtre Windows PowerShell® ISE, entrez la commande suivante et appuyez sur Entrée :

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-
WindowsFeature NLB,RSAT-NLB}
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Créer un nouveau cluster NLB dans Windows Server 2012

1. Sur LON-SVR1, dans la fenêtre Windows PowerShell ISE, saisissez la commande suivante et appuyez sur Entrée :

```
New-NlbCluster -InterfaceName "Connexion au réseau local" -OperationMode Multicast -
ClusterPrimaryIP 172.16.0.42 -ClusterName LON-NLB
```

2. Dans la fenêtre Windows PowerShell ISE, saisissez la commande suivante et appuyez sur Entrée :

```
Invoke-Command -Computername LON-DC1 -command {Add-DNSServerResourceRecordA      –
zonename adatum.com –name LON-NLB –Ipv4Address 172.16.0.42}
```

▶ Tâche 4 : Ajouter un deuxième hôte au cluster

- Sur LON-SVR1, dans la fenêtre Windows PowerShell ISE, saisissez la commande suivante et appuyez sur Entrée :

```
Add-NlbClusterNode -InterfaceName "Connexion au réseau local" -NewNodeName "LON-SVR2"
-NewNodeInterface "Connexion au réseau local"
```

▶ Tâche 5 : Valider le cluster NLB

1. Sur LON-SVR1, dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis cliquez sur **Gestionnaire d'équilibrage de la charge réseau**.
2. Dans le Gestionnaire d'équilibrage de la charge réseau, vérifiez que les nœuds LON-SVR1 et LON-SVR2 s'affichent avec l'état **Convergé** pour le cluster LON-NLB.
3. Cliquez avec le bouton droit sur le cluster **LON-NLB**, puis cliquez sur **Propriétés du cluster**.
4. Dans la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**, sous l'onglet **Paramètres de cluster**, vérifiez que le cluster est défini pour utiliser le mode d'opérations de **multidiffusion**.
5. Sous l'onglet **Règles de port**, vérifiez qu'il n'y a qu'une seule règle de port nommée **Tous** qui commence au port **0** et se termine au port **65535** pour le protocole **TCP** et le protocole **UDP**, et utilise l'affinité **Unique**.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**.

Résultats : À la fin de cet exercice, vous aurez implémenté un cluster NLB avec succès.

Exercice 2 : Configuration et gestion d'un cluster NLB

▶ Tâche 1 : Configurer les règles et l'affinité de port

1. Sur LON-SVR2, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. Dans l'invite Windows PowerShell, tapez chacune des commandes suivantes, en appuyant sur Entrée après chaque commande :

```
Cmd.exe
Mkdir c:\porttest
Xcopy /s c:\inetpub\wwwroot c:\porttest
Exit
New-Website –Name PortTest –PhysicalPath “C:\porttest” –Port 5678
New-NetFirewallRule –DisplayName PortTest –Protocol TCP –LocalPort 5678
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
4. Cliquez sur le lecteur **C**, double-cliquez sur le dossier **porttest**, puis double-cliquez sur **iis-8.png**. Cette opération permettra d'ouvrir le fichier dans Microsoft Paint.
5. Sélectionnez la couleur bleu dans la palette, et utilisez le pinceau **Bleu** pour différencier le logo IIS.
6. Enregistrez les modifications effectuées dans le fichier **iis-8.png**, puis fermez Microsoft Paint.
7. Basculez vers LON-DC1.
8. Cliquez sur l'écran d'accueil.
9. Dans l'écran d'accueil, cliquez sur l'icône Internet Explorer.
10. Dans la barre d'adresses d'Internet Explorer, tapez l'adresse **http://LON-SVR2:5678**, puis appuyez sur Entrée.
11. Vérifiez que la page de démarrage IIS comportant le logo IIS soit identifiée par les marquages bleus.
12. Basculez vers LON-SVR1.
13. Sur LON-SVR1, basculez vers le **Gestionnaire d'équilibrage de la charge réseau**.
14. Dans le Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-NLB**, puis cliquez sur **Propriétés du cluster**.
15. Dans la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**, sous l'onglet **Règles de port**, sélectionnez la règle **Tous**, puis cliquez sur **Supprimer**.
16. Sous l'onglet **Règles de port**, cliquez sur **Ajouter**.
17. Dans la boîte de dialogue **Ajouter/Modifier une règle de port**, entrez les informations suivantes, puis cliquez sur **OK** :
    - Étendue du port : **80 à 80**
    - Protocoles : **Les deux**
    - Mode de filtrage : **Hôte multiple**
    - Affinité : **Aucun**
18. Sous l'onglet **Règles de port**, cliquez sur **Ajouter**.
19. Dans la boîte de dialogue **Ajouter/Modifier une règle de port**, entrez les informations suivantes, puis cliquez sur **OK** :
    - Étendue du port : **5678 à 5678**
    - Protocoles : **Les deux**
    - Mode de filtrage : **Hôte unique**
20. Cliquez sur OK pour fermer la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**.
21. Dans le Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Propriétés de l'hôte**.
22. Sur l'onglet **Règles de port**, cliquez sur la règle de port qui a **5678** comme valeur de début et de fin, puis cliquez sur **Modifier**.
23. Cliquez sur la valeur **Priorité de traitement** et modifiez-la avec la valeur **10**.
24. Cliquez sur **OK** deux fois pour fermer à la fois la boîte de dialogue **Ajouter/Modifier une règle de port** et la boîte de dialogue **Propriétés de l'hôte**.

▶ Tâche 2 : Valider les règles de port

1. Basculez vers LON-DC1.
2. Basculez vers l'écran d'accueil.
3. Dans l'écran d'accueil, cliquez sur l'icône Internet Explorer.
4. Dans la Barre d'adresses d'Internet Explorer, tapez **http://lon-nlb** et appuyez sur Entrée.
5. Cliquez sur l'icône **Actualiser** 20 fois. Vérifiez que vous visualisez bien les pages Web avec et sans le marquage de différenciation rouge.
6. Sur LON-DC1, vérifiez qu'Internet Explorer est ouvert.
7. Dans la barre d'adresses d'Internet Explorer, entrez l'adresse **http://LON-NLB:5678**, puis appuyez sur Entrée.
8. Dans la barre d'adresses, cliquez sur l'icône **Actualiser** 20 fois. Vérifiez que vous pouvez afficher seulement la page Web avec le marquage de différenciation bleu.

▶ Tâche 3 : Gérer la disponibilité hôte dans le cluster NLB

1. Basculez vers LON-SVR1.
2. Sélectionnez le Gestionnaire d'équilibrage de la charge réseau.
3. Cliquez avec le bouton droit sur **LON-SVR1**, cliquez sur **Hôte de contrôle**, puis cliquez sur **Suspendre**.
4. Cliquez sur le nœud **LON-NLB**. Vérifiez que le nœud LON-SVR1 s'affiche à l'état **Exécution suspendue** et que le nœud LON-SVR2 s'affiche à l'état **Convergé**.
5. Cliquez avec le bouton droit sur LON-SVR1, cliquez sur **Hôte de contrôle**, puis cliquez sur **Reprendre**.
6. Cliquez avec le bouton droit sur LON-SVR1, cliquez sur **Hôte de contrôle**, puis cliquez sur **Accueil**.
7. Cliquez sur le nœud LON-NLB. Vérifiez que les deux nœuds LON-SVR1 et LON-SVR2 s'affichent maintenant à l'état **Convergé**. Il se peut que vous deviez actualiser l'affichage.

Résultats : À la fin de cet exercice, vous aurez configuré et géré un cluster NLB avec succès.

Exercice 3 : Validation de la haute disponibilité pour le cluster NLB

▶ Tâche 1 : Valider la disponibilité de site Web lorsque l'hôte est indisponible

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. Tapez la commande suivante, puis appuyez sur Entrée :

```
Shutdown /r /t 5
```

3. Basculez vers LON-DC1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Sur LON-DC1, sur le bureau, cliquez sur l'icône d'Internet Explorer.
5. Dans la barre d'adresses d'Internet Explorer, tapez l'adresse **http://LON-NLB**, puis appuyez sur Entrée.
6. Actualisez le site Web 20 fois. Vérifiez que le site Web est disponible au moment où LON-SVR1 redémarre, mais qu'il n'affiche pas la marque de différenciation rouge sur le logo IIS jusqu'à la fin du cycle de réinitialisation de LON-SVR1.

▶ Tâche 2 : Configurer et valider une action Drainer et arrêter

1. Ouvrez une session sur LON-SVR1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$word**.
2. Sur le bureau, cliquez sur l'icône du Gestionnaire de serveur.
3. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire d'équilibrage de la charge réseau**.
4. Dans la console du Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-SVR2**, ensuite cliquez sur **Hôte de contrôle**, puis sur **Drainer et arrêter**.
5. Basculez vers LON-DC1.
6. Dans Internet Explorer, dans la barre d'adresses, tapez **http://lon-nlb**, puis appuyez sur Entrée.
7. Actualisez le site 20 fois et vérifiez que seule la page d'accueil avec le logo IIS rouge s'affiche.

Résultats : À la fin de cet exercice, vous aurez réussi à valider une haute disponibilité pour le cluster NLB.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste Ordinateurs virtuels, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1** et **22412B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10 : Implémentation du clustering avec basculement

Atelier pratique : Implémentation du clustering avec basculement

Exercice 1 : Configuration d'un cluster de basculement

▶ Tâche 1 : Connecter les nœuds de cluster aux cibles iSCSI (Internet Small Computer System Interface)

1. Sur LON-SVR3, dans la Gestion de serveur, cliquez sur **Outils**, puis sur **Initiateur iSCSI**.
2. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
3. Cliquez sur l'onglet **Découverte**.
4. Cliquez sur **Découvrir un portail**.
5. Dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.21**, puis cliquez sur **OK**.
6. Cliquez sur l'onglet **Cibles**.
7. Cliquez sur **Actualiser**.
8. Dans la liste **Cibles**, sélectionnez **iqn.1991-05.com.microsoft:lon-SVR1-target1-target**, puis cliquez sur **Connexion**.
9. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez deux fois sur **OK**.
10. Sur LON-SVR4, dans la Gestion de serveur, cliquez sur **Outils**, puis sur Initiateur iSCSI.
11. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
12. Cliquez sur l'onglet **Découverte**.
13. Cliquez sur **Découvrir un portail**.
14. Dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.21**, puis cliquez sur **OK**.
15. Cliquez sur l'onglet **Cibles**.
16. Cliquez sur **Actualiser**.
17. Dans la liste **Cibles**, sélectionnez **iqn.1991-05.com.microsoft:lon-SVR1-target1-target**, puis cliquez sur **Connexion**.
18. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez deux fois sur **OK**.
19. Sur LON-SVR3, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
20. Développez **Stockage** si nécessaire, puis cliquez sur **Gestion des disques**.
21. Si nécessaire, puis cliquez sur **Gestion des disques**
22. Cliquez avec le bouton droit sur **Disque 1**, puis cliquez sur **En ligne**.
23. Cliquez avec le bouton droit sur **Disque 1**, puis sur **Initialiser le disque**. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

24. Cliquez avec le bouton droit sur l'espace non alloué en regard de **Disque 1**, puis cliquez sur **Nouveau volume simple**.
25. Sur la page de **démarrage**, cliquez sur **Suivant**.
26. Sur la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
27. Sur la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
28. Sur la page **Formater une partition**, dans la zone **Nom de volume**, tapez sur **Données**. Activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
29. Cliquez sur **Terminer**.

Remarque : Si la fenêtre Microsoft Windows s'affiche avec une invite de formatage du disque, cliquez sur **Annuler**.

30. Répétez les étapes 21 à 28 pour les **Disque 2 et Disque 3**.

Remarque : Utilisez Data2 et Data3 comme noms de volume

31. Fermez la fenêtre **Gestion de l'ordinateur**.
32. Sur LON-SVR4, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
33. Développez **Stockage** si nécessaire, puis cliquez sur **Gestion des disques**.
34. Cliquez avec le bouton droit sur **Gestion des disques**, puis cliquez sur **Actualiser**.
35. Cliquez avec le bouton droit sur **Disque 1**, puis cliquez sur **En ligne**.
36. Cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**.
37. Cliquez avec le bouton droit sur **Disque 3**, puis cliquez sur **En ligne**.
38. Fermez la fenêtre Gestion de l'ordinateur.

▶ Tâche 2 : Installer la fonctionnalité Clustering avec basculement

1. Sur LON-SVR3, dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, dans la liste **Fonctionnalités**, cliquez sur **Clustering avec basculement**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Dans la fenêtre Ajouter les fonctionnalités requises pour le clustering avec basculement, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
8. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Une fois l'installation terminée, cliquez sur **Fermer**.
10. Répétez les étapes 1 à 9 sur LON-SVR4.

▶ Tâche 3 : Valider les serveurs pour le clustering avec basculement

1. Sur LON-SVR3, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
2. Dans le volet **Action** de la console du Gestionnaire du cluster de basculement, cliquez sur **Validez la configuration**.
3. Dans l'**Assistant Validation d'une configuration**, cliquez sur **Suivant**.
4. Dans la zone **Entrez un nom**, tapez **LON-SVR3**, puis cliquez sur **Ajouter**.
5. Dans la zone **Entrer un nom**, tapez **LON-SVR4**, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
6. Vérifiez que l'option **Exécuter tous les tests (recommandé)** est sélectionnée, puis cliquez sur **Suivant**.
7. Sur la page **Confirmation**, cliquez sur **Suivant**.
8. Attendez la fin des tests de validation (cela peut prendre jusqu'à 5 minutes), puis sur la page **Résumé**, cliquez sur **Rapport**.
9. Vérifiez que tous les tests ont été réalisés sans erreurs. Certains avertissements peuvent cependant s'afficher.
10. Fermez Windows® Internet Explorer®.
11. Sur la page **Résumé**, décochez la case en regard de **Créer le cluster maintenant en utilisant les nœuds validés**, puis cliquez sur **Terminer**.

▶ Tâche 4 : Créer le cluster de basculement

1. Sur LON-SVR3, dans la console Gestionnaire du cluster de basculement, sous la section **Administration** du volet central, cliquez sur **Créer le cluster**.
2. Dans l'Assistant Création d'un cluster, sur la page **Avant de commencer**, lisez les informations, puis cliquez sur **Suivant**.
3. Dans la zone **Entrer le nom du serveur,** tapez **LON-SVR3**, puis cliquez sur **Ajouter**. Dans la zone **Entrer le nom du serveur**, tapez **LON-SVR4**, puis cliquez sur **Ajouter**.
4. Vérifiez les entrées, puis cliquez sur **Suivant**.
5. Sur la page **Point d'accès pour l'administration du cluster**, entrez **Cluster1** comme Nom du cluster. Sous **Adresse**, tapez **172.16.0.125**, puis cliquez sur **Suivant**.
6. Dans la boîte de dialogue **Confirmation**, vérifiez les informations affichées, puis cliquez sur **Suivant**.
7. Sur la page **Résumé**, cliquez sur **Terminer** pour revenir au Gestionnaire du cluster de basculement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Configurer les volumes partagés de cluster (CSV)

1. Sur LON-SVR3, dans la console Gestionnaire du cluster de basculement, développez **Cluster1.Adatum.com**, développez **Stockage** et cliquez avec le bouton droit sur **Disques**.
2. Dans le volet droit, localisez un disque qui est attribué à **Stockage disponible** (vous pouvez le voir dans la colonne **Attribué à**). Cliquez avec le bouton droit sur ce disque, puis cliquez sur **Ajouter aux volumes partagés de cluster**. (Si possible, utilisez le disque du cluster 2).
3. Assurez-vous que le disque est attribué à **Volume partagé de cluster**.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré la fonctionnalité Clustering avec basculement.

Exercice 2 : Déploiement et configuration d'un serveur de fichiers hautement disponibles

▶ Tâche 1 : Ajouter l'application de serveur de fichiers au cluster de basculement

1. Sur LON-SVR3, dans le Gestionnaire de serveur, cliquez sur **Tableau de bord**, puis cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, sélectionnez **LON-SVR3.Adatum.com**, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI**, et sélectionnez **Serveur de fichiers**.
6. Cliquez deux fois sur **Suivant**.
7. Sur la page **Confirmation**, cliquez sur **Installer**.
8. Lorsque le message **Installation réussie** s'affiche, cliquez sur **Fermer**.
9. Répétez les étapes 1 à 8 sur LON-SVR4. À l'étape 4, sélectionnez **LON-SVR4.Adatum.com.**
10. Sur LON-SVR3, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestionnaire du cluster de basculement** pour ouvrir **Gestionnaire du cluster de basculement**, développez **Cluster1.Adatum.com**, cliquez avec le bouton droit sur **Rôles**, puis cliquez sur **Configurer un rôle**.
11. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
12. Sur la page **Sélectionner un rôle**, sélectionnez **Serveur de fichiers**, puis cliquez sur **Suivant**.
13. Sur la page **Type de serveur de fichiers**, cliquez sur **Serveur de fichiers avec montée en puissance parallèle pour les données d'application**, puis sur **Suivant**.
14. Sur la page **Point d'accès client**, dans la zone **Nom**, saisissez **AdatumFS**, puis cliquez sur **Suivant**.
15. Sur la page **Confirmation**, cliquez sur **Suivant**.
16. Sur la page **Résumé**, cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Ajouter un dossier partagé à un serveur de fichiers à haut niveau de disponibilité

1. Sur LON-SVR3, dans la console Gestionnaire du cluster de basculement, cliquez sur **Rôles**, cliquez avec le bouton droit sur **AdatumFS**, puis cliquez sur **Ajouter le partage de fichiers**.

Remarque : Si vous recevez un message d'erreur qui indique que le cluster est encore indisponible, attendez une minute et redémarrez le gestionnaire du cluster de basculement sur un autre nœud.

2. Dans l'**Assistant Nouveau partage**, sur la page **Sélectionner le profil de ce partage**, cliquez sur **Partage SMB – Rapide**, puis cliquez sur Suivant.
3. Sur la page **Sélectionner le serveur et le chemin d'accès au partage**, cliquez sur l'option de **sélection par volume**, puis cliquez sur **Suivant**.
4. Sur la page **Indiquer le nom de partage**, dans la zone **Nom du partage**, tapez **Data**, puis cliquez sur **Suivant**.
5. Sur la page **Configurer les paramètres de partage**, vérifiez que l'option **Activer la disponibilité continue** est sélectionnée, puis cliquez sur **Suivant**.
6. Sur la page **Spécifier les autorisations pour contrôler l'accès**, cliquez sur **Suivant**.
7. Sur la page **Confirmation**, cliquez sur **Créer**.
8. Sur la page **Afficher les résultats**, cliquez sur **Fermer**.

▶ Tâche 3 : Configurer les paramètres de basculement et de restauration automatique

1. Sur LON-SVR3, dans le Gestionnaire du cluster de basculement, cliquez sur **Rôles**, cliquez avec le bouton droit sur **AdatumFS**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de AdatumFS**, cliquez sur l'onglet **Basculement**, puis sur **Autoriser la restauration automatique**.
3. Cliquez sur **Restauration entre** et définissez les valeurs sur **4** et **5** heures.
4. Cliquez sur l'onglet **Général**, puis sélectionnez **LON-SVR3** et **LON-SVR4** comme propriétaires favoris.
5. Faites remonter **LON-SVR4**, puis cliquez sur **OK**.

▶ Tâche 4 : Valider des paramètres de quorum de cluster

1. Dans le Gestionnaire du cluster de basculement, cliquez sur **Cluster1.Adatum.com**.
2. Dans le volet central, vérifiez le paramétrage de la **Configuration de Quorum**. Il devrait être défini sur **Nœud et disque majoritaires**.

Résultats : À la fin de cet exercice, vous aurez déployé et configuré un serveur de fichiers à haut niveau de disponibilité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Validation du déploiement du serveur de fichier hautement disponibles

▶ Tâche 1 : Valider le déploiement du serveur de fichiers à haut niveau de disponibilité

1. Sur LON-DC1, sur le bureau, cliquez sur l'icône de l'Explorateur de fichiers.
2. Dans l'Explorateur de fichiers, dans la barre d'adresses, tapez **\\AdatumFS**, puis appuyez sur Entrée.
3. Vérifiez que vous pouvez accéder à l'emplacement et que vous pouvez ouvrir le dossier **Data**. Créez un document texte de test dans ce dossier.
4. Sur LON-SVR3, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
5. Dans la console Gestionnaire du cluster de basculement, développez **Cluster1.adatum.com**, puis cliquez sur **Rôles**. Notez le propriétaire actuel d'AdatumFS.

Remarque : Vous pouvez afficher le nom du propriétaire dans la colonne de nœud de propriétaire. Il s'agira de LON-SVR3 ou LON-SVR4).

6. Cliquez avec le bouton droit sur **AdatumFS**, puis cliquez sur **Déplacer**, puis sur **Sélectionnez un nœud**.
7. Dans la boîte de dialogue **Déplacer le rôle en cluster**, cliquez sur **OK**.
8. Vérifiez qu'**AdatumFS** a été déplacé vers un nouveau propriétaire.
9. Basculez vers LON-DC1.
10. Sur LON-DC1, vérifiez que vous pouvez encore accéder à l'emplacement **\\AdatumFS**.

▶ Tâche 2 : Valider la configuration de basculement et de quorum pour le rôle de serveur de fichiers

1. Sur LON-SVR3, dans le Gestionnaire du cluster de basculement, cliquez sur **Rôles**.
2. Vérifiez le propriétaire actuel pour le rôle AdatumFS.

Remarque : Vous pouvez afficher le propriétaire dans la colonne de nœud de propriétaire, qui peut être LON-SVR3 ou LON-SVR4.

3. Développez **Nœuds**, puis sélectionnez le nœud qui est le propriétaire actuel du rôle AdatumFS.
4. Cliquez avec le bouton droit sur le nœud, cliquez sur **Autres actions**, puis cliquez sur **Arrêter le service de cluster**.
5. Dans la boîte de dialogue **Arrêter le service de cluster**, cliquez sur **Oui**.
6. Vérifiez qu'**AdatumFS** a été déplacé vers un autre nœud. Pour ce faire, cliquez sur l'autre nœud et vérifiez qu'AdatumFS est en cours d'exécution.
7. Basculez vers l'ordinateur LON-DC1.
8. Vérifiez que vous pouvez encore accéder à l'emplacement **\\AdatumFS**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Basculez vers l'ordinateur LON-SVR3.
10. Dans le Gestionnaire du cluster de basculement, cliquez avec le bouton droit sur le nœud arrêté, cliquez sur **Autres actions**, puis cliquez sur **Démarrer le service de cluster**.
11. Dans le Gestionnaire du cluster de basculement, développez **Stockage**, puis cliquez sur **Disques**. Dans le volet central, cliquez avec le bouton droit sur le disque qui est attribué à **Disque témoin dans le quorum**.

Remarque : Pour savoir de quel disque il s'agit, consultez la colonne Attribué à.

12. Cliquez sur **Mettre hors connexion**, puis cliquez sur **Oui**.
13. Basculez vers LON-DC1.
14. Vérifiez que vous pouvez encore accéder à l'emplacement **\\AdatumFS**. Vous avez ainsi vérifié que le cluster continue de s'exécuter, même si le disque témoin est hors connexion.
15. Basculez vers LON-SVR3.
16. Dans le Gestionnaire du cluster de basculement, cliquez sur **Stockage**, cliquez sur **Disques**, cliquez avec le bouton droit sur le disque qui est **Hors connexion**, puis cliquez sur **Mettre en ligne**.

Résultats : À la fin de cet exercice, vous aurez testé les scénarios de basculement et de restauration automatique.

Exercice 4 : Configuration de la mise à jour adaptée aux clusters sur le cluster de basculement

▶ Tâche 1 : Configurer la mise à jour adaptée aux clusters (CAU)

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, dans la liste de fonctionnalités, cliquez sur **Clustering avec basculement**. Dans la boîte de dialogue **Ajouter les fonctionnalités requises pour le clustering avec basculement**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
7. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.
9. Sur LON-DC1, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Mise à jour adaptée aux clusters**.
10. Dans la fenêtre Mise à jour adaptée aux clusters, dans la liste déroulante **Se connecter à un cluster de basculement**, cliquez sur **Cluster1**, puis sur **Connecter**.

11. Dans le volet Actions de cluster, cliquez sur **Cluster1 - Afficher un aperçu des mises à jour**.
12. Dans la fenêtre **Afficher un aperçu des mises à jour-Cluster1**, cliquez sur **Générer la liste des aperçus de mises à jour**. Après quelques minutes, des mises à jour apparaissent dans la liste. Examinez les mises à jour, puis cliquez sur **Fermer**.

Remarque : Une connexion Internet est requise pour compléter cette étape. Vérifiez que le serveur MSL-TMG1 est opérationnel et que vous pouvez accéder à Internet sur LON-DC1. Dans un environnement de production, nous ne recommandons pas de déployer les outils CAU sur un contrôleur de domaine. Cela ne s'applique qu'à l'atelier pratique.

▶ Tâche 2 : Mettre à jour le cluster de basculement et configurer la mise à jour automatique

1. Sur LON-DC1, dans la **console Mise à jour adaptée aux clusters**, cliquez sur **Appliquer les mises à jour à ce cluster**.
2. Sur la page **Mise en route**, cliquez sur **Suivant**.
3. Sur la page **Options avancées**, examinez les options de mise à jour, puis cliquez sur **Suivant**.
4. Sur la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
5. Sur la page **Confirmation**, cliquez sur **Mettre à jour**, puis sur **Fermer**.
6. Dans le volet Nœuds de cluster, examinez la progression de la mise à jour.

Remarque : Notez qu'un nœud du cluster est En attente, tandis que l'autre nœud redémarre une fois qu'il a été mis à jour.

7. Patientez jusqu'à la fin du processus.

Remarque : Le redémarrage des deux nœuds peut être requis. Le processus est terminé lorsque deux nœuds affichent la valeur Opération réussie dans la colonne État de la dernière exécution.

8. Ouvrez une session sur LON-SVR3 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
9. Sur LON-SVR3, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Mise à jour adaptée aux clusters**.
10. Dans la boîte de dialogue **Mise à jour adaptée aux clusters**, dans la liste déroulante **Se connecter à un cluster de basculement**, sélectionnez **Cluster1**, puis cliquez sur **Connecter**.
11. Dans le volet **Actions de cluster**, cliquez sur **Configurer les options de mise à jour automatique du cluster**.
12. Sur la page **Mise en route**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

13. Sur la page **Ajouter le rôle en cluster de la mise à jour adaptée aux clusters avec la mise à jour automatique activée**, cliquez sur **Ajouter le rôle en cluster de la mise à jour adaptée aux clusters, avec le mode de mise à jour automatique activé, à ce cluster**, puis sur **Suivant**.
14. Sur la page **Spécifier la planification de la mise à jour automatique**, cliquez sur **Chaque semaine** et dans la zone **Heure du jour**, cliquez sur **04:00**, puis dans la zone **Jour de la semaine**, cliquez sur **Dimanche**, puis cliquez sur **Suivant**.
15. Sur la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
16. Sur la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
17. Sur la page **Confirmation**, cliquez sur **Appliquer**.
18. Une fois que le rôle en cluster est installé, cliquez sur **Fermer**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré la mise à jour adaptée aux clusters sur le cluster de basculement.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, **22412B-LON-SVR3**, **22412B-LON-SVR4** et **MSL-TMG1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11 : Implémentation du clustering avec basculement à l'aide d'Hyper-V

Atelier pratique : Implémentation du clustering avec basculement à l'aide d'Hyper-V

Exercice 1 : Configuration des réplicas Hyper-V

▶ Tâche 1 : Démarrez les ordinateurs hôtes physiques à partir du disque dur virtuel

1. Redémarrez l'ordinateur de la classe, et dans le **Windows Boot Manager**, cliquez sur **22412B-LON-HOST1** ou **22412B-LON-HOST2**.

Remarque : Si vous démarrez LON-HOST1, votre partenaire doit faire de même avec LON-HOST2.

2. Ouvrez une session en tant que **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Sur LON-HOST1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire Hyper-V**.
4. Assurez-vous que l'ordinateur virtuel **22412B-LON-DC1** est en cours d'exécution.
5. Répétez les étapes 3 et 4 sur LON-HOST2, et assurez-vous que l'ordinateur virtuel **22412B-LON-SVR1** est en cours d'exécution.

▶ Tâche 2 : Importation de l'ordinateur virtuel LON-CORE sur LON-HOST1

1. Sur LON-HOST1, ouvrez la console Gestionnaire Hyper-V.
2. Dans le volet Actions, cliquez sur **Importer un ordinateur virtuel**.
3. Dans l'Assistant Importation d'ordinateur virtuel, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Localiser le dossier**, cliquez sur **Parcourir**.
5. Accédez au dossier **E:\Programmes\Microsoft Learning\22412\Drivers\22412B-LON-CORE**, cliquez sur **Sélectionner un dossier**, puis cliquez sur **Suivant**.

Remarque : La lettre du lecteur peut varier en fonction du nombre de lecteurs sur l'ordinateur hôte physique.

6. Sur la page **Sélectionner l'ordinateur virtuel**, cliquez sur **22412B-LON-CORE**, puis sur **Suivant**.
7. Sur la page **Choisir le type d'importation**, cliquez sur **Suivant**.
8. Sur la page **Résumé**, cliquez sur **Terminer**.
9. Dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22412B-LON-CORE**, cliquez sur **Paramètres**, dans le panneau de navigation, sélectionnez **Carte réseau héritée**, puis sélectionnez **Réseau externe** pour le **Commutateur virtuel.** Cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer un réplica sur les deux ordinateurs hôtes

1. Sur LON-HOST2, ouvrez la console **Gestionnaire Hyper-V®**.
2. Dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **LON-HOST2**, puis cliquez sur **Paramètres Hyper-V**.
3. Dans **Paramètres Hyper-V de LON-HOST2**, cliquez sur **Configuration de la réplication**.
4. Dans le volet Configuration de la réplication, cliquez sur **Activez ce ordinateur en tant que serveur de réplication**.
5. Dans la section Authentification et ports, cliquez sur **Utiliser Kerberos (HTTP)**.
6. Dans la section Autorisation et stockage, cliquez sur **Autoriser la réplication à partir de n'importe quell serveur authentifié**, puis cliquez sur **Parcourir**.
7. Cliquez sur **Ordinateur**, double-cliquez sur **Disque local (E:)**, cliquez sur **Nouveau dossier**, dans la zone de texte **Nom**, entrez **VMReplica**, puis appuyez sur Entrée.
8. Sélectionnez le dossier **E:\VMReplica**, puis cliquez sur **Sélectionner un dossier**.
9. Dans **Paramètres Hyper-V de LON-HOST2**, cliquez sur **OK**.
10. Dans la boîte de dialogue **Paramètres**, lisez la notification et cliquez sur **OK**.
11. Pointez dans l'angle inférieur gauche du Bureau, puis cliquez sur **Paramètres**.
12. Dans Paramètres, cliquez sur **Panneau de configuration**, sur **Système et sécurité**, puis sur **Pare-feu Windows**.
13. Cliquez sur **Paramètres avancés**.
14. Dans Pare-feu Windows avec fonctions avancées de sécurité, cliquez sur **Règles de trafic entrant**.
15. Dans le volet droit, dans la liste de règles, recherchez la règle nommée **Écouteur HTTP de replica Hyper-V (TCP-IN)**. Cliquez avec le bouton droit sur la règle et cliquez sur **Activer la règle**.
16. Fermez la console Pare-feu Windows Firewall avec fonctions avancées de sécurité, puis fermez le Pare-feu Windows.
17. Répétez les étapes 1 à 16 sur LON-HOST1.

▶ Tâche 4 : Configuration de la réplication pour l'ordinateur virtuel LON-CORE

1. Sur LON-HOST1, ouvrez le Gestionnaire Hyper-V, cliquez sur **LON-HOST1**, cliquez avec le bouton droit sur **22412B-LON-CORE**, puis cliquez sur **Activer la réplication**.
2. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Spécifier le serveur de réplication**, cliquez sur **Parcourir**.
4. Dans la fenêtre Sélectionner l'ordinateur, saisissez **LON-HOST2**, cliquez sur **Vérifier les noms**, cliquez sur **OK**, puis sur **Suivant**.
5. Sur la page **Spécifier les paramètres de connexion**, examinez les paramètres et assurez-vous que l'option **Utiliser l'authentification Kerberos (HTTP)** est sélectionnée, puis cliquez sur **Suivant**.
6. Sur la page **Choisir les disques durs virtuels de réplication**, assurez-vous que le fichier **22412B-LON-CORE.vhd** est sélectionné, puis cliquez sur **Suivant**.
7. Sur la page **Configurer l'historique de récupération**, sélectionnez **Uniquement le dernier point de récupération**, puis sur **Suivant**.
8. Sur la page **Choisir la méthode de réplication initiale**, cliquez sur **Envoyer la copie initiale sur le réseau**, sélectionnez **Démarrer la réplication immédiatement**, puis cliquez sur **Suivant**.

9. Sur la page **Fin de l'Assistant Activation de la réplication**, cliquez sur **Terminer**.
10. Patientez 10 à 15 minutes. Dans la console Gestionnaire Hyper-V, vous pouvez suivre la progression de la réplication initiale dans la colonne **Statut**.
11. Quand la réplication est terminée, assurez-vous que **22412B-LON-CORE** s'affiche sur LON-HOST2 dans le Gestionnaire Hyper-V.

▶ Tâche 5 : Valider un basculement planifié vers le site de réplication

1. Sur LON-HOST2, dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22412B-LON-CORE**, cliquez sur **Réplication**, puis sur **Afficher l'intégrité de la réplication**.
2. Dans la fenêtre qui s'affiche, examinez le contenu. Assurez-vous qu'il n'existe aucune erreur, puis cliquez sur **Fermer**.
3. Sur LON-HOST1, ouvrez le **Gestionnaire Hyper-V** et vérifiez que **22412B-LON-CORE** est arrêté.
4. Cliquez avec le bouton droit sur **22412B-LON-CORE**, cliquez sur **Réplication**, puis sur **Basculement planifié**.
5. Dans la fenêtre Basculement planifié, assurez-vous que l'option **Démarrez l'ordinateur virtuel réplica après le basculement** est sélectionnée, puis cliquez sur **Basculement**.
6. Dans la fenêtre Basculement planifié, cliquez sur **Fermer**.
7. Sur LON-HOST2, dans le Gestionnaire Hyper-V, assurez-vous que **22412B-LON-CORE** est en cours d'exécution.
8. Sur LON-HOST1, cliquez avec le bouton droit sur **22412B-LON-CORE**, pointez sur **Réplication**, puis cliquez sur **Supprimer la réplication**.
9. Dans la boîte de dialogue **Supprimer la réplication**, cliquez sur **Supprimer la réplication**.
10. Sur LON-HOST2, cliquez avec le bouton droit sur **22412B-LON-CORE**, puis cliquez sur **Arrêter**.
11. Dans la boîte de dialogue **Arrêter l'ordinateur**, cliquez sur **Arrêter**.

Résultats : À l'issue de cet exercice, vous aurez configuré un réplica Hyper-V.

Exercice 2 : Configuration d'un cluster avec basculement pour Hyper-V

▶ Tâche 1 : Connectez-vous à la cible iSCSI à partir des deux ordinateurs hôtes

1. Sur LON-HOST1, dans la barre des tâches, cliquez sur l'icône **Gestionnaire de serveur**.
2. Dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Initiateur iSCSI**.
3. À l'invite **Microsoft iSCSI**, cliquez sur **Oui**.
4. Cliquez sur l'onglet **Découverte**, puis sur **Découvrir un portail**.
5. Dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.21**, puis cliquez sur **OK**.
6. Cliquez sur l'onglet **Cibles**, puis sur **Actualiser**.
7. Dans la liste Cibles, sélectionnez **iqn.1991-05.com.microsoft:lon-svr1-target1-target**, puis cliquez sur **Connexion**.
8. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez deux fois sur **OK**.
9. Sur LON-HOST2, dans la barre des tâches, cliquez sur l'icône **Gestionnaire de serveur**.
10. Dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Initiateur iSCSI**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
12. Cliquez sur l'onglet **Découverte**, puis sur **Découvrir un portail**.
13. Dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.21**, puis cliquez sur **OK**.
14. Cliquez sur l'onglet **Cibles**, puis sur **Actualiser**.
15. Dans la liste **Cibles découvertes**, sélectionnez **iqn.1991-05.com.microsoft:lon-svr1-target1-target**, puis cliquez sur **Connexion**.
16. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez deux fois sur **OK**.
17. Sur LON-HOST2, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
18. Développez **Stockage**, cliquez sur **Gestion des disques**, cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**.
19. Cliquez de nouveau avec le bouton droit sur **Disque 2,** puis cliquez sur **Initialiser le disque**.
20. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.
21. Cliquez avec le bouton droit sur l'espace non alloué en regard de Disque 2, puis cliquez sur **Nouveau volume simple**.
22. Sur la page de **Assistant Création d'un volume simple**, cliquez sur **Suivant**.
23. Sur la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
24. Sur la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
25. Sur la page **Formater une partition**, dans la zone **Nom de volume**, tapez **ClusterDisk**, activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
26. Cliquez sur **Terminer**.
27. Répétez les étapes 17 à 26 pour le disque 3 et le disque 4. À l'étape 25, indiquez le nom **ClusterVMs** pour le disque 3 et le nom **Quorum** pour le disque 4.
28. Sur LON-HOST1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
29. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
30. Cliquez avec le bouton droit sur **Gestion des disques**, puis cliquez sur **Actualiser**.
31. Cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**.
32. Cliquez avec le bouton droit sur **Disque 3**, puis cliquez sur **En ligne**.
33. Cliquez avec le bouton droit sur **Disque 4**, puis cliquez sur **En ligne**.

▶ Tâche 2 : Configurer un clustering avec basculement sur les deux ordinateurs hôtes

1. Sur LON-HOST1, dans la barre des tâches, cliquez sur l'icône **Gestionnaire de serveur** pour ouvrir le **Gestionnaire de serveur**.
2. À partir du Tableau de bord, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Sur la page **Sélectionner des fonctionnalités**, dans la liste **Fonctionnalités**, cliquez sur **Clustering avec basculement**.
8. À l'invite **Ajouter les fonctionnalités requises pour le Clustering avec basculement**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Une fois l'installation terminée, cliquez sur **Fermer**.
11. Répétez les étapes 1 à 10 sur LON-HOST2.
12. Sur LON-HOST1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
13. Dans le Gestionnaire du cluster de basculement, dans le volet central, sous **Administration**, cliquez sur **Créer le cluster**.
14. Dans l'Assistant Création d'un cluster, sur la page **Avant de commencer**, lisez les informations, puis cliquez sur **Suivant**.
15. Sur la page Sélectionner des serveurs, dans al zone **Nom du serveur**, tapez **LON-HOST1**, puis cliquez sur **Ajouter**.
16. Dans la zone **Nom du serveur**, tapez **LON-HOST2**, puis cliquez sur **Ajouter**.
17. Vérifiez les entrées, puis cliquez sur **Suivant**.
18. Sur la page **Avertissement de validation**, cliquez sur **Non. Je n'ai pas besoin de l'assistance de Microsoft pour ce cluster**, puis cliquez sur **Suivant**.
19. Sur la page **Point d'accès pour l'administration du cluster**, dans le champ **Nom du cluster**, tapez **VMCluster**.
20. Dans la zone **Nom de l'adresse IP**, sous Adresse, tapez **172.16.0.126**, puis cliquez sur **Suivant**.
21. Dans la boîte de dialogue **Confirmation**, vérifiez les informations, désactivez la case à cocher **Ajouter la totalité du stockage disponible au cluster**, puis cliquez sur **Suivant**.
22. Sur la page **Résumé**, cliquez sur **Terminer**.

▶ Tâche 3 : Configuration des disques pour le cluster de basculement

1. Sur LON-HOST1, dans le Gestionnaire du cluster de basculement, développez **VMCluster.Adatum.com**, **Stockage**, cliquez avec le bouton droit sur **Disques**, puis cliquez sur **Ajouter un disque**.
2. Dans la boîte de dialogue **Ajouter des disques à un cluster**, vérifiez que tous les disques sont sélectionnés, puis cliquez sur **OK**.
3. Dans le Gestionnaire du cluster de basculement, vérifiez que tous les disques sont disponibles pour le stockage en cluster.
4. Sélectionnez et cliquez avec le bouton droit sur le disque **ClusterVMs**, puis sélectionnez **Ajouter aux volumes partagés de cluster**.
5. Cliquez avec le bouton droit sur **VMCluster.Adatum.com**, sélectionnez **Autres actions**, cliquez sur **Configurer les paramètres du quorum de cluster**, puis sur **Suivant**.
6. Sur la page **Sélectionner l'option du configuration du quorum**, cliquez sur **Utiliser les paramètres standard**, puis sur **Suivant**.

7. Sur la page **Confirmation**, cliquez sur **Suivant**.
8. Sur la page **Résumé**, cliquez sur **Terminer**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré un cluster de basculement pour Hyper-V.

Exercice 3 : Configuration d'un ordinateur virtuel hautement disponible

▶ Tâche 1 : Déplacer le stockage de l'ordinateur virtuel vers la cible iSCSI

1. Dans le Gestionnaire du cluster de basculement, vérifiez que **LON-HOST1** est le propriétaire du disque **ClusterVMs**. Si tel n'est pas le cas, déplacez le disque ClusterVMs vers LON-HOST1.
2. Sur LON-HOST1, dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
3. Dans la fenêtre de l'Explorateur de fichiers, développez successivement le lecteur **E**, **Programmes**, **Microsoft Learning**, **22412**, **Drivers**, **22412B-LON-CORE**, puis double-cliquez sur **Virtual Hard Disks**.
4. Déplacez le fichier virtuel de disque dur **22412B-LON-CORE.vhd** à l'emplacement de **C:\ClusterStorage\Volume1**.

▶ Tâche 2 : Configurer l'ordinateur virtuel en tant qu'ordinateur à haut niveau de disponibilité

1. Sur LON-HOST1, dans la console Gestionnaire du cluster de basculement, cliquez sur **Rôles**, et dans le volet Actions, cliquez sur **Ordinateurs virtuels**.
2. Cliquez sur **Nouvel ordinateur virtuel**.
3. Sélectionnez **LON-HOST1**, puis cliquez sur **OK**.
4. Dans l'Assistant Nouvel ordinateur virtuel, cliquez sur **Suivant**.
5. Sur la page **Spécifier le nom et l'emplacement**, dans la zone de texte **Nom**, tapez **TestClusterVM**, cliquez sur **Stocker l'ordinateur virtuel à un autre emplacement**, puis sur **Parcourir**.
6. Accédez à et sélectionnez **C:\ClusterStorage\Volume1**, cliquez sur **Sélectionner un dossier**, puis sur **Suivant**.
7. Sur la page **Affecter la mémoire**, tapez **1536**, puis cliquez sur **Suivant**.
8. Sur la page **Configurer la mise en réseau,** cliquez sur **Réseau externe**, puis sur **Suivant**.
9. Sur la page **Connecter un disque dur virtuel,** cliquez sur **Utiliser un disque dur virtuel existant**, puis sur **Parcourir**.
10. Accédez à **C:\ClusterStorage\Volume1**, cliquez sur **22412B-LON-CORE.vhd**,, puis sur **Ouvrir**.
11. Cliquez sur **Suivant**, puis sur **Terminer**.
12. Dans l'Assistant Haute disponibilité, sur la page **Résumé**, cliquez sur **Terminer**.
13. Dans le Gestionnaire du cluster de basculement, dans le nœud Rôles, cliquez avec le bouton droit sur **TestClusterVM**, puis cliquez sur **Redémarrer**.
14. Assurez-vous que l'ordinateur démarre correctement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Exécuter une migration dynamique pour l'ordinateur virtuel

1. Sur LON-HOST1, ouvrez le **Gestionnaire du cluster de basculement**, développez **VMCluster.Adatum.com**, puis cliquez sur **Rôles**.
2. Cliquez avec le bouton droit sur **TestClusterVM**, cliquez sur **Déplacer**, **Migration dynamique**, puis cliquez sur **Sélectionner le nœud**.
3. Cliquez sur **LON-HOST2**, puis sur **OK**.
4. Cliquez avec le bouton droit sur **TestClusterVM**, puis sur **Connecter**.
5. Assurez-vous que vous pouvez accéder à l'ordinateur virtuel et que vous pouvez l'utiliser pendant sa migration vers un autre hôte.
6. Patientez jusqu'à la fin de la migration.

▶ Tâche 4 : Réalisation d'une migration du stockage pour l'ordinateur virtuel

1. Sur LON-HOST2, ouvrez le **Gestionnaire Hyper-V**.
2. Dans le volet central, cliquez sur **22412B-LON-SVR1-B**.
3. Dans le volet Actions, cliquez sur **Déplacer**.
4. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
5. Sur la page **Choisir le type de déplacement**, cliquez sur **Déplacer le stockage de l'ordinateur virtuel**, puis cliquez sur **Suivant**.
6. Sur la page **Choisir les options de déplacement du stockage**, cliquez sur **Déplacer toutes les données de l'ordinateur virtuel vers un seul emplacement**, puis cliquez sur **Suivant**.
7. Sur la page **Choisir un nouvel emplacement pour l'ordinateur virtuel**, cliquez sur **Parcourir**.
8. Accédez à **C:**, créez un dossier nommé **LON-SVR1**, cliquez sur **Sélectionner un dossier**, puis sur **Suivant**.
9. Sur la page **Résumé**, cliquez sur **Terminer**.
10. Pendant la migration de l'ordinateur virtuel, connectez-vous y et vérifiez qu'il est entièrement opérationnel.
11. À l'issue du processus de déplacement, cliquez sur **Fermer**.
12. Arrêtez tous les ordinateurs virtuels en cours d'exécution.

Résultats : À la fin de cet exercice, vous aurez déployé et configuré un ordinateur virtuel à haut niveau de disponibilité.

▶ Préparer le prochain module

1. Redémarrez LON-HOST1.
2. À l'invite du menu de démarrage, sélectionnez **Windows Server 2008 R2**, et appuyez sur Entrée.
3. Connectez-vous à l'ordinateur hôte, comme demandé par votre instructeur.
4. Répétez les étapes 1 à 3 sur LON-HOST2.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12 : Implémentation de la récupération d'urgence

Atelier pratique : Implémentation des fonctionnalités de sauvegarde et de restauration de Windows Server

Exercice 1 : Sauvegarde de données sur un serveur Windows Server 2012

▶ Tâche 1 : Installer Sauvegarde Windows Server

1. Basculez vers LON-SVR1.
2. Dans le Gestionnaire de serveur, dans le volet d'accueil, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, sélectionnez **Sauvegarde Windows Server**, puis cliquez sur **Suivant**.
8. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Sur la page **Progression de l'installation**, attendez que le message **Installation réussie sur LON-SVR1.Adatum.com** s'affiche, puis cliquez sur **Fermer**.

▶ Tâche 2 : Configurer une sauvegarde planifiée

1. Sur LON-SVR1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sauvegarde Windows Server**.
2. Dans le volet de navigation, cliquez sur **Sauvegarde locale**.
3. Cliquez sur **Planification de sauvegarde**.
4. Dans l'Assistant Planification de sauvegarde, sur la page **Mise en route**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner la configuration de la sauvegarde**, cliquez sur **Serveur complet (recommandé)**, puis sur **Suivant**.
6. Sur la page **Spécifier l'heure de la sauvegarde**, à côté de **Sélectionnez une heure**, sélectionnez **01:00**, puis cliquez sur **Suivant**.
7. Sur la page **Spécifier le type de destination**, cliquez sur **Sauvegarder sur un dossier réseau partagé**, puis cliquez sur **Suivant**. Consultez l'avertissement, puis cliquez sur **OK**.
8. Sur la page **Spécifier le dossier partagé distant**, dans la zone de texte **Emplacement**, tapez **\\LON-DC1\Backup**, puis cliquez sur **Suivant**.

9. Dans la boîte de dialogue **Enregistrer la planification de sauvegarde**, dans la zone de texte **Nom d'utilisateur**, tapez **Administrateur**, dans la zone de texte **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **OK**.
10. Cliquez sur **Terminer**, puis sur **Fermer**.

Remarque : Dans un environnement de production, vous n'enregistrerez pas la sauvegarde dans un contrôleur de domaine. Vous le faites ici uniquement dans le cadre de l'atelier pratique.

▶ Tâche 3 : Terminer une sauvegarde à la demande

1. Sur LON-SVR1, dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Sauvegarde de Windows Server**.
2. Dans le volet Actions, cliquez sur **Sauvegarde locale**, et puis sur **Sauvegarde unique**.
3. Dans l'Assistant Sauvegarde unique, sur la page **Options de sauvegarde**, cliquez sur **Autres options**, puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner la configuration de la sauvegarde**, cliquez sur **Personnalisé**, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner les éléments à sauvegarder**, cliquez sur **Ajouter des éléments**.
6. Développez **Disque local (C:)**, sélectionnez la case à cocher **Financial Data**, cliquez sur **OK**, puis cliquez sur **Suivant**.
7. Sur la page **Spécifier le type de destination**, cliquez sur **Dossier partagé distant**, puis cliquez sur **Suivant**.
8. Sur la page **Spécifier un dossier distant**, saisissez **\\LON-DC1\Backup**, puis cliquez sur **Suivant**.
9. Sur la page **Confirmation**, cliquez sur **Sauvegarde**.
10. Sur la page **Progression de la sauvegarde**, une fois la sauvegarde terminée, cliquez sur **Fermer**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré la fonctionnalité Sauvegarde Windows Server, aurez planifié une tâche de sauvegarde, et aurez effectué une sauvegarde à la demande.

Exercice 2 : Restauration de fichiers à l'aide des fonctionnalités de sauvegarde de Windows Server

▶ Tâche 1 : Supprimer un fichier du serveur de fichiers

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
2. Dans l'Explorateur de fichiers, double-cliquez sur **Disque local (C:)**, cliquez avec le bouton droit sur **Financial Data**, puis cliquez sur **Supprimer**.

▶ Tâche 2 : Restaurer un fichier à partir de la sauvegarde

1. Dans la console de la **Sauvegarde Windows Server**, cliquez sur **Récupérer** dans le volet Actions.
2. Sur la page **Mise en route**, cliquez sur **Un autre emplacement**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Sur la page **Spécifier un type d'emplacement**, cliquez sur **Dossier partagé distant**, puis sur **Suivant**.
4. Sur la page **Spécifier un dossier distant**, saisissez **\\LON-DC1\Backup**, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner une date de sauvegarde**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner le type de récupération**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner les éléments à récupérer**, développez **LON-SVR1**, cliquez sur **Disque local (C:)** et sélectionnez **Financial Data**, dans le volet droit, puis cliquez sur **Suivant**.
8. Sur la page **Spécifier les options de récupération**, sous **Autre emplacement**, saisissez **C:**, puis cliquez sur **Suivant**.
9. Sur la page **Confirmation**, cliquez sur **Récupérer**.
10. Sur la page **Statut de la récupération**, cliquez sur **Fermer**.
11. Ouvrez le lecteur **C**, et vérifiez que le dossier **Financial Data** est restauré.

Résultats : Après avoir effectué cet exercice, vous aurez testé et validé la procédure de restauration d'un fichier à partir d'une sauvegarde.

Exercice 3 : Implémentation de sauvegarde et de restauration Windows Azure Online

▶ Tâche 1 : Installer le composant de Windows Azure™ Online Backup

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
2. Dans **Allfiles (E:)**, dans le volet d'informations, double-cliquez sur **OBSInstaller.exe**.
3. Dans la boîte de dialogue **Windows Azure Online Backup**, sélectionnez l'option **J'accepte les termes de la notification supplémentaire**, puis cliquez sur **OK**.
4. Sur la page **Vérification de la configuration requise**, cliquez sur **Suivant**.
5. Sur la page **Paramètres d'installation**, spécifiez les paramètres suivants (si vous ne conservez pas ceux par défaut), puis cliquez sur **Suivant**.
   - Dossier d'installation : **C:\Program Files\Windows Azure Online Backup Agent**
   - Emplacement du cache : **C:\Program Files\Windows Azure Online Backup Agent\Scratch**
6. Sur la page **Abonnement à Microsoft Update**, cliquez sur **Je ne souhaite pas utiliser Microsoft Update**, puis sur **Installer**.
7. Sur la page **Installation,** assurez-vous que le message **L'exécution de l'Assistant Installation de Windows Azure Online Backup Agent a réussi** s'affiche, décochez la case **Rechercher les mises à jour plus récentes**, puis cliquez sur **Terminer**.
8. Sur LON-SVR1, cliquez sur **Accueil**, puis cliquez sur **Windows Azure Online Backup**.
9. Sur LON-SVR1, cliquez sur **Accueil**, puis cliquez sur **Windows Azure Online Backup Shell**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Inscrire le serveur à Windows Azure Online Backup

Avant que vous inscriviez le serveur, vous devez renommer **LON-SVR1** en *NOMDEVOTREVILLE-VOTRENOM*. Par exemple, **PARIS-ALICE**. Cet exercice étant effectué en ligne, les noms des ordinateurs utilisés dans cet atelier pratique doivent être uniques. Si plusieurs stagiaires dans la classe portent un nom identique, ajoutez un numéro à la fin du nom de l'ordinateur, tel que **PARIS-ALICE-1**.

Pour renommer **LON-SVR1**, procédez comme suit :

1. Dans la fenêtre sur Gestionnaire de serveurs, sur la page **BIENVENUE DANS GESTIONNAIRE DE SERVEUR**, cliquez sur **1. Configurer ce serveur local**.
2. Dans la fenêtre Gestionnaire de serveur**,** sur la page **Serveur local,** cliquez sur **LON-SVR1**.
3. Dans la fenêtre Propriétés du système, cliquez sur **Modifier**, dans la zone **Nom de l'ordinateur**, tapez *NOMDEVOTREVILLE-VOTRENOM*, cliquez deux fois sur **OK**, puis cliquez sur **Fermer**.
4. Dans la fenêtre indiquant que vous devez redémarrer votre ordinateur, cliquez sur **Redémarrer maintenant**.
5. Attendez que *NOMDEVOTREVILLE-VOTRENOM* ait redémarré, puis connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Pour inscrire le serveur à Windows Azure Online Backup, procédez comme suit :

1. Démarrez la console Windows Azure Online Backup, puis cliquez sur **Inscrire un serveur**.
2. Dans l'assistant Inscrire le serveur**,** sur la page **Configuration du proxy**, cliquez sur **Suivant**.
3. Sur la page **Paramètres de chiffrement**, dans les zones **Entrer la phrase secrète** et **Confirmer la phrase secrète**, tapez **Pa$$w0rdPa$$w0rd**, puis, à côté de **Définir un emplacement pour enregistrer la phrase secrète**, cliquez sur **Parcourir**.
4. Dans une boîte de dialogue Rechercher un dossier, développez **Ordinateur**, cliquez sur **AllFiles (E:)**, cliquez sur **OK**, puis sur **Suivant**.
5. Sur la page **Informations d'identification du compte,** dans la zone **Identificateur d'utilisateur**, tapez **MSLTestUser@MSL TestOrg.onmicrosoft.com**, dans la zone **Mot de passe,** tapez **Pa$$w0rd**, puis cliquez sur **Inscrire**.
6. Sur la page **Inscription du serveur,** vérifiez que le message **Windows Azure Online Backup est maintenant disponible pour ce serveur** s'affiche, puis cliquez sur **Fermer**.

 **Remarque :** en situation réelle, vous saisiriez le nom d'utilisateur et le mot de passe de votre compte d'abonnement à Windows Azure Online Backup.

▶ Tâche 3 : Configurer Windows Azure Online Backup et démarrer une sauvegarde

1. Basculez vers la console Windows Azure Online Backup, puis dans le volet d'actions, cliquez sur **Planifier la sauvegarde**.
2. Sur la page **Mise en route**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner les éléments à sauvegarder**, cliquez sur **Ajouter des éléments**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la boîte de dialogue **Sélectionner des éléments**, développez le lecteur **C**, sélectionnez **Financial Data**, cliquez sur **OK**, puis sur **Suivant**.
5. Sur la page **Spécifier l'heure de la sauvegarde**, sélectionnez **Samedi**, cliquez sur **01:00**, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
6. Sur la page **Spécifier les paramètres de rétention**, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
7. Sur la page **Confirmation**, cliquez sur **Terminer**.
8. Sur la page **Modifier la progression de la sauvegarde**, cliquez sur **Fermer**.
9. Dans le volet Actions de la console Windows Azure Online Backup, cliquez sur **Sauvegarder maintenant**.
10. Dans l'assistant Sauvegarder maintenant, sur la page **Confirmation**, cliquez sur **Sauvegarder**.
11. Sur la page **Progression de la sauvegarde**, attendez que le message **Sauvegarde réussie** s'affiche, puis cliquez sur **Fermer**.

▶ Tâche 4 : Restaurer des fichiers à l'aide de la Windows Azure Online Backup

1. Sur LON-SVR1, sur la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**, puis dans le volet de navigation de l'Explorateur de fichiers, cliquez sur **Disque local (C:)**.
2. Dans la fenêtre Lecteur local (C:)**,** cliquez avec le bouton droit sur **Financial Data**, puis cliquez sur **Supprimer**.
3. Basculez vers la console Windows Azure Online Backup, puis dans le volet d'actions, cliquez sur **Récupérer des données**.
4. Dans l'assistant Récupérer les données, sur la page **Mise en route**, sélectionnez **Ce serveur**, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionnez le mode de récupération**, sélectionnez **Naviguer jusqu'aux fichiers**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner un volume et une date,** dans la zone de liste déroulante **Sélectionner le volume,** sélectionnez **C:**. Dans le calendrier, cliquez sur la date à laquelle vous avez effectué la sauvegarde, dans la liste déroulante **Heure**, cliquez sur l'heure à laquelle vous avez effectué la sauvegarde, puis cliquez sur **Suivant**.
7. Sur la page **Rechercher les éléments à récupérer**, développez **C:**, cliquez sur le dossier **Financial Data**, puis cliquez sur **Suivant**.
8. Sur la page **Spécifier les options de récupération**, sélectionnez à la fois **Emplacement d'origine** et **Créer des copies pour avoir les deux versions**, puis cliquez sur **Suivant**.
9. Sur la page **Confirmation**, cliquez sur **Récupérer**.
10. Sur la page **Statut de la récupération**, vérifiez que le message d'état **Tâche de récupération de fichier(s) réussie** apparaît, puis cliquez sur **Fermer**.
11. Dans l'Explorateur de fichiers, développez le lecteur **C:**, et vérifiez que le dossier **Financial Data** est restauré sur le lecteur C.

▶ Tâche 5 : Désinscrire le serveur à partir de Windows Azure Online Backup

1. Basculez vers la console **Windows Azure Online Backup**, puis cliquez sur **Annuler l'inscription du serveur**.
2. Sur la page **Mise en route**, cliquez sur **Annuler l'inscription de ce serveur**, puis cliquez sur **Suivant**.
3. Sur la page **Informations d'identification du compte**, fournissez les informations d'identification suivantes :
   - Identificateur d'utilisateur : **MSLTestUser@MSLTestOrg.onmicrosoft.com**
   - Mot de passe : **Pa$$w0rd**
4. Cliquez sur **Annuler l'inscription**.
5. Sur la page **Annulation de l'inscription du serveur**, cliquez sur **Fermer**.

Résultats : Après avoir terminé cet exercice, vous aurez installé l'agent Windows Azure Online Backup, inscrit le serveur avec Windows Azure Online Backup, configuré une sauvegarde planifiée, et effectué une restauration à l'aide de Windows Azure Online Backup.

▶ Pour préparer la prochaine application pratique, vous devez effectuer les tâches suivantes

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22412B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22412B-LON-SVR1**, et **MSL-TMG1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT