Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22410B

Installation et configuration 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 commerciales figurant sur la page http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx sont des marques commerciales du groupe de sociétés Microsoft. Toutes les autres marques sont la propriété de leurs propriétaires respectifs.

Numéro de produit : 22410B

Numéro de référence : X18-86872

Date de publication : 7/2013

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 et expert technique

Stan Reimer est président de S. R. Technical Services Inc et travaille comme consultant, instructeur et auteur. Stan bénéficie d'une expérience approfondie en matière de conseil sur les déploiements des services de domaine Active Directory® (AD DS) et Microsoft Exchange Server pour 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 — Développeur de contenu et expert technique

Damir Dizdarevic, MCT, MCSE (Microsoft Certified Solutions Expert), MCTS (Microsoft Certified Technology Specialist) et MCITP (Microsoft Certified IT Professional), est responsable et certificateur au Learning Center chez Logosoft d.o.o., à 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, en termes de sécurité et de virtualisation. Il a travaillé en tant qu'expert technique et réviseur technique sur de nombreux cours MOC (Microsoft® Official Curriculum) et a publié plus de 400 articles dans différents magazines informatiques tels que *Windows ITPro et INFO Magazine*. Damir est aussi un présentateur fréquent et reconnu lors de nombreuses conférences Microsoft en Europe de l'Est. En outre, il est membre du programme Microsoft MVP (Most Valuable Professional) pour la gestion de l'infrastructure de Windows Server.

Gary Dunlop — Expert technique

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

Siegfried Jagott – Développeur de contenu

Siegfried Jagott est consultant principal et responsable de l'équipe dédiée aux solutions de messagerie et de collaboration chez Atos Germany, Allemagne. Il est auteur-lauréat de *Microsoft Exchange Server 2010 Best Practices* (Microsoft Press) et il a écrit et effectuée la révision technique de plusieurs cours MOC sur différents sujets tels que MOC 10165 : *Mise à niveau des compétences concernant Microsoft Exchange Server 2003 ou Exchange Server 2007 vers Exchange Server 2010 SP1*. Siegfried a été coauteur d'autres manuels relatifs au système d'exploitation Windows®, à System Center Virtual Machine Manager (SC VMM) et à Exchange, et il a souvent présenté ces sujets lors de conférences internationales, telles que le conférence IT & Dev Connections qui s'est tenue au printemps 2012, à Las Vegas. Siegfried a planifié, conçu et implémenté certaines des plus grandes infrastructures Exchange Server et Windows au monde pour des clients internationaux. Il est titulaire d'un MBA obtenu à l'université Open University, Royaume-Uni, et il est certifié MCSE depuis 1997.

Jason Kellington — Expert technique

Jason Kellington (MCT, MCITP et MCSE) est consultant, instructeur et auteur. Il a une certaine expérience de l'utilisation d'un large éventail de technologies Microsoft, et s'intéresse essentiellement à l'infrastructure réseau d'entreprise. Jason exerce différentes fonctions chez Microsoft. Il est à la fois développeur de contenu pour les cours Microsoft Learning, responsable rédacteur technique pour Microsoft IT Showcase et auteur pour Microsoft Press.

Vladimir Meloski — Développeur de contenu

Vladimir est MCT, MVP sur Exchange Server, et un consultant, qui fournit des solutions de communications et d'infrastructure unifiées basées sur Microsoft Exchange Server, Microsoft Lync® Server et Microsoft System Center. Vladimir a 16 ans d'expérience professionnelle en informatique. Vladimir a participé à des conférences Microsoft en Europe et aux États-Unis en tant qu'un 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 — Expert technique

Nick a été MCT pendant 15 ans. Il est instructeur informatique indépendant, consultant et auteur. L'année dernière, Nick a enseigné dans plus de 20 pays. Il est spécialiste d'AD DS, des stratégies de groupe, de DNS, et il est intervenu en tant que consultant dans de nombreuses entreprises au cours des dix dernières années. Il a révisé plus de 100 cours Microsoft. Nick est membre du programme Springboard Series Technical Expert Panel (STEP) de Windows 7.

Brian Svidergol — Réviseur technique

Brian Svidergol est spécialisé dans les solutions d'infrastructure Microsoft et les solutions basées sur le cloud dans les environnements Windows, AD DS, Exchange Server, System Center, virtualisation et Microsoft Desktop Optimization Package (MDOP). Il possède les certifications MCT, MCITP (Enterprise Administrator (EA)), MCITP (Virtualization Administrator (VA)), MCITP (Exchange 2010) et plusieurs autres certifications Microsoft et du secteur. Brian est l'auteur du cours MOC (Microsoft Official Curriculum) 6426C : *Configuration et dépannage des solutions d'identité et d'accès avec Windows Server 2008 Active Directory*. Il a également travaillé pendant plusieurs années sur le développement d'examens de certification Microsoft et du contenu de formation associé.

Orin Thomas — Expert technique

Orin Loïg 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. Il 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 le client Windows, System Center, et sur des sujets relatifs à la sécurité. Orin a fondé et dirige le Melbourne System Center Users Group.

Byron Wright — Développeur de contenu et expert technique

Byron Wright est un partenaire qui intervient pour une société de conseil pour laquelle il fournit des services de consulting réseau, d'implémentation de systèmes informatiques et de formation technique. Byron occupe également un poste de chargé d'enseignement à la Asper School of Business de l'University du Manitoba, où il enseigne sur les systèmes de gestion de l'information et la gestion de réseau. Byron est l'auteur et le coauteur de plusieurs livres sur les systèmes d'exploitation Windows, Windows Vista et Exchange Server, notamment le *Windows Server 2008 Active Directory Resource Kit (en anglais)*.

Sommaire

Module 1 : Déploiement et gestion de Windows Server 2012

Leçon 1 : Vue d'ensemble de Windows Server 2012 **1-2**
Leçon 2 : Vue d'ensemble de l'administration de Windows Server 2012 **1-16**
Leçon 3 : Installation de Windows Server 2012 **1-22**
Leçon 4 : Configuration post-installation de Windows Server 2012 **1-28**
Leçon 5 : Présentation de Windows PowerShell **1-38**
Atelier pratique : Déploiement et gestion de Windows Server 2012 **1-44**

Module 2 : Présentation des services de domaine Active Directory

Leçon 1 : Vue d'ensemble d'AD DS **2-2**
Leçon 2 : Vue d'ensemble des contrôleurs de domaine **2-9**
Leçon 3 : Installation d'un contrôleur de domaine **2-16**
Atelier pratique : Installation de contrôleurs de domaine **2-22**

Module 3 : Gestion des objets de services de domaine Active Directory

Leçon 1 : Gestion de comptes d'utilisateurs **3-3**
Leçon 2 : Gestion des comptes de groupes **3-12**
Leçon 3 : Gestion des comptes d'ordinateurs **3-20**
Leçon 4 : Délégation de l'administration **3-26**
Atelier pratique : Gestion des objets de services de domaine Active Directory **3-30**

Module 4 : Automatisation de l'administration des domaines de services Active Directory

Leçon 1 : Utilisation des outils en ligne de commande pour l'administration d'AD DS **4-2**
Leçon 2 : Utilisation de Windows PowerShell pour l'administration d'AD DS **4-8**
Leçon 3 : Exécution d'opérations en bloc avec Windows PowerShell **4-15**
Atelier pratique : Automatisation de l'administration d'AD DS à l'aide de Windows PowerShell **4-23**

Module 5 : Implémentation du protocole IPv4

Leçon 1 : Vue d'ensemble de TCP/IP **5-2**
Leçon 2 : Fonctionnement de l'adressage IPv4 **5-7**
Leçon 3 : Sous-réseau et super-réseau **5-12**
Leçon 4 : Configuration et résolution des problèmes liés à IPv4 **5-18**
Atelier pratique : Implémentation du protocole IPv4 **5-28**

Module 6 : Implémentation du protocole DHCP (Dynamic Host Configuration Protocol)

Leçon 1 : Installation d'un rôle Serveur DHCP **6-2**
Leçon 2 : Configuration des étendues DHCP **6-8**
Leçon 3 : Gestion d'une base de données DHCP **6-13**
Leçon 4 : Sécurisation et surveillance DHCP **6-17**
Atelier pratique : Implémentation de DHCP **6-23**

Module 7 : Implémentation du système DNS (Domain Name System)

Leçon 1 : Résolution de noms pour les clients et les serveurs Windows **7-2**
Leçon 2 : Installation et gestion d'un serveur DNS **7-12**
Leçon 3 : Gestion des zones DNS **7-19**
Atelier pratique : Implémentation de la réplication DNS **7-23**

Module 8 : Implémentation d'IPv6

Leçon 1 : Vue d'ensemble du protocole IPv6 **8-2**
Leçon 2 : Adressage IPv6 **8-8**
Leçon 3 : Cohabitation avec le protocole IPv4 **8-15**
Leçon 4 : Technologies de transition IPv6 **8-20**
Atelier pratique : Implémentation d'IPv6 **8-26**

Module 9 : Implémentation d'un système de stockage local

Leçon 1 : Vue d'ensemble du stockage **9-2**
Leçon 2 : Gestion des disques et des volumes **9-13**
Leçon 3 : Implémentation d'espaces de stockage **9-25**
Atelier pratique : Implémentation d'un système de stockage local **9-30**

Module 10 : Implémentation des services de fichier et d'impression

Leçon 1 : Sécurisation des fichiers et des dossiers **10-2**
Leçon 2 : Protection des fichiers et des dossiers partagés à l'aide de clichés instantanés **10-17**
Leçon 3 : Configuration de l'impression réseau **10-21**
Atelier pratique : Implémentation des services de fichier et d'impression **10-28**

Module 11 : Implémentation d'une stratégie de groupe

Leçon 1 : Vue d'ensemble d'une stratégie de groupe **11-2**
Leçon 2 : Traitement d'une stratégie de groupe **11-11**
Leçon 3 : Implémentation d'un magasin central pour les modèles d'administration **11-18**
Atelier pratique : Implémentation d'une stratégie de groupe **11-23**

Module 12 : Sécurisation des serveurs Windows à l'aide d'objets de stratégie de groupe

Leçon 1 : Vue d'ensemble de la sécurité des systèmes d'exploitation Windows **12-2**
Leçon 2 : Configuration des paramètres de sécurité **12-7**
Atelier pratique A : Renforcement de la sécurité des ressources de serveur **12-18**
Leçon 3 : Restriction de l'accès aux logiciels **12-26**
Leçon 4 : Configuration du Pare-feu Windows avec fonctions avancées de sécurité **12-31**
Atelier pratique B : Configuration d'AppLocker et du Pare-feu Windows **12-36**

Module 13 : Implémentation de la virtualisation de serveur avec Hyper-V

Leçon 1 : Vue d'ensemble des technologies de virtualisation **13-2**
Leçon 2 : Implémentation d'Hyper-V **13-9**
Leçon 3 : Gestion du stockage d'ordinateur virtuel **13-17**
Leçon 4 : Gestion des réseaux virtuels **13-25**
Atelier pratique : Implémentation de la virtualisation de serveur avec Hyper-V **13-30**

Corrigés des ateliers pratiques

Atelier pratique du module 1 : Déploiement et gestion de Windows Server 2012 **L1-1**
Atelier pratique du module 2 : Installation de contrôleurs de domaine **L2-11**
Atelier pratique du module 3 : Gestion des objets de services de domaine Active Directory **L3-15**
Atelier pratique du module 4 : Automatisation de l'administration d'AD DS à l'aide de Windows PowerShell **L4-25**
Atelier pratique du module 5 : Implémentation du protocole IPv4 **L5-29**
Atelier pratique du module 6 : Implémentation de DHCP **L6-33**
Atelier pratique du module 7 : Implémentation de la réplication DNS **L7-39**
Atelier pratique du module 8 : Implémentation d'IPv6 **L8-47**
Atelier pratique du module 9 : Implémentation d'un système de stockage local **L9-51**
Atelier pratique du module 10 : Implémentation des services de fichier et d'impression **L10-57**
Atelier pratique du module 11 : Implémentation d'une stratégie de groupe **L11-65**
Atelier pratique A du module 12 : Renforcement de la sécurité des ressources de serveur **L12-69**
Atelier pratique B du module 12 : Configuration d'AppLocker et du Pare-feu Windows **L12-77**
Atelier pratique du module 13 : Implémentation de la virtualisation de serveur avec Hyper-V **L13-85**

À propos de ce cours

Cette section décrit brièvement le cours—22410B : Installation et configuration de Windows Server® 2012 et ses objectifs, le public visé, ainsi que les connaissances préalables requises.

Description du cours

Ce cours constitue la première partie d'une série de trois cours qui apportent les qualifications et connaissances nécessaires pour implémenter une infrastructure Windows Server 2012 principale dans un environnement d'entreprise existant. L'intégralité des trois cours couvre l'implémentation, la gestion, la maintenance et la mise en route des services et de l'infrastructure dans un environnement Windows Server 2012. Même si certaines compétences et tâches se recoupent d'un cours à l'autre, celui-ci couvre principalement l'implémentation et la configuration initiales de services principaux tels qu'Active Directory® Domain Services (AD DS), les services de mise en réseau et la configuration de Microsoft® Hyper-V® Server 2012 .

Public visé

Ce cours s'adresse aux professionnels des technologies de l'information qui ont une bonne connaissance et une bonne expérience des systèmes d'exploitation Windows® et souhaitent acquérir les compétences et connaissances nécessaires pour implémenter des services d'infrastructure essentiels dans un environnement Windows Server 2012 existant.

Il s'adresse accessoirement à toute personne souhaitant obtenir la certification à l'examen 70-410, *Installation et configuration de Windows Server® 2012*.

Connaissances préalables des stagiaires

Pour suivre ce cours, les stagiaires doivent :

- avoir une bonne compréhension des principes fondamentaux de la mise en réseau ;
- comprendre la configuration de la sécurité et des tâches administratives dans un environnement d'entreprise et avoir de l'expérience en la matière ;
- avoir de l'expérience en matière de prise en charge et de configuration des clients utilisant le système d'exploitation Windows ;
- avoir une bonne expérience pratique des systèmes d'exploitation Windows Vista®, Windows 7 ou Windows 8.

Une expérience de systèmes d'exploitation Windows Server précédents serait également profitable aux stagiaires.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Objectifs du cours

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

- installer et configurer Windows Server 2012 ;
- décrire AD DS ;
- gérer des objets Active Directory ;
- automatiser l'administration d'Active Directory ;
- implémenter IPv4 ;
- implémenter le protocole DHCP (Dynamic Host Configuration Protocol) ;
- implémenter le système DNS (Domain Name System) ;
- implémenter IPv6 ;
- implémenter le stockage local ;
- partager des fichiers et des imprimantes ;
- implémenter une stratégie de groupe ;
- utiliser des objets de stratégie de groupe pour sécuriser les serveurs Windows Server ;
- implémenter la virtualisation de serveur avec Hyper-V.

Plan du cours

Cette section présente le plan du cours :

Module 1, Déploiement et gestion de Windows Server 2012

Ce module commence par décrire l'installation de Windows Server 2012. Il ne s'agit pas de la tâche la plus récurrente du cours mais elle constitue un point de départ logique pour permettre aux stagiaires de commencer à travailler avec Windows Server 2012.

Module 2, Présentation des services de domaine Active Directory

Les services de domaine Active Directory (AD DS) constituent un élément central de la gestion réseau dans un environnement d'entreprise. Ils sont présenté en début de cours de sorte que les stagiaires puissent les utiliser pour effectuer d'autres tâches, telles que la création d'utilisateurs et de groupes, au cours des modules suivants. Dans ce module, les stagiaires vont installer un contrôleur de domaine.

Module 3, Gestion des objets de services de domaine Active Directory

Ce module décrit la création et la gestion d'objets Active Directory spécifiques, tels que des utilisateurs, des groupes ou des comptes d'ordinateur. Il s'agit d'un élément essentiel des tâches quotidiennes effectuées par un administrateur de serveur débutant. Certaines de ces tâches sont également déléguées au personnel de support technique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4, Automatisation de l'administration des domaines de services Active Directory

Ce module étend les connaissances acquises lors du module 3 en fournissant aux stagiaires des méthodes permettant d'automatiser la création et la gestion des objets Active Directory. Il s'agit d'un sujet relativement avancé, mais qui découle logiquement du module 3.

Module 5, Implémentation du protocole IPv4

Ce module commence un nouveau thème de formation dans le cours. Configurer et maîtriser IPv4 est un élément fondamental du rôle d'administrateur système.

Module 6, Implémentation du protocole DHCP (Dynamic Host Configuration Protocol)

Ce module décrit l'utilisation du protocole DHCP pour la diffusion des informations d'adresse IPv4.

Module 7, Implémentation du système DNS (Domain Name System)

Ce module explique comment le système DNS convertit les noms en adresses IP, et pourquoi cela est important dans un environnement Active Directory.

Module 8, Implémentation d'IPv6

Ce module présente la configuration IPv6, ce qui constitue probablement un nouveau contenu pour les stagiaires. Le module 8 est séparé du module 5 car ces deux modules sont très théoriques et pourraient surcharger les stagiaires s'ils étaient séquentiels. La connaissance d'IPv6 n'est pas requise pour les modules 6 et 7.

Module 9, Implémentation d'un système de stockage local

Ce module inclut des informations sur la configuration du stockage pour Windows Server 2012. Ces informations constituent un prérequis au module 10, lequel décrit la création et la sécurisation des partages de fichiers.

Module 10, Implémentation des services de fichier et d'impression

Ce module décrit à la fois les partages de fichiers et l'impression car ces deux tâches sont des services réseau couramment utilisés. La sécurité concernant les partages de fichiers et l'impression utilise les connaissances relatives aux comptes d'utilisateurs et aux groupes qui font l'objet des modules 2 et 3.

Module 11, Implémentation d'une stratégie de groupe

Ce module repose sur les informations que les stagiaires connaissent déjà au sujet d'AD DS et présente la création et la gestion des objets de stratégie de groupe.

Module 12, Sécurisation des serveurs Windows à l'aide d'objets de stratégie de groupe

Ce module décrit les paramètres de stratégie de groupe spécifiques qui permettent d'accroître la sécurité. Ces paramètres comprennent les stratégies de sécurité, les stratégies de restriction d'application et les règles de Pare-feu Windows.

Module 13, Implémentation de la virtualisation de serveur avec Hyper-V

Ce dernier module explique comment configurer Hyper-V et comment créer des ordinateurs virtuels. Ce module est présenté en dernier car son atelier pratique pourrait avoir un impact négatif sur les ordinateurs virtuels qui sont déjà déployés sur les machines des stagiaires.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Mappage d'examen/de cours

Ce cours, *22410B : Installation et configuration de Windows Server® 2012*, mappe directement son contenu aux objectifs de l'examen Microsoft *70-410 : Installation et configuration 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 il fournit plutôt des connaissance 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'aide de l'URL suivante : http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-410&locale=en-us#tab2 (*Certains de ces sites adressées dans ce cours sont en anglais.*).

Objectifs de l'examen : Examen 70-410 : Installation et configuration de Windows Server® 2012		**Contenu du cours**		
Installer et configurer des serveurs		Module	Lesson	Lab
Installer des serveurs	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Planifier une installation de serveur, planifier des rôles de serveur, planifier une mise à niveau de serveur, effectuer une installation minimale, optimiser l'utilisation des ressource à l'aide des fonctionnalités à la demande, migrer les rôles des versions précédentes de Windows Server	Mod 1	Leçon 1	Mod 1 Ex 1
Configurer des serveurs	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer installation minimale, déléguer l'administration, ajouter et supprimer des fonctionnalités dans des images hors connexion, déployer les rôles sur des serveurs distants, passer d'une installation minimale à/à partir d'une interface graphique complète, configurer les services, configurer l'association de cartes réseau	Mod 1	Leçon 1/2/4	Mod 1 Ex 1/2/3
		Mod 3	Leçon 4	Mod 3 Ex 2
Configurer le stockage local	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Concevoir des espaces de stockage, configurer des disques de base et des disques dynamiques, configurer des disques MBR et GPT, gérer des volumes, créer et monter des disques durs virtuels (VHD), configurer des pools de stockage et des pools de disque	Mod 9	Leçon 1/2/3	Mod 9 Ex 1/2/3

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Objectifs de l'examen : Examen 70-410 : Installation et configuration de Windows Server® 2012		Contenu du cours		
Configurer les rôles et les fonctionnalités serveur				
Configurer l'accès aux fichiers et aux partages	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Créer et configurer des partages, configurer des autorisations de partage, configurer des fichiers hors connexion, configurer des autorisations NTFS, configurer l'énumération basée sur l'accès (ABE), configurer le service VSS, configurer les quotas NTFS	Mod 10	Leçon 1/2	Mod 10 Ex 1/2
Configurer les services d'impression et de document	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer le pilote d'impression Easy Print, configurer la gestion de l'impression d'entreprise, configurer des pilotes, configurer le pool d'imprimante, configurer les priorités d'impression, configurer les autorisations d'imprimante	Mod 10	Leçon 3	Mod 10 Ex 3
Configurer des serveurs pour la gestion à distance	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer WinRM, configurer la gestion de serveur de bas niveau, configurer les serveurs pour des tâches de gestion quotidiennes, configurer la gestion de plusieurs serveurs, configurer une installation minimale, configurer le Pare-feu Windows	Mod 1	Leçon 1/2/4	Mod 1 Ex 2
		Mod 12	Leçon 4	Mod 12 Atelier B Ex 2

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Objectifs de l'examen : Examen 70-410 : Installation et configuration de Windows Server® 2012		Contenu du cours		
Configurer Hyper-V				
Créer et configurer des paramètres d'ordinateur virtuel	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer la mémoire dynamique, configurer la pagination intelligente, configurer le contrôle des ressources, configurer les services d'intégration d'invité	Mod 13	Leçon 2	Mod 13 Ex 3/4
Créer et configurer un stockage d'ordinateur virtuel	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Créer des disques durs VHD et VHDX, configurer des lecteurs de différenciation, modifier des disques VHD, configurer des disques directs, gérer des instantanés, implémenter une carte de Fibre Channel virtuelle	Mod 9	Leçon 1	
		Mod 13	Leçon 2/3	Mod 13 Ex 3/4
Créer et configurer des réseaux virtuels	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Implémenter la virtualisation de réseau Hyper-V, configurer les commutateurs virtuels Hyper-V, optimiser les performances réseau, configurer des adresses MAC, configurer l'isolement réseau, configurer des cartes réseau virtuelles synthétiques et héritées	Mod 13	Leçon 4	Mod 13 Ex 2
Déployer et configurer des services réseau de base				
Configurer l'adressage IPv4 et IPv6	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer les options d'adresse IP, configurez un sous-réseau, configurer un super-réseau, configurer l'interopérabilité entre IPv4 et IPv6, configurer ISATAP, configurer Teredo	Mod 1	Leçon 4	Mod 1 Ex 1/2
		Mod 5	Leçon 2/3/4	Mod 5 Ex 1/2
		Mod 8	Leçon 3/4	Mod 8 Ex 2
Déployer et configure le service DHCP (Dynamic Host Configuration Protocol)	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Créez et configurez les étendues, configurer une réservation DHCP, configurer des options DHCP, configurer un client et un serveur pour le démarrage PXE, configurer un agent relais DHCP, autoriser un serveur DHCP	Mod 6	Leçon 1/2/3/4	Mod 6 Ex 1/2
Déployer et configurer un service DNS	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer l'intégration d'Active Directory des zones principales, configurer des redirecteurs, configurer des indications de racine, gérer le cache DNS, créer des enregistrements de ressource A et PTR	Mod 7	Leçon 1/2/3	Mod 7 Ex 1/2/3

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Objectifs de l'examen : Examen 70-410 : Installation et configuration de Windows Server® 2012		Contenu du cours		
Installer et administrer Active Directory				
Installer des contrôleurs de domaine	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Ajouter ou supprimer un contrôleur de domaine d'un domaine, mettre à niveau un contrôleur de domaine, installer des services de domaine Active Directory (AD DS) dans une installation minimale, installer un contrôleur à partir d'une installation à partir du support, résoudre les problèmes d'inscription des enregistrement SRV DNS, configurer un serveur de catalogue global	Mod 2	Leçon 3	Mod 2 Ex 1/2
Créer et gérer des utilisateurs et des ordinateurs Active Directory	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Automatiser la création de comptes Active Directory, créer, copier, configurer et supprimer des utilisateurs et des ordinateurs, configurer des modèles, exécuter des opérations Active Directory en bloc, configurer des droits utilisateur, joindre des domaines hors connexion, gérer les comptes inactifs et désactivés	Mod 1	Leçon 4	
		Mod 3	Leçon 1	Mod 3 Ex 2/3
		Mod 4	Leçon 1/2/3	Mod 4 Ex 1/2/3
Créer et gérer des groupes et des unités d'organisation Active Directory	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer l'imbrication de groupes, convertir les groupes y compris les groupes de sécurité, les groupes de distribution, les groupes 'universels, les groupes locaux de domaine et les groupes globaux de domaine, gérer l'appartenance de groupe à l'aide de la stratégie de groupe, énumérer l'appartenance de groupe, déléguer la création et la gestion des objets Active Directory, gérer les conteneurs Active Directory par défaut, créer, copier, configurer et supprimer des groupes et des unité d'organisation	Mod 3	Leçon 1/2/4	Mod 3 Ex 1/2/3
		Mod 4	Leçon 1/2	Mod 4 Ex 1

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Objectifs de l'examen : Examen 70-410 : Installation et configuration de Windows Server® 2012		Contenu du cours		
Installer et administrer Active Directory				
Créer et gérer une stratégie de groupe				
Créer des objets de stratégie de groupe	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer un magasin central, gérer des objets de stratégie de groupe Starter, configurer des liens de stratégie de groupe, configurer des plusieurs stratégies de groupe locales, configurer le filtrage de sécurité	Mod 11	Leçon 1/2	Mod 11 Ex 1/2
Configurer des stratégies de sécurité	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer l'attribution des droits utilisateurs, configurer les paramètres d'options de sécurité, configurer des modèles de sécurité, configurer une stratégie d'audit, configurer des utilisateurs et des groupes locaux, configurer le contrôle de compte d'utilisateur	Mod 12	Leçon 1/2	Mod 12 Atelier A Ex 1/2/3

Objectifs de l'examen : Examen 70-410 : Installation et configuration de Windows Server® 2012		Contenu du cours		
Créer et gérer une stratégie de groupe				
configurer des stratégies de restriction d'application	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer l'application de règles, configurer des règles Applocker, configurer des stratégies de restriction logicielle	Mod 12	Leçon 3	Mod 12 Atelier B Ex 1
Configurer le Pare-feu Windows	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : Configurer des règles pour plusieurs profils à l'aide d'une stratégie de groupe, configurer des règles de sécurité de connexion, configurer le Pare-feu Windows pour autoriser ou refuser des applications, des étendues, des ports et des utilisateurs, configurer des exceptions de pare-feu authentifiées, importer et exporter des paramètres	Mod 12	Leçon 4	Mod 12 Atelier B Ex 2

Remarque : 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 :

- posséder une expérience réelle et pratique de l'installation et de la configuration d'une infrastructure Windows Server 2012 ;
- disposer d'une expérience en termes de configuration client Windows 7 ou Windows 8 ;
- 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=70-410&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=70-410&locale=en-us#tab1

La table de mappage d'examen/cours tracée les grandes lignes ci-dessus est exacte au moment de l'impression, toutefois elle est sujette à la modification à tout moment et des ours de Microsoft aucune responsabilité de toutes les anomalies entre la version publiée ici et la version accessible en ligne et ne donnera aucune notification 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 de l'atelier pratique** : fournissent des instructions pas à pas que vous pourrez consulter à tout moment au cours d'un atelier pratique.

Contenu d'accompagnement du cours sur le site http://www.microsoft.com/learning/companionmoc : Contenu numérique facile à parcourir et dans lequel il est possible d'effectuer des recherches, 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 meilleures pratiques, 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® et Microsoft Press®.

Fichiers de cours destinés aux stagiaires sur le site http://www.microsoft.com/learning/companionmoc *:* incluent le fichier exécutable à extraction automatique Allfiles.exe, lequel contient les fichiers requis pour les ateliers pratiques et 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 d'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 et vous ne devez enregistrer aucune modification. 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
22410B-LON-DC1	Contrôleur de domaine exécutant Windows Server 2012 dans le domaine Adatum.com.
22410B-LON-SVR1	Serveur membre exécutant Windows Server 2012 dans le domaine Adatum.com.
22410B-LON-SVR2	Serveur membre exécutant Windows Server 2012 dans le domaine Adatum.com. Ce serveur se trouvera dans un deuxième sous-réseau.
22410B-LON-SVR3	Ordinateur virtuel vierge sur lequel les stagiaires vont installer Windows Server 2012.
22410B-LON-HOST1	Disque dur virtuel (VHD) amorçable pour l'exécution de Windows Server 2012 sur l'hôte pour Hyper-V.
22410B-LON-CORE	Serveur autonome exécutant l'installation minimale de Windows Server 2012
22410B-LON-RTR	Routeur qui est utilisé pour les activités réseau nécessitant un sous-réseau distinct.
22410B-LON-CL1	Ordinateur client exécutant Windows 8 et Microsoft® Office 2010 Service Pack 1 (SP1) dans le domaine Adatum.com.
22410B-LON-CL2	Ordinateur client exécutant Windows 8 et Office 2010 SP1 dans le domaine Adatum.com qui se trouve dans un deuxième sous-réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration logicielle

Les logiciels suivants sont installés sur chaque ordinateur virtuel :

- Moniteur réseau Microsoft 3.4 est installé sur LON-SVR2.

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 expérience 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.

- Niveau matériel 6 avec 8 gigaoctets (Go) de mémoire vive (RAM)

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 Accueil : 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 **Accueil**.
- Windows+C : ouvre le même menu avec 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

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1

Déploiement et gestion de Windows Server 2012

Table des matières :

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

Leçon 1 : Vue d'ensemble de Windows Server 2012 **1-2**

Leçon 2 : Vue d'ensemble de l'administration de Windows Server 2012 **1-16**

Leçon 3 : Installation de Windows Server 2012 **1-22**

Leçon 4 : Configuration post-installation de Windows Server 2012 **1-28**

Leçon 5 : Présentation de Windows PowerShell **1-38**

Atelier pratique : Déploiement et gestion de Windows Server 2012 **1-44**

Contrôle des acquis et éléments à retenir **1-53**

Vue d'ensemble du module

Comprendre les capacités d'un nouveau système d'exploitation Windows Server® 2012 vous permet de tirer profit efficacement de ce système d'exploitation. Si vous ne comprenez pas les fonctions de votre nouveau système d'exploitation Windows Server 2012, vous risquez de l'utiliser au final de la même manière que le système d'exploitation précédent et de passer à côté des avantages de ce nouveau système. En comprenant comment exploiter complètement votre nouveau système d'exploitation Windows Server 2012 et en comprenant le fonctionnement des outils disponibles pour gérer ces fonctionnalités, vous fournirez une valeur ajoutée supérieure à votre organisation.

Ce module présente la nouvelle interface d'administration de Windows Server 2012. Dans ce module, vous allez découvrir les différents rôles et fonctionnalités que vous propose le système d'exploitation Windows Server 2012. Vous découvrirez également les différentes options d'installation de Windows Server 2012 que vous pouvez utiliser.

Ce module présente les étapes de configuration que vous pouvez effectuer pendant l'installation et après le déploiement pour vous assurer que les serveurs pourront commencer à fonctionner dans le rôle qui leur a été attribué. Vous apprendrez également à utiliser Windows PowerShell® pour effectuer des tâches d'administration courantes dans Windows Server 2012.

Objectifs

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

- décrire Windows Server 2012 ;
- décrire les outils de gestion disponibles dans Windows Server 2012 ;
- installer Windows Server 2012 ;
- effectuer la configuration post-installation de Windows Server 2012 ;
- exécuter les tâches d'administration de base à l'aide de Windows PowerShell.

Leçon 1
Vue d'ensemble de Windows Server 2012

Avant de déployer Windows Server 2012, vous devez comprendre comment chacune des éditions de Windows Server 2012 peut bénéficier aux serveurs de votre organisation. Vous devez également savoir si une configuration matérielle particulière est appropriée pour Windows Server 2012, si un déploiement virtuel peut être plus approprié qu'un déploiement physique et quelle source d'installation permet de déployer Windows Server 2012 de façon efficace. Si vous ne comprenez pas clairement ces problèmes, vous risquez de faire des choix que vous devrez corriger ultérieurement, ce qui coûtera au final du temps et de l'argent à votre organisation.

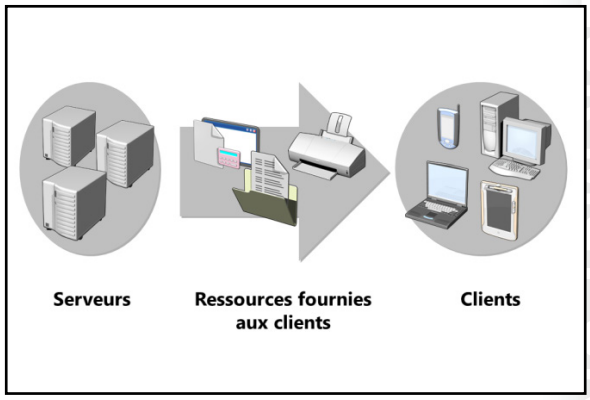
Cette leçon fournit une vue d'ensemble des divers éditions, options d'installation, rôles et fonctionnalités de Windows Server 2012. Ces informations vous permettront de déterminer l'édition et les options d'installation de Windows Server 2012 les plus appropriées pour votre organisation.

Objectifs de la leçon

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

- décrire le rôle des serveurs locaux dans un réseau moderne ;
- expliquer la différence entre les clouds privés et publics ;
- répertorier les différentes éditions de Windows Server 2012 ;
- décrire la différence entre l'installation minimale et standard de Windows Server 2012 ;
- expliquer la fonction des rôles de serveur disponibles sur les ordinateurs exécutant Windows Server 2012 ;
- expliquer l'objet de diverses fonctionnalités de Windows Server 2012.

Serveurs locaux



En tant que professionnel de l'informatique, vous avez très probablement entendu parler du cloud computing. Vous avez peut-être entendu que des logiciels et des services sont déplacés vers un cloud public ou privé parce que les prévisions indiquent que le cloud constituera un aspect important de l'avenir de l'informatique d'entreprise. Vous avez peut-être également entendu que Windows Server 2012 est prêt pour le cloud. En tant que professionnel de l'informatique ayant travaillé avec des serveurs déployés localement, vous pouvez raisonnablement vous poser la question suivante: si tout évolue vers le cloud computing, est-il nécessaire d'apprendre à déployer Windows Server 2012 localement ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En réalité, le fait est que tous les services et les applications qui sont utilisés quotidiennement ne doivent pas être hébergés via un cloud computing. Les serveurs déployés localement forment la colonne vertébrale d'un réseau organisationnel et fournissent les ressources suivantes aux clients :

- Services d'infrastructure. Les serveurs fournissent aux clients les ressources d'infrastructure, y compris les services DNS (Domain Name System) et DHCP (Dynamic Host Configuration Protocol). Ces services permettent aux clients de se connecter et de communiquer avec d'autres ressources. Sans ces services, les clients ne pourraient pas se connecter entre eux ni à des ressources distantes, telles que les ressources hébergées via un cloud computing.
- Fichiers et imprimantes partagés. Les serveurs fournissent un emplacement centralisé qui permet aux utilisateurs de stocker et de partager des documents. Les serveurs hébergent également des ressources telles que les imprimantes partagées, qui permettent aux groupes d'utilisateurs de tirer profit plus efficacement des ressources. Sans ces ressources centralisées, déployées localement, le partage et la sauvegarde de fichiers de manière centralisée constitueraient un processus plus long et plus complexe. Il serait possible d'héberger certaines de ces informations via un cloud computing, mais il ne semble pas vraiment raisonnable d'envoyer un travail à une imprimante située dans une pièce voisine via un serveur hébergé à un emplacement distant.
- Applications hébergées. Les serveurs hébergent des applications telles que Microsoft® Exchange Server, Microsoft SQL Server®, Microsoft Dynamics® et Microsoft System Center. Les clients accèdent à ces applications pour accomplir différentes tâches, telles qu'accéder à leur courrier électronique ou déployer en libre-service des applications de bureau. Dans certains cas, ces ressources peuvent être déployées via un cloud computing. Dans de nombreux cas, ces ressources doivent être hébergées localement pour des raisons liées aux performances, au coût et à la réglementation. Le fait qu'il soit plus judicieux d'héberger ces ressources localement ou via un cloud computing dépend des spécificités de l'organisation elle-même.
- Accès au réseau. Les serveurs fournissent des ressources d'authentification et d'autorisation aux clients dans le réseau. L'authentification au niveau d'un serveur permet à un utilisateur et à un client de prouver leur identité. Même lorsqu'un grand nombre de serveurs d'une organisation sont situés dans un cloud public ou privé, les personnes doivent encore disposer d'une certaine forme d'infrastructure locale d'authentification et d'autorisation.
- Déploiement d'applications, de mises à jour et de systèmes d'exploitation. Les serveurs sont souvent déployés localement pour faciliter le déploiement d'applications, de mises à jour et de systèmes d'exploitation sur les clients dans le réseau organisationnel. En raison de l'utilisation intensive de la bande passante, ces serveurs doivent être à proximité des clients auxquels ils fournissent ce service.

Chaque organisation possède ses propres exigences. Une organisation située dans une zone dotée d'une connectivité Internet limitée devra compter davantage sur les serveurs locaux qu'une organisation qui dispose d'une connexion haut débit. Dans une organisation, il est important que, même dans l'éventualité de problèmes de connectivité Internet, le travail puisse continuer. La productivité sera affectée si la défaillance de la connexion Internet de l'organisation signifie que soudainement personne ne peut accéder à ses fichiers et imprimantes partagés.

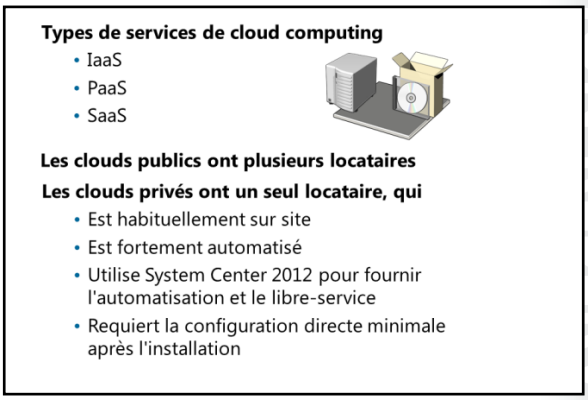
Windows Server 2012 est prêt pour l'intégration avec le cloud computing, mais il est encore parfaitement adapté aux tâches traditionnelles que les systèmes d'exploitation Windows Server effectuaient généralement. Par conséquent, vous pouvez encore configurer et déployer Windows Server 2012 pour effectuer les charges de travail identiques ou similaires que vous avez configurées pour les serveurs exécutant Windows Server 2003, voire peut-être même pour Microsoft Windows NT® Server 4.0.

Question : Quelle est la différence entre un système d'exploitation serveur et client ?

Question : Comment le rôle du serveur a-t-il évolué au fil du temps depuis le système d'exploitation serveur Microsoft Windows NT 4.0 jusqu'à Windows Server 2012 ?

Qu'est-ce que le cloud computing ?

Le *cloud computing* est une description générale qui recouvre plusieurs technologies différentes.



Les formes les plus courantes de cloud computing sont les suivantes :

- *Infrastructure en tant que service (IaaS)*. Avec cette forme de cloud computing, vous exécutez un ordinateur virtuel complet dans le cloud. Le fournisseur d'hébergement du cloud gère la plateforme de l'hyperviseur et vous gérez l'ordinateur virtuel qui fonctionne dans l'infrastructure du fournisseur du cloud. Windows Azure™ Compute est un exemple d'infrastructure IaaS. Vous pouvez exécuter Windows Server 2012 en tant qu'ordinateur virtuel dans un cloud IaaS, mais dans certains cas le système d'exploitation hébergera les ordinateurs virtuels dans un cloud IaaS.
- *Plateforme en tant que service (PaaS)*. Avec PaaS, le fournisseur d'hébergement du cloud vous fournit une plateforme particulière. Par exemple, un fournisseur peut vous permettre d'héberger des bases de données. Vous gérez la base de données elle-même et le fournisseur d'hébergement du cloud héberge le serveur de base de données. SQL Azure™ est un exemple de plateforme en tant que service.
- *Logiciel en tant que service (SaaS)*. Le fournisseur d'hébergement du cloud héberge votre application et l'infrastructure entière qui prend en charge cette application. Vous achetez et exécutez une application logicielle à partir d'un fournisseur d'hébergement de cloud. Windows InTune™ et Microsoft Office 365 sont des exemples de SaaS.

Clouds publics et privés

Un *cloud public* est un service de cloud computing qui est hébergé par un fournisseur de services de cloud computing et mis à disposition pour un usage public. Un cloud public peut héberger un locataire unique ou il peut héberger des locataires issus de plusieurs organisations. En tant que tel, la sécurité d'un cloud public n'est pas aussi forte que celle d'un cloud privé, mais l'hébergement dans un cloud public est en général moins coûteux parce que les différents locataires absorbent le coût.

À l'inverse, les *clouds privés* représentent une infrastructure de cloud computing dédiée à une organisation unique. Les clouds privés peuvent être hébergés par l'organisation elle-même ou peuvent être hébergés par un fournisseur de services de cloud computing qui garantit que les services de cloud computing ne sont partagés avec aucune autre organisation.

Les clouds privés sont plus que des déploiements d'hyperviseur à grande échelle. Ils peuvent utiliser la suite de gestion Microsoft System Center 2012, qui permet d'assurer la remise en libre-service de services et d'applications. Par exemple, dans une organisation disposant de son propre cloud privé, les utilisateurs pourraient utiliser un portail en libre-service pour demander des applications multicouches comprenant le serveur Web, le serveur de base de données et les composants de stockage. Windows Server 2012 et les composants de la suite System Center 2012 sont configurés de telle manière que cette demande de service puisse être traitée automatiquement, sans requérir le déploiement manuel d'ordinateurs virtuels ni du logiciel serveur de base de données.

> **Question :** Quel type de cloud utiliseriez-vous pour déployer un ordinateur virtuel personnalisé exécutant Windows Server 2012 ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éditions de Windows Server 2012

Il existe plusieurs éditions différentes de Windows Server 2012 parmi lesquelles choisir. Ces éditions permettent aux organisations de sélectionner une version de Windows Server 2012 qui répond au mieux à leurs besoins, plutôt que de payer pour des fonctionnalités dont elles n'ont pas besoin.

Lors du déploiement d'un serveur pour un rôle spécifique, les administrateurs système peuvent faire des économies substantielles en sélectionnant l'édition appropriée.

Le tableau ci-dessous répertorie les éditions de Windows Server 2012.

Édition	Description
Système d'exploitation Windows Server 2012 Standard	Fournit l'ensemble des rôles et des fonctionnalités disponibles sur la plateforme Windows Server 2012. Prend en charge jusqu'à 64 sockets et jusqu'à 4 téraoctets (To) de mémoire vive (RAM). Inclut deux licences d'ordinateur virtuel.
Système d'exploitation Windows Server 2012 Datacenter	Fournit l'ensemble des rôles et des fonctionnalités qui sont disponibles sur la plateforme Windows Server 2012. Inclut des licences d'ordinateur virtuel illimitées pour les ordinateurs virtuels qui sont exécutés sur le même matériel. Prend en charge 64 sockets, jusqu'à 640 cœurs de processeur et jusqu'à 4 To de RAM.
Système d'exploitation Windows Server 2012 Foundation	Conçu pour les gérants de PME, prend en charge seulement 15 utilisateurs, ne peut pas être joint à un domaine et inclut des rôles serveur limités. Prend en charge un cœur de processeur et jusqu'à 32 gigaoctets (Go) de RAM.
Système d'exploitation Windows Server 2012 Essentials	Édition suivante de Small Business Server. Doit être le serveur racine du domaine. Il ne peut pas fonctionner en tant que serveur Hyper-V®, de clustering avec basculement, avec installation minimale, ni de services Bureau à distance. Il présente des limites pour 25 utilisateurs et 50 périphériques. Prend en charge deux cœurs de processeur et 64 Go de RAM.
Microsoft Hyper-V Server 2012	Plateforme Hyper-V autonome pour ordinateurs virtuels sans interface utilisateur. Aucun coût de licence (gratuit) pour le système d'exploitation hôte, mais les ordinateurs virtuels font l'objet de licences standard. Prend en charge 64 sockets et 4 To de RAM. Prend en charge la jonction de domaine. Ne prend pas en charge d'autres rôles Windows Server 2012 que les fonctionnalités de services de fichiers limitées.
Système d'exploitation Windows Storage Server°2012 Workgroup	Périphérique de stockage unifié au niveau des entrées. Limité à 50 utilisateurs, à un cœur de processeur et à 32 Go de RAM. Prend en charge la jonction de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

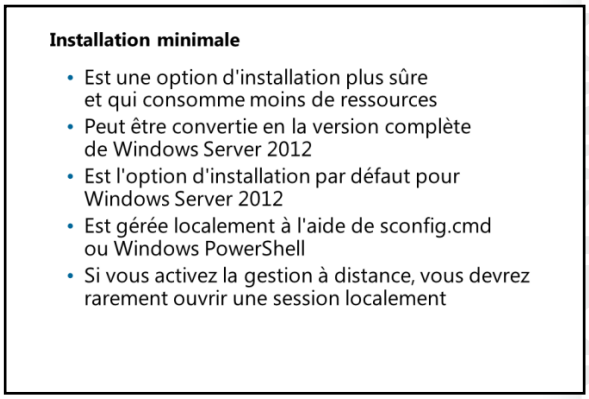
(suite)

Édition	Description
Système d'exploitation Windows Storage Server 2012 Standard	Prend en charge 64 sockets, mais fait l'objet d'une licence sur la base d'une incrémentation à deux sockets. Prend en charge 4 To de RAM. Inclut deux licences d'ordinateur virtuel. Prend en charge la jonction de domaine. Prend en charge certains rôles, y compris les rôles serveur DNS et DHCP, mais n'en prend pas en charge d'autres, dont notamment Services de domaine Active Directory® (AD DS), Services de certificats Active Directory (AD CS) et Services ADFS (Active Directory Federation Services).
Système d'exploitation Windows MultiPoint Server 2012 Standard	Prend en charge plusieurs utilisateurs accédant directement au même ordinateur hôte en utilisant une souris, un clavier et des moniteurs distincts. Limité à un socket, à 32 Go de RAM et à un maximum de 12 sessions. Prend en charge certains rôles, y compris les rôles serveur DNS et DHCP, mais n'en prend pas en charge d'autres, dont notamment AD DS, AD CS et ADFS. Ne prend pas en charge la jonction de domaine.
Système d'exploitation Windows MultiPoint Server 2012 Premium	Prend en charge plusieurs utilisateurs accédant directement au même ordinateur hôte en utilisant une souris, un clavier et des moniteurs distincts. Limité à deux sockets, à 4 To de RAM et à un maximum de 22 sessions. Prend en charge certains rôles, y compris les rôles serveur DNS et DHCP, mais n'en prend pas en charge d'autres, dont notamment AD DS, AD CS et ADFS. Prend en charge la jonction de domaine.

Documentation supplémentaire : Pour plus d'informations sur les différences entre les éditions de Windows Server 2012, consultez le catalogue Windows Server à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkID=266736.

Qu'est-ce que l'installation minimale ?

L'*installation minimale* est une option d'installation utilisée pour Windows Server 2012, qui peut contenir des variantes de l'interface graphique utilisateur selon les exigences. L'installation minimale peut être gérée localement à l'aide de Windows PowerShell ou d'une interface de ligne de commande, plutôt qu'en utilisant des outils basés sur l'interface graphique utilisateur, ou à distance à l'aide de l'une des options de gestion à distance que nous étudierons plus tard dans le module. L'installation minimale est l'option d'installation par défaut utilisée lors de l'installation de Windows Server 2012.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'installation minimale est l'option d'installation par défaut utilisée lors de l'installation de Windows Server 2012. L'installation minimale présente les avantages suivants par rapport à un déploiement traditionnel de Windows Server 2012 :

- Réduction des exigences en matière de mise à jour. Comme l'installation minimale installe moins de composants, son déploiement exige que vous installiez moins de mises à jour logicielles. Ceci réduit le nombre de redémarrages mensuels et le temps de maintenance requis pour un administrateur.
- Encombrement matériel réduit. Les ordinateurs avec installation minimale requièrent moins de RAM et moins d'espace disque. Une fois virtualisé, ceci signifie que vous pouvez déployer plus de serveurs sur le même hôte.

De plus en plus d'applications serveur Microsoft sont conçues pour s'exécuter sur des ordinateurs dotés de systèmes d'exploitation avec installation minimale. Par exemple, vous pouvez installer SQL Server 2012 sur des ordinateurs qui exécutent la version avec installation minimale de Windows Server 2008 R2.

Vous pouvez basculer d'une installation minimale à la version graphique de Windows Server 2012 en exécutant l'applet de commande Windows PowerShell suivante, où c:\mount correspond au répertoire racine d'une image montée contenant la version complète des fichiers d'installation de Windows Server 2012 :

```
Install-WindowsFeature -IncludeAllSubFeature User-Interfaces-Infra -Source c:\mount
```

Vous pouvez également utiliser Windows Update ou le DVD d'installation comme source des fichiers d'installation. L'installation des composants graphiques vous permet d'effectuer les tâches d'administration en utilisant les outils graphiques.

Une fois que vous avez effectué les tâches d'administration nécessaires, vous pouvez rétablir l'ordinateur dans sa configuration avec installation minimale d'origine. Vous pouvez basculer un ordinateur doté de la version graphique de Windows Server 2012 en mode d'installation minimale en supprimant les composants suivants dans la fonctionnalité « Interfaces utilisateur et infrastructure » :

- Outils et infrastructure de gestion graphique. Ce composant contient une interface serveur minimale qui fournit des outils d'interface utilisateur de gestion de serveur, tels qu'un gestionnaire de serveur et des outils d'administration.)
- Shell graphique du serveur. Ce composant contient l'interface utilisateur graphique complète avec Internet Explorer, l'Explorateur de fichiers et d'autres composants d'interface utilisateur. (Il est plus encombrant que l'option Outils et infrastructure de gestion graphique.)

Remarque : Soyez prudent lorsque vous supprimez les fonctionnalités graphiques, car certains serveurs auront d'autres composants installés qui dépendent de ces fonctionnalités.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous êtes connecté localement, vous pouvez utiliser les outils répertoriés dans le tableau ci-dessous pour gérer les déploiements avec installation minimale de Windows Server 2012.

Outil	Fonction
Cmd.exe	Vous permet d'exécuter des outils en ligne de commande traditionnels tels que ping.exe, ipconfig.exe et netsh.exe.
PowerShell.exe	Lance une session Windows PowerShell sur le déploiement avec installation minimale. Vous pouvez alors effectuer les tâches Windows PowerShell normalement.
Sconfig.cmd	Outil d'administration en ligne de commande piloté par menus qui permet d'effectuer les tâches d'administration de serveur les plus courantes.
Notepad.exe	Permet d'utiliser l'éditeur de texte Notepad.exe dans l'environnement avec installation minimale.
Regedt32.exe	Fournit l'accès au Registre dans l'environnement avec installation minimale.
Msinfo32.exe	Permet d'afficher les informations système sur le déploiement avec installation minimale.
Taskmgr.exe	Lance le Gestionnaire des tâches.
SCregEdit.wsf	Permet d'activer le Bureau à distance sur le déploiement avec installation minimale.

Remarque : Si vous fermez par erreur la fenêtre de commande sur un ordinateur qui exécute l'installation minimale, vous pouvez récupérer la fenêtre de commande en procédant comme suit :

1. Appuyez sur les touches Ctrl+Alt+Suppr, puis cliquez sur Ouvrir le Gestionnaire des tâches.
2. Dans le menu Fichier, cliquez sur Nouvelle tâche (Exécuter...), puis tapez cmd.exe.

L'installation minimale prend en charge la plupart des rôles et fonctionnalités de Windows Server 2012. Toutefois, vous ne pouvez pas installer les rôles suivants sur un ordinateur exécutant l'installation minimale :

- ADFS
- Serveur d'applications
- Services de stratégie et d'accès réseau (NPAS)
- Services de déploiement Windows (WDS)

Même si un rôle est disponible pour un ordinateur qui exécute l'option d'installation minimale, un service de rôle spécifique associé à ce rôle peut ne pas être disponible.

Remarque : Vous pouvez vérifier les rôles disponibles ou non dans l'installation minimale en exécutant la requête **Get-WindowsFeature | where-object {$_.InstallState -eq "Removed"}**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez utiliser les outils suivants pour gérer à distance un ordinateur qui exécute l'option d'installation minimale :

- Gestionnaire de serveur. Vous pouvez ajouter un serveur exécutant l'installation minimale au Gestionnaire de serveur sur un serveur qui exécute une installation complète de Windows. Vous pouvez alors gérer les rôles Serveur s'exécutant sur l'ordinateur avec installation minimale dans le Gestionnaire de serveur. Vous pouvez configurer le Bureau à distance avec Sconfig.cmd.
- Windows PowerShell à distance. Windows PowerShell à distance vous permet d'exécuter des commandes ou des scripts Windows PowerShell sur des serveurs distants correctement configurés quand le script est hébergé sur le serveur local. Windows PowerShell à distance vous permet également de charger des modules Windows PowerShell, tels que le Gestionnaire de serveur, localement et d'exécuter les applets de commande disponibles dans ces modules sur des serveurs distants convenablement configurés.
- Bureau à distance. Vous pouvez vous connecter à un ordinateur qui exécute l'option d'installation minimale en utilisant le Bureau à distance. Vous pouvez configurer le Bureau à distance avec Sconfig.cmd.
- Consoles de gestion à distance. Pour la plupart des rôles serveur, vous pouvez ajouter un ordinateur exécutant l'installation minimale à une console de gestion qui s'exécute sur un autre ordinateur.

Rôles de Windows Server 2012

Pour planifier correctement comment vous allez utiliser Windows Server 2012 pour prendre en charge les exigences de votre organisation, vous devez être pleinement conscient des rôles qui sont disponibles dans le cadre du système d'exploitation. Chaque version de Windows Server présente un ensemble différent de rôles. Lorsque de nouvelles versions de Windows Server sont mises sur le marché, certains rôles sont améliorés et d'autres sont abandonnés. Dans l'ensemble, les rôles disponibles dans Windows Server 2012 sont bien connus des professionnels de l'informatique ayant déjà administré Windows Server 2008 et Windows Server 2003.

Fonctions

- Serveur Web
- Contrôleur de domaine
- Serveur de certificats

Rôles

- Se composent des composants de services de rôle qui fournissent la fonctionnalité supplémentaire associée au rôle
- Dans le Gestionnaire de serveur 2012, les serveurs de console disposant d'un rôle semblable sont regroupés
- Le déploiement des rôles comprend également la configuration des dépendances

Windows Server 2012 prend en charge les rôles serveur répertoriés dans le tableau ci-dessous.

Rôle	Fonction
AD CS	Permet de déployer des autorités de certification et les services de rôle associés.
AD DS	Banque centralisée d'informations sur les objets réseau, y compris les comptes d'utilisateur et d'ordinateur. Utilisé pour l'authentification et l'autorisation.
ADFS	Fournit la prise en charge de l'authentification unique (SSO) via le Web et de la fédération des identités sécurisée.
Active Directory Lightweight Directory Services (AD LDS)	Prend en charge le stockage des données spécifiques aux applications pour les applications orientées annuaire qui ne requièrent pas l'infrastructure complète des services de domaine Active Directory.

(suite)

Rôle	Fonction
Active Directory Rights Management Services (AD RMS)	Permet d'appliquer des stratégies de gestion des droits pour empêcher tout accès non autorisé à des documents sensibles.
Serveur d'applications	Prend en charge la gestion et l'hébergement centralisés d'applications métier distribuées à hautes performances, telles que celles créées à l'aide de Microsoft .NET Framework 4.5.
Serveur DHCP	Configure les ordinateurs clients dans le réseau avec les adresses IP temporaires.
Serveur DNS	Fournit la résolution des noms pour les réseaux TCP/IP.
Serveur de télécopie	Prend en charge l'envoi et la réception de télécopies. Permet également de gérer les ressources de télécopie dans le réseau.
Services de fichiers et de stockage	Prend en charge la gestion du stockage des dossiers partagés, du système de fichiers distribués (DFS) et du stockage réseau.
Hyper-V	Permet d'héberger des ordinateurs virtuels sur des ordinateurs qui exécutent Windows Server 2012.
Stratégie réseau et services d'accès	Infrastructure d'autorisation pour connexions à distance, y compris l'autorité HRA (Health Registration Authority) pour la protection d'accès réseau (NAP).
Services document et d'impression et de numérisation	Prend en charge la gestion centralisée des tâches de document, y compris les scanneurs réseau et les imprimantes en réseau.
Accès à distance	Prend en charge une connectivité transparente, toujours active et toujours gérée, basée sur la fonctionnalité DirectAccess de Windows 7. Prend en charge également l'accès à distance via un réseau privé virtuel (VPN) et de connexions d'accès à distance.
Services Bureau à distance (RDS)	Prend en charge l'accès aux bureaux virtuels, aux bureaux basés sur une session et aux programmes RemoteApp.
Services d'activation en volume	Permet d'automatiser et de simplifier la gestion des clés de licence en volume et de l'activation des clés de volume. Permet de gérer un hôte du service de gestion de clés (KMS) ou de configurer l'activation basée sur AS DS pour les ordinateurs membres du domaine.
Serveur Web (IIS)	Composant de serveur Web de Windows Server 2012.
Services de déploiement Windows	Permettent de déployer des systèmes d'exploitation serveur sur des clients via un réseau.
Windows Server Update Services (WSUS)	Fournit une méthode de déploiement de mises à jour des produits Microsoft aux ordinateurs du réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Quand vous déployez un rôle, Windows Server 2012 configure automatiquement les aspects de la configuration du serveur (tels que les paramètres du pare-feu), pour prendre en charge le rôle. Windows Server 2012 déploie également automatiquement et simultanément les dépendances des rôles. Par exemple, quand vous installez le rôle WSUS, les composants du rôle Serveur Web (IIS) qui sont requis pour prendre en charge le rôle WSUS sont également installés automatiquement.

Vous ajoutez et supprimez des rôles à l'aide de l'Assistant Ajout de rôles et de fonctionnalités, qui est disponible à partir de la console du Gestionnaire de serveur de Windows Server 2012. Si vous utilisez l'installation minimale, vous pouvez également ajouter et supprimer des rôles à l'aide des applets de commande Windows PowerShell **Install-WindowsFeature** et **Remove-WindowsFeature**.

Question : Quels rôles sont souvent colocalisés sur le même serveur ?

Quelles sont les fonctionnalités de Windows Server 2012 ?

Les *fonctionnalités* Windows Server 2012 sont des composants indépendants qui prennent souvent en charge les services de rôle ou prennent en charge le serveur directement. Par exemple, la Sauvegarde Windows Server est une fonctionnalité car elle fournit uniquement la prise en charge de la sauvegarde pour le serveur local ; ce n'est pas une ressource que d'autres serveurs du réseau peuvent utiliser.

Windows Server 2012 inclut les fonctionnalités répertoriées dans le tableau ci-dessous.

Fonctionnalités
- Sont les composants qui prennent en charge le serveur tel que la Sauvegarde Windows Server ou le clustering avec basculement
- Ne fournissent habituellement pas un service directement aux clients sur le réseau

Gardez à l'esprit les points suivants
- Les rôles peuvent avoir des fonctionnalités comme dépendances
- Les fonctionnalités à la demande sont des fonctionnalités qui doivent être installées à l'aide d'une image montée comme source

Fonctionnalité	Description
Fonctionnalités .NET Framework 3.5	Installe les technologies .NET Framework 3.5.
Fonctionnalités .NET Framework 4.5	Installe les technologies .NET Framework 4.5. Cette fonctionnalité est installée par défaut.
Service de transfert intelligent en arrière-plan (BITS)	Permet le transfert asynchrone des fichiers pour garantir que d'autres applications réseau ne sont pas affectées défavorablement.
Chiffrement de lecteur BitLocker® Windows	Prend en charge le chiffrement de disque complet et de volume complet, ainsi que la protection d'environnement de démarrage.
Déverrouillage réseau BitLocker	Fournit un protecteur de clé basé sur le réseau qui peut déverrouiller les systèmes d'exploitation verrouillés, joints au domaine et protégés par BitLocker.
Windows BranchCache®	Permet au serveur de fonctionner en tant que serveur de cache hébergé ou serveur de contenu BranchCache pour les clients BranchCache.
Client pour NFS	Fournit un accès aux fichiers stockés sur les serveurs NFS (Network File System).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Fonctionnalité	Description
Data Center Bridging	Permet d'appliquer une allocation de bande passante à des cartes réseau convergentes.
Stockage étendu	Fournit une prise en charge pour les fonctionnalités supplémentaires disponibles dans le périphérique d'accès au stockage étendu (protocole IEEE 1667), y compris des restrictions d'accès aux données.
Clustering avec basculement	Fonctionnalité à haute disponibilité qui permet à Windows Server 2012 de participer au clustering avec basculement.
Gestion des stratégies de groupe	Outil de gestion administrative permettant d'administrer une stratégie de groupe sur l'ensemble d'une entreprise.
Services d'encre et de reconnaissance de l'écriture manuscrite	Permet d'utiliser la prise en charge du mode d'entrée manuscrite et la reconnaissance de l'écriture manuscrite.
Client d'impression Internet	Prend en charge l'utilisation du protocole IPP (Internet Printing Protocol).
Serveur de gestion d'adresses IP (IPAM)	Gestion centralisée de l'infrastructure d'adresse IP et d'espace de noms.
Fournisseur de stockage cible iSCSI (Internet SCSI)	Fournit des services de gestion de disques et de cible iSCSI à Windows Server 2012.
Service Serveur iSNS (Internet Storage Name Service)	Prend en charge les services de découverte des réseaux SAN iSCSI.
Moniteur de port LPR (Line Printer Remote)	Permet à l'ordinateur d'envoyer les travaux d'impression aux imprimantes qui sont partagées à l'aide du service LPD (Line Printer Daemon).
Extension IIS de gestion OData (Open Data Protocol)	Permet d'exposer les applets de commande Windows PowerShell via un service Web basé sur OData qui s'exécute sur la plateforme des services Internet (IIS).
Media Foundation	Prend en charge l'infrastructure des fichiers multimédia.
Message Queuing	Prend en charge la remise de messages entre les applications.
MPIO (Multipath Input/Output)	Prend en charge plusieurs chemins de données jusqu'aux dispositifs de stockage.
Équilibrage de la charge réseau	Permet la distribution du trafic avec équilibrage de la charge entre plusieurs serveurs qui hébergent la même application sans état.
Protocole PNRP (Peer Name Resolution Protocol)	Protocole de résolution de noms qui permet aux applications de résoudre les noms sur l'ordinateur.
Expérience audio-vidéo haute qualité Windows (qWave)	Prend en charge les applications de flux audio et vidéo sur les réseaux domestiques IP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Fonctionnalité	Description
Kit d'administration du Gestionnaire des connexions Microsoft de serveur d'accès à distance	Permet de créer des profils de gestionnaire de connexions qui simplifient le déploiement d'une configuration d'accès à distance sur les ordinateurs client.
Assistance à distance	Autorise un support technique à distance via d'invitations.
Compression différentielle à distance (RDC)	Transfère les différences entre les fichiers sur un réseau, réduisant au maximum l'utilisation de la bande passante.
Outils d'administration de serveur distant	Collection de consoles et d'outils pour gérer à distance les rôles et les fonctionnalités sur d'autres serveurs.
Proxy RPC sur HTTP	Transmet le trafic RPC via HTTP comme alternative aux connexions VPN.
Services TCP/IP simples	Prend en charge les services TCP/IP de base, y compris Citation du jour.
Serveur SMTP (Simple Mail Transfer Protocol)	Prend en charge le transfert des messages électroniques.
Service SNMP (Simple Network Management Protocol)	Inclut des agents SNMP qui sont utilisés avec les services de gestion de réseau.
Sous-système pour les applications UNIX	Prend en charge les applications UNIX compatibles POSIX (Portable Operating System Interface for UNIX).
Client Telnet	Autorise les connexions sortantes aux serveurs Telnet et à d'autres services TCP (Transmission Control Protocol).
Serveur Telnet	Permet aux clients de se connecter au serveur à l'aide du protocole Telnet.
Client TFTP (Trivial File Transfer Protocol)	Permet d'accéder aux serveurs TFTP.
Interfaces utilisateur et infrastructure	Contient les composants nécessaires pour prendre en charge l'option d'installation d'interface graphique sur Windows Server 2012. Sur les installations graphiques, cette fonctionnalité est installée par défaut.
Windows Biometric Framework (WBF)	Permet l'utilisation de lecteurs d'empreintes digitales pour l'authentification.
Transfert de commentaires sur Windows	Prend en charge l'envoi de commentaires à Microsoft lors de l'adhésion à un programme d'amélioration de l'expérience utilisateur.
Windows Identity Foundation 3.5	Ensemble de classes .NET Framework qui prennent en charge l'implémentation d'une identité basée sur des demandes pour les applications .NET.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Fonctionnalité	Description
Base de données interne Windows	Banque de données relationnelles qui peut être utilisée uniquement par les rôles et les fonctionnalités de Windows, tels que WSUS.
Windows PowerShell	Langage de script et interpréteur de ligne de commande basé sur les tâches, utilisé pour administrer les ordinateurs exécutant des systèmes d'exploitation Windows. Cette fonctionnalité est installée par défaut.
Accès Web Windows PowerShell	Permet la gestion à distance d'ordinateurs via l'exécution de sessions Windows PowerShell dans un navigateur Web.
Service d'activation des processus Windows (WAS)	Permet aux applications hébergeant les services WCF (Windows Communication Foundation) qui n'utilisent pas les protocoles HTTP d'utiliser les fonctionnalités IIS.
Service de recherche Windows	Permet une recherche rapide des fichiers hébergés sur un serveur pour les clients compatibles avec le service de recherche Windows.
Sauvegarde Windows Server	Logiciel de sauvegarde et de restauration pour Windows Server 2012.
Outils de migration de Windows Server	Collection d'applets de commande Windows PowerShell qui favorisent la migration des rôles serveur, des paramètres du système d'exploitation, des fichiers et des partages à partir d'ordinateurs exécutant des versions antérieures des systèmes d'exploitation Windows Server vers Windows Server 2012.
Gestion du stockage Windows basé sur des normes	Ensemble d'interfaces de programmation d'applications (API) qui permettent la découverte, la gestion et la surveillance des dispositifs de stockage qui utilisent des standards, tels que la norme SMI-S (Storage Management Initiative Specification).
Gestionnaire de ressources système Windows (WSRM)	Permet de contrôler l'allocation des ressources processeur et mémoire.
Windows TIFF IFilter	Prend en charge la reconnaissance optique des caractères dans les fichiers compatibles TIFF 6.0.
Extension WinRM IIS	Gestion à distance de Windows pour IIS.
Serveur WINS (Windows Internet Naming Service)	Prend en charge la résolution des noms pour les noms NetBIOS.
Service WLAN (Wireless Local Area Network)	Permet au serveur d'utiliser une interface de réseau sans fil.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Fonctionnalité	Description
Prise en charge WoW (Windows on Windows) 64	Prend en charge l'exécution des applications 32 bits sur les installations minimales. Cette fonctionnalité est installée par défaut.
Visionneuse XPS	Prend en charge l'affichage et la signature de documents dans des formats XPS.

Fonctionnalités à la demande

Les fonctionnalités à la demande permettent d'ajouter et de supprimer des fichiers de rôle et de fonctionnalités, également appelés *charge utile de fonctionnalité*, du système d'exploitation Windows Server 2012 pour économiser de l'espace. Vous pouvez installer des rôles et des fonctionnalités lorsque la charge utile de fonctionnalité n'est pas présente à l'aide d'une source distante, telle qu'une image montée du système d'exploitation complet. Si une source d'installation n'est pas présente mais qu'une connexion Internet l'est, les fichiers sources seront téléchargés de Windows Update. L'avantage d'une installation de type Fonctionnalités à la demande tient au fait qu'elle requiert moins d'espace disque qu'une installation traditionnelle. L'inconvénient est que si vous souhaitez ajouter un rôle ou une fonctionnalité, vous devez avoir accès à une source d'installation montée. Ceci n'est pas nécessaire si vous effectuez une installation de Windows Server 2012 avec les fonctionnalités graphiques activées.

Question : Quelle fonctionnalité devez-vous installer pour prendre en charge la résolution de noms NetBIOS pour les ordinateurs clients exécutant le système d'exploitation de type station de travail Microsoft Windows NT® 4.0 ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Vue d'ensemble de l'administration de Windows Server 2012

La configuration correcte d'un serveur peut vous permettre d'éviter des problèmes ultérieurs substantiels. Windows Server 2012 fournit plusieurs outils permettant d'effectuer des tâches d'administration spécifiques, dont chacune est appropriée à un ensemble spécifique de circonstances. L'interface de gestion de Windows Server 2012 améliore également votre capacité à effectuer les tâches d'administration sur plusieurs serveurs simultanément.

Dans cette leçon, vous allez découvrir les différents outils de gestion que vous pouvez utiliser pour effectuer les tâches d'administration sur les ordinateurs dotés du système d'exploitation Windows Server 2012.

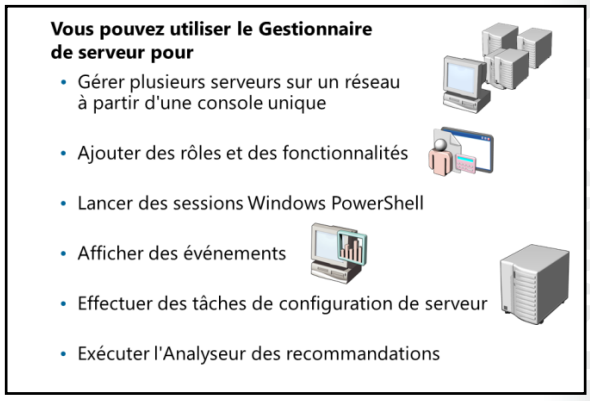
Objectifs de la leçon

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

- décrire le Gestionnaire de serveur ;
- expliquer comment utiliser les outils d'administration et les outils d'administration de serveur distant ;
- expliquer comment utiliser le Gestionnaire de serveur pour effectuer diverses tâches ;
- expliquer comment configurer les services ;
- expliquer comment configurer la gestion à distance de Windows.

Qu'est-ce que le Gestionnaire de serveur ?

Le Gestionnaire de serveur est le principal outil graphique que vous utilisez pour gérer les ordinateurs exécutant Windows Server 2012. Vous pouvez utiliser la console du Gestionnaire de serveur pour gérer le serveur local et les serveurs distants. Vous pouvez également gérer les serveurs sous forme de groupes. En gérant les serveurs sous forme de groupes, vous pouvez effectuer rapidement les mêmes tâches d'administration sur plusieurs serveurs exécutant le même rôle ou membres du même groupe.



Vous pouvez utiliser la console du Gestionnaire de serveur pour effectuer les tâches suivantes sur des serveurs locaux et des serveurs distants :

- ajouter des rôles et des fonctionnalités ;
- lancer des sessions Windows PowerShell ;
- afficher des événements ;
- effectuer des tâches de configuration de serveur.

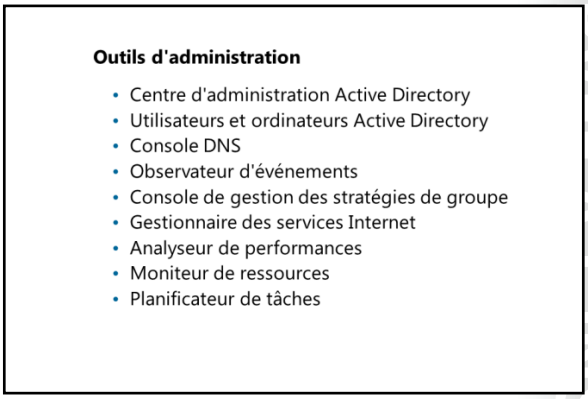
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Best Practices Analyzer

Le Gestionnaire de serveur inclut l'outil Best Practices Analyzer pour tous les rôles de Windows Server 2012. Best Practices Analyzer vous permet de déterminer si les rôles sur votre réseau fonctionnent efficacement ou si des problèmes se posent, qu'il convient de résoudre. Best Practices Analyzer examine comment un rôle fonctionne (notamment en interrogeant les journaux d'événements associés pour obtenir les événements d'erreur et d'avertissement). Vous pouvez ainsi vous rendre compte des problèmes d'intégrité associés à des rôles spécifiques, avant que ces derniers ne provoquent une défaillance pouvant affecter la fonctionnalité du serveur.

Outils d'administration et outils d'administration de serveur distant

Lorsque vous utilisez le Gestionnaire de serveur pour effectuer une tâche d'administration associée à un rôle ou à une fonctionnalité spécifique, la console lance l'outil d'administration approprié. Quand vous installez un rôle ou une fonctionnalité à l'aide du Gestionnaire de serveur localement ou à distance, vous êtes invité à installer l'outil d'administration approprié. Par exemple, si vous utilisez le Gestionnaire de serveur pour installer le rôle DHCP sur un autre serveur, vous serez invité à installer la console DHCP sur le serveur local.



Outils d'administration de serveur distant

Vous pouvez installer l'ensemble complet d'outils d'administration pour Windows Server 2012 en installant la fonctionnalité Outils d'administration de serveur distant (RSAT). Lorsque vous installez RSAT, vous pouvez choisir d'installer tous les outils ou seulement ceux permettant de gérer des rôles et des fonctionnalités spécifiques. Vous pouvez également installer RSAT sur les ordinateurs dotés du système d'exploitation Windows 8. Ceci permet aux administrateurs de gérer les serveurs à distance sans avoir à se connecter directement à chaque serveur.

La meilleure pratique générale consiste à exécuter les serveurs Windows Server 2012 avec une installation minimale gérée à distance via RSAT pour Windows 8 ou l'une des nombreuses autres méthodes de gestion à distance.

Outre Windows PowerShell, voici quelques-uns des outils que les administrateurs utilisent le plus généralement :

- Centre d'administration Active Directory. Cette console vous permet d'effectuer des tâches d'administration d'Active Directory, telles que l'augmentation des niveaux fonctionnels de domaine et de forêt et l'activation de la Corbeille Active Directory. Vous utilisez également cette console pour gérer le contrôle d'accès dynamique.
- Utilisateurs et ordinateurs Active Directory. Cet outil vous permet de créer et gérer des utilisateurs, des ordinateurs et des groupes Active Directory. Vous pouvez également utiliser cet outil pour créer des unités d'organisation (OU).
- Console DNS. La console DNS vous permet de configurer et de gérer le rôle serveur DNS. Ceci inclut la création de zones de recherche directe et inversée, ainsi que la gestion des enregistrements DNS.
- Observateur d'événements. Vous pouvez utiliser l'Observateur d'événements pour afficher les événements enregistrés dans les journaux d'événements de Windows Server 2012.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Console de gestion des stratégies de groupe. Cet outil vous permet de modifier les objets de stratégie de groupe (GPO) et de gérer leur application dans AD DS.
- Outil Gestionnaire des services Internet. Vous pouvez utiliser cet outil pour gérer des sites Web.
- Analyseur de performances. Vous pouvez utiliser cette console pour afficher les données de performance des enregistrements en sélectionnant les compteurs associés aux ressources spécifiques que vous souhaitez surveiller.
- Moniteur de ressources. Vous pouvez utiliser cette console pour afficher des informations en temps réel sur le processeur, la mémoire et l'utilisation du disque et du réseau.
- Planificateur de tâches. Vous pouvez utiliser cette console pour gérer l'exécution des tâches planifiées.

Vous pouvez accéder à chacun de ces outils dans le Gestionnaire de serveur en accédant au menu **Outils**.

Remarque : Vous pouvez également épingler les outils fréquemment utilisés à la barre des tâches de Windows Server 2012 ou à l'écran d'accueil.

Démonstration : Utilisation du Gestionnaire de serveur

Dans cette démonstration, vous allez apprendre à utiliser le Gestionnaire de serveur pour effectuer les tâches suivantes :

- se connecter à Windows Server 2012 et afficher le Bureau de Windows Server 2012 ;
- ajouter une fonctionnalité en utilisant l'Assistant Ajout de rôles et de fonctionnalités ;
- afficher les événements associés à un rôle ;
- exécuter Best Practice Analyzer pour un rôle ;
- répertorier les outils disponibles à partir du Gestionnaire de serveur ;
- redémarrer Windows Server 2012.

Procédure de démonstration

Se connecter à Windows Server 2012 et afficher le Bureau de Windows Server 2012

- Connectez-vous à **LON-DC1** avec le compte **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**, puis fermez la console du Gestionnaire de serveur.

Ajouter une fonctionnalité en utilisant l'Assistant Ajout de rôles et de fonctionnalités

1. Dans la barre des tâches, ouvrez le **Gestionnaire de serveur**.
2. Démarrez l'Assistant Ajout de rôles et de fonctionnalités.
3. Activez la case à cocher **Installation basée sur un rôle ou une fonctionnalité**.
4. Cliquez sur **Sélectionner un serveur du pool de serveurs**, vérifiez que **LON-DC1.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez **Serveur de télécopie**.
6. Dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
7. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **BranchCache**.
8. Dans la page **Serveur de télécopie**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans la page **Services document et d'impression et de numérisation**, cliquez sur **Suivant** à deux reprises.
10. Dans la page **Confirmation**, activez la case à cocher **Redémarrer automatiquement le serveur de destination, si nécessaire**, cliquez sur **Oui**, cliquez sur **Installer**, puis cliquez sur **Fermer**.
11. Cliquez sur l'icône en forme de drapeau en regard de **Tableau de bord du Gestionnaire de serveur** et passez en revue les messages.

Remarque : Vous pouvez fermer cette console sans terminer la tâche.

Afficher les événements associés à un rôle

1. Cliquez sur le nœud **Tableau de bord**.
2. Dans le volet **Rôles et groupes de serveurs**, sous **DNS**, cliquez sur **Événements**.
3. Dans la boîte de dialogue **DNS - Événements Affichage des détails**, remplacez la période par **48 heures** et **Source de l'événement** par **Tous**.

Exécuter Best Practice Analyzer pour un rôle

1. Sous **DNS**, cliquez sur **Résultats BPA**.
2. Sélectionnez **Tous** dans le menu déroulant **Niveaux de gravité**, puis cliquez sur **OK**.

Répertorier les outils disponibles à partir du Gestionnaire de serveur

- Cliquez sur le menu **Outils** et examinez les outils qui sont installés sur **LON-DC1**.

Déconnecter l'utilisateur actuellement connecté

1. Déconnectez-vous de LON-DC1.
2. Reconnectez-vous à **LON-DC1** à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.

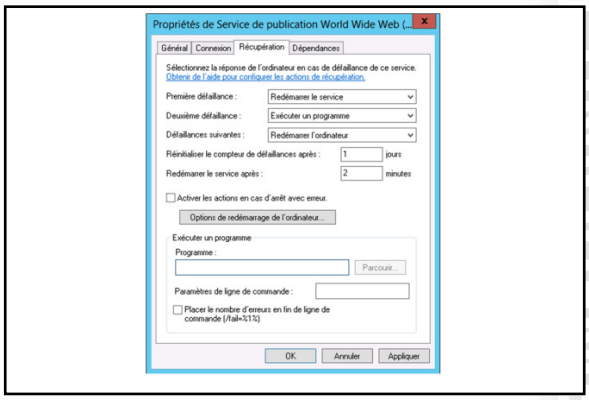
Redémarrer Windows Server 2012

- Dans une fenêtre Windows PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
Shutdown /r /t 15
```

Configuration de services

Les services sont des programmes qui s'exécutent en arrière-plan et fournissent des services aux clients et au serveur hôte. Vous pouvez gérer les services via la console Services, qui est disponible dans le Gestionnaire de serveur, dans le menu **Outils**. Lorsque vous sécurisez un ordinateur, vous devriez désactiver tous les services à l'exception de ceux qui sont requis par les rôles, les fonctionnalités et les applications qui sont installés sur le serveur.



Types de démarrage

Les services utilisent l'un des types de démarrage suivants :

- Automatique. Le service démarre automatiquement au démarrage du serveur.
- Automatique (début différé). Le service démarre automatiquement après le démarrage du serveur.
- Manuel. Le service doit être démarré manuellement, soit par un programme, soit par un administrateur.
- Désactivé. Le service est désactivé et ne peut pas être démarré.

Remarque : Si un serveur se comporte de façon problématique, ouvrez la console Services, triez par type de démarrage, puis localisez les services qui sont configurés pour démarrer automatiquement et ceux qui ne sont pas en état d'exécution.

Récupération des services

Les options de récupération déterminent ce qu'un service doit faire en cas de défaillance. Vous accédez à l'onglet **Récupération** à partir de la fenêtre des propriétés des serveurs DNS. Dans l'onglet **Récupération**, vous avez les options de récupération suivantes :

- Ne rien faire. Le service demeure dans un état défaillant jusqu'à ce qu'un administrateur s'en occupe.
- Redémarrer le service. Le service redémarre automatiquement.
- Exécuter un programme. Permet d'exécuter un programme ou un script.
- Redémarrer l'ordinateur. L'ordinateur redémarre après un nombre préconfiguré de minutes.

Vous pouvez configurer différentes options de récupération pour la première défaillance, la deuxième défaillance et les défaillances suivantes. Vous pouvez également configurer un laps de temps après lequel l'horloge de défaillance de service est réinitialisée.

Comptes de service administrés

Les comptes de service administrés sont des comptes spéciaux basés sur un domaine que vous pouvez utiliser avec des services. L'avantage d'un compte de service administré est que le mot de passe du compte fait l'objet d'une rotation automatique en fonction d'une planification. Ces changements du mot de passe sont automatiques et ne requièrent pas l'intervention de l'administrateur. Ceci réduit au maximum la probabilité que le mot de passe du compte de service soit compromis, chose qui se produit car des administrateurs attribuent généralement des mots de passe simples à des comptes de service avec le même service sur un grand nombre de serveurs et ne prennent jamais la peine de mettre à jour ces mots de passe. Les comptes virtuels sont des comptes spécifiques aux services, qui sont locaux plutôt que basés sur un domaine. Windows Server 2012 applique une rotation au mot de passe des comptes virtuels et le gère.

Question : Quel est l'avantage d'un compte de service administré par rapport à un compte de service traditionnel, basé sur un domaine ?

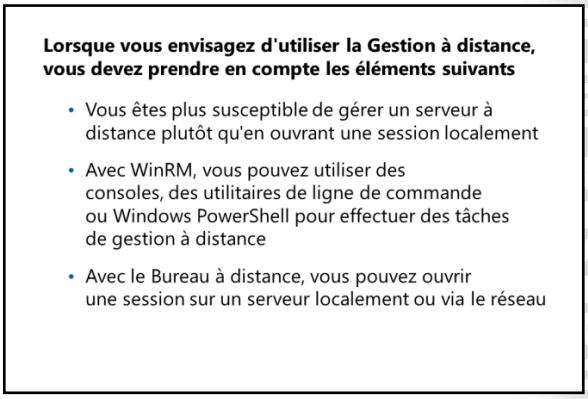
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de la gestion à distance de Windows

La plupart des administrateurs n'effectuent plus les tâches d'administration des systèmes uniquement dans la salle des serveurs. Presque toutes les tâches qu'ils effectuent quotidiennement sont à présent effectuées à l'aide des technologies de gestion à distance.

Avec la gestion à distance de Windows (WinRM), vous pouvez utiliser l'interpréteur de commandes distant, Windows PowerShell distant et d'autres outils d'administration à distance pour gérer à distance un ordinateur.



Vous pouvez activer WinRM à partir du Gestionnaire de serveur en procédant comme suit :

1. Dans la console du Gestionnaire de serveur, cliquez sur le nœud **Serveur local**.
2. Dans la boîte de dialogue **Propriétés** pour le serveur local, à côté de Gestion à distance, cliquez sur **Désactivé**. Ceci ouvre la boîte de dialogue **Configurer l'administration à distance**.
3. Dans la boîte de dialogue **Configurer l'administration à distance**, activez la case à cocher **Autoriser la gestion à distance de ce serveur depuis d'autres ordinateurs**, puis cliquez sur **OK**.

Vous pouvez également activer WinRM à partir d'une ligne de commande en exécutant la commande **WinRM -qc**. Vous désactivez WinRM à l'aide de la même méthode qui permet de l'activer. Vous pouvez désactiver WinRM sur un ordinateur exécutant l'option d'installation minimale à l'aide de l'outil sconfig.cmd.

Bureau à distance

Le Bureau à distance est la méthode traditionnelle utilisée par les administrateurs de systèmes pour se connecter à distance aux serveurs qu'ils administrent. Vous pouvez configurer le Bureau à distance sur un ordinateur qui exécute la version complète de Windows Server 2012 en procédant comme suit :

1. Dans la console du Gestionnaire de serveur, cliquez sur le nœud Serveur local.
2. À côté de Bureau à distance, cliquez sur **Désactivé**.
3. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Utilisation à distance**, sélectionnez l'une des options suivantes :
    - **Ne pas autoriser les connexions à cet ordinateur**. L'état par défaut du Bureau à distance est désactivé.
    - **Autoriser la connexion des ordinateurs exécutant n'importe quelle version du Bureau à distance**. Autorise la connexion des clients Bureau à distance qui ne prennent pas en charge l'authentification au niveau du réseau.
    - **Autoriser les connexions uniquement pour les ordinateurs exécutant les services Bureau à distance avec authentification au niveau du réseau**. Autorise la connexion sécurisée des ordinateurs exécutant des clients Bureau à distance qui prennent en charge l'authentification au niveau du réseau.

Vous pouvez activer et désactiver le Bureau à distance sur les ordinateurs qui exécutent l'option d'installation minimale à l'aide de l'outil en ligne de commande **sconfig.cmd**.

Leçon 3
Installation de Windows Server 2012

Lorsque vous préparez l'installation de Windows Server 2012, vous devez comprendre si une configuration matérielle particulière est appropriée. Vous devez également savoir si un déploiement avec installation minimale peut être plus approprié qu'un déploiement de l'interface utilisateur graphique complète, et quelle source d'installation vous permet de déployer Windows Server 2012 de façon efficace.

Dans cette leçon, vous allez découvrir le processus d'installation de Windows Server 2012, notamment les méthodes permettant d'installer le système d'exploitation, les différentes options d'installation, la configuration requise minimale et les décisions que vous devez prendre lors de l'utilisation de l'Assistant Installation.

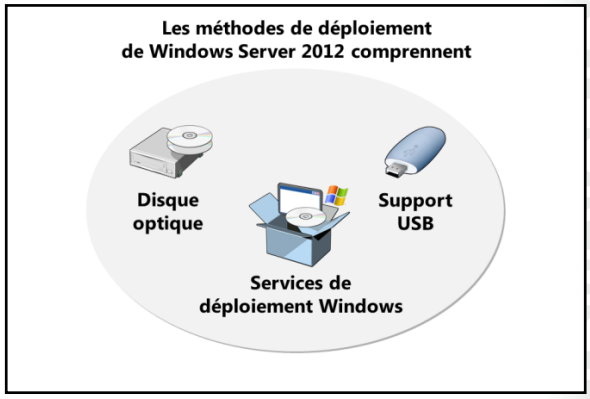
Objectifs de la leçon

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

- décrire les différentes méthodes que vous pouvez utiliser pour installer Windows Server 2012 ;
- identifier les différents types d'installation que vous pouvez choisir en installant Windows Server 2012 ;
- déterminer si un ordinateur ou un ordinateur virtuel répond à la configuration matérielle minimale requise pour l'installation de Windows Server 2012 ;
- décrire les décisions que vous devez prendre lorsque vous effectuez une installation de Windows Server 2012.

Méthodes d'installation

Microsoft distribue Windows Server 2012 sur des médias optiques et dans un format d'image ISO (.iso). Le format ISO devient plus courant que l'obtention d'un média amovible physique, du fait que les organisations acquièrent des logiciels via Internet.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une fois que vous avez obtenu le système d'exploitation Windows Server 2012 auprès de Microsoft, vous pouvez utiliser votre propre méthode pour déployer le système d'exploitation. Vous pouvez installer Windows Server 2012 en utilisant diverses méthodes, y compris les méthodes suivantes :

- Supports optiques
  - Avantages :
    - Méthode traditionnelle de déploiement.
  - Inconvénients :
    - Exige que l'ordinateur ait accès à un lecteur de DVD-ROM.
    - Généralement plus lent qu'un média USB.
    - Vous ne pouvez pas mettre à jour l'image d'installation sans remplacer le média.
    - Vous pouvez effectuer une seule installation par DVD-ROM à la fois.
- Support USB
  - Avantages :
    - Tous les ordinateurs avec des lecteurs USB permettent un démarrage à partir du média USB.
    - L'image peut être mise à jour lorsque de nouvelles mises à jour logicielles et de nouveaux pilotes sont disponibles.
    - Le fichier de réponse peut être stocké sur un lecteur USB, réduisant ainsi au maximum la part d'interaction requise de l'administrateur.
  - Inconvénients :
    - Requiert que l'administrateur effectue des opérations spéciales pour préparer le média USB à partir d'un fichier ISO.
- Image ISO montée
  - Avantages :
    - Un logiciel de virtualisation vous permet de monter l'image ISO directement et d'installer Windows Server 2012 sur l'ordinateur virtuel.
  - Inconvénients :
    - Aucun.
- Partage réseau
  - Avantages :
    - Il est possible de démarrer un serveur à partir d'un périphérique de démarrage (DVD ou lecteur USB) et de l'installer à partir des fichiers d'installation qui sont hébergés sur un partage réseau.
  - Inconvénients :
    - Cette méthode est beaucoup plus lente que l'utilisation des services de déploiement Windows. Si vous avez déjà accès à un DVD ou à un média USB, il est plus simple d'utiliser ces outils pour le déploiement du système d'exploitation.

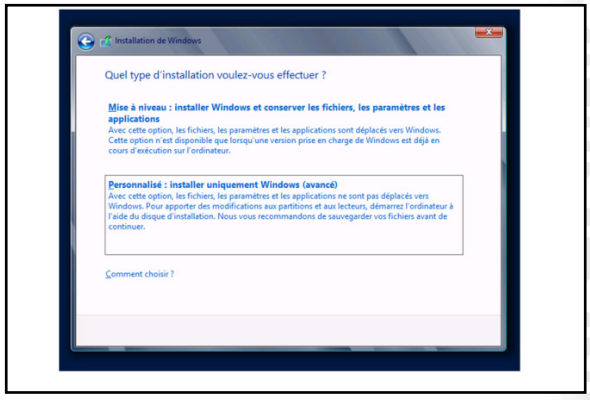
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Services de déploiement Windows
  - Avantages :
    - Vous pouvez déployer Windows Server 2012 à partir de fichiers image .wim ou de fichiers VHD spécialement préparés.
    - Vous pouvez utiliser le Kit d'installation automatisée (AIK) pour configurer un déploiement de type Lite Touch.
    - Les clients exécutent un démarrage PXE (Preboot eXecution Environment) pour contacter le serveur Windows DS et l'image du système d'exploitation est transmise au serveur via le réseau.
    - Les services de déploiement Windows permettent plusieurs installations simultanées de Windows Server 2012 en utilisant des transmissions de réseau de multidiffusion.
- System Center Configuration Manager
  - Avantages :
    - Le Gestionnaire de configuration vous permet d'automatiser entièrement le déploiement de Windows Server 2012 sur de nouveaux serveurs qui ne sont pas dotés d'un système d'exploitation. Ce processus est appelé *Déploiement Zero Touch*.
- Modèles Virtual Machine Manager
  - Avantages :
    - Windows Server 2012 est généralement déployé dans des scénarios de cloud privé à partir de modèles préconfigurés d'ordinateur virtuel. Vous pouvez configurer plusieurs composants de la suite System Center pour permettre le déploiement en libre-service des ordinateurs virtuels Windows Server 2012.

Question : Quelle autre méthode est-il possible d'utiliser pour déployer Windows Server 2012 ?

Types d'installation

La manière dont vous déployez Windows Server 2012 sur un serveur spécifique dépend des circonstances de cette installation. L'installation sur un serveur qui exécute Windows Server 2008 R2 requiert des actions différentes par rapport à l'installation sur un serveur exécutant une édition x86 de Windows Server 2003.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous effectuez une installation du système d'exploitation Windows Server 2012, vous pouvez choisir l'une des options répertoriées dans le tableau ci-dessous.

Option d'installation	Description
Nouvelle installation	Vous permet d'effectuer une nouvelle installation sur un nouveau disque ou volume. Les nouvelles installations sont celles qui sont le plus souvent utilisées et qui prennent le moins de temps. Vous pouvez également utiliser cette option pour configurer Windows Server 2012 afin d'effectuer un double démarrage si vous souhaitez conserver le système d'exploitation existant.
Mise à niveau	Une mise à niveau conserve les fichiers, les paramètres et les applications qui sont déjà installés sur le serveur d'origine. Vous pouvez effectuer une mise à niveau lorsque vous souhaitez conserver tous ces éléments et souhaitez continuer à utiliser le même matériel de serveur. Vous pouvez effectuer une mise à niveau vers une édition équivalente ou plus récente de Windows Server 2012 uniquement à partir des versions x64 de Windows Server 2008 ou Windows Server 2008 R2. Vous lancez une mise à niveau en exécutant setup.exe au sein du système d'exploitation Windows Server d'origine.
Migration	Utilisez la migration pour migrer des versions x86 et x64 de Windows Server 2003, Windows Server 2003 R2 ou Windows Server 2008 vers Windows Server 2012. Vous pouvez utiliser les fonctionnalités des Outils de migration de Windows Server dans Windows Server 2012 pour transférer des fichiers et des paramètres.

Quand vous effectuez une nouvelle installation, vous pouvez déployer Windows Server 2012 sur un disque non partitionné ou sur un volume existant. Vous pouvez aussi installer Windows Server 2012 dans un fichier de disque dur virtuel préparé à cet effet dans un scénario « Démarrage depuis un disque dur virtuel » ou « Démarrage natif depuis un disque dur virtuel » (ces deux termes sont utilisés tels quels ou avec des variantes pour désigner ce scénario). Le démarrage à partir d'un VHD requiert une préparation spéciale et n'est pas une option possible lorsque vous effectuez une installation par défaut à l'aide de l'Assistant Installation de Windows.

Configuration matérielle requise pour Windows Server 2012

La configuration matérielle requise définit le matériel minimal qui est requis pour exécuter le serveur Windows Server 2012. Votre configuration matérielle requise peut être plus importante selon les services que le serveur héberge, la charge sur le serveur et la réactivité de votre serveur.

Chaque service de rôle et fonctionnalité place une charge unique sur le réseau, les E/S de disque, le processeur et les ressources mémoire. Par exemple, le rôle de serveur de fichiers place sur le matériel de serveur des contraintes différentes de celles du rôle DHCP.

Windows Server 2012 présente la configuration matérielle minimale requise suivante

- Architecture du processeur x64
- Cadence du processeur 1,4 GHz
- Mémoire vive (RAM) 512 Mo
- Espace disponible sur le disque dur 32 Go
  - Davantage d'espace est disponible sur le disque dur si le serveur possède plus de 16 Go de RAM

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous prenez en compte la configuration matérielle requise, souvenez-vous que Windows Server 2012 peut être déployé virtuellement. Windows Server 2012 est pris en charge sur Hyper-V et sur certaines autres plateformes de virtualisation non-Microsoft. Les déploiements virtualisés de Windows Server 2012 doivent correspondre aux mêmes spécifications matérielles que les déploiements physiques. Par exemple, lorsque vous créez un ordinateur virtuel pour héberger Windows Server 2012, vous devez vous assurer de configurer l'ordinateur virtuel avec suffisamment de mémoire et d'espace disque.

Windows Server 2012 présente la configuration matérielle minimale requise suivante :

- Architecture du processeur : x64
- Cadence du processeur : 1,4 gigahertz (GHz)
- Mémoire vive (RAM) : 512 mégaoctets (Mo)
- Espace disponible sur le disque dur : 32 Go, plus si le serveur a plus de 16 Go de RAM.

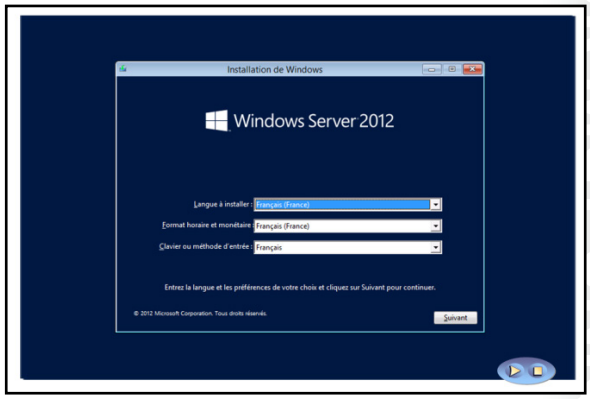
L'édition Datacenter de Windows Server 2012 prend en charge la configuration matérielle maximale suivante :

- 640 processeurs logiques
- 4 To de RAM
- 63 nœuds de cluster de basculement

Documentation supplémentaire : Pour plus d'informations sur le programme Windows Server Virtualization Validation Program, voir http://go.microsoft.com/fwlink/?LinkID=266736.

Question : Pourquoi un serveur a-t-il besoin de plus d'espace disponible sur le disque dur s'il possède plus de 16 Go de RAM ?

Installation de Windows Server 2012



Le processus de déploiement du système d'exploitation Windows Server est plus simple aujourd'hui qu'il était auparavant. L'administrateur chargé du déploiement a moins de décisions à prendre, bien que ces décisions soient essentielles au succès du déploiement. Une installation par défaut de Windows Server 2012 (si vous n'avez pas encore de fichier de réponse) implique l'exécution des opérations suivantes :

1. Connectez-vous à la source d'installation. Les options correspondantes sont les suivantes :
   - Insérez un DVD-ROM contenant les fichiers d'installation de Windows Server 2012 et démarrez à partir du DVD-ROM.
   - Connectez un lecteur USB spécialement préparé qui héberge les fichiers d'installation de Windows Server 2012.
   - Exécutez un démarrage PXE et connectez-vous à un serveur Windows DS.

2. Dans la première page de l'Assistant Installation de Windows, sélectionnez les éléments suivants :
   - langue à installer,
   - format horaire et monétaire,
   - clavier ou méthode d'entrée.
3. Dans la deuxième page de l'Assistant Installation de Windows, cliquez sur **Installer maintenant**. Vous pouvez également utiliser cette page pour sélectionner **Réparer l'ordinateur**. Vous pouvez utiliser cette option au cas où une installation aurait été endommagée et que vous ne seriez plus à même de démarrer Windows Server 2012.
4. Dans l'Assistant Installation de Windows, dans la page **Sélectionner le système d'exploitation à installer**, choisissez une option d'installation du système d'exploitation parmi les options disponibles. L'option Installation minimale est l'option par défaut.
5. Dans la page **Termes du contrat de licence**, examinez les termes de la licence du système d'exploitation. Vous devez accepter les termes du contrat de licence avant de pouvoir procéder à l'installation.
6. Dans la page **Quel type d'installation voulez-vous effectuer ?**, les options suivantes s'offrent à vous :
   - **Mise à niveau**. Sélectionnez cette option si vous disposez d'une installation existante de Windows Server que vous souhaitez mettre à niveau vers Windows Server 2012. Vous devez lancer les mises à niveau au sein de la version précédente de Windows Server plutôt que démarrer à partir de la source d'installation.
   - **Personnalisé**. Sélectionnez cette option pour effectuer une nouvelle installation.
7. Dans la page **Où souhaitez-vous installer Windows ?**, choisissez un disque disponible sur lequel installer Windows Server 2012. Vous pouvez également choisir de partitionner et de formater à nouveau les disques dans cette page. Lorsque vous cliquez sur **Suivant**, le processus d'installation copie les fichiers et redémarre l'ordinateur plusieurs fois.
8. Dans la page **Paramètres**, fournissez un mot de passe pour le compte d'administrateur local.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Configuration post-installation de Windows Server 2012

Le processus d'installation de Windows Server 2012 implique de répondre à un nombre minimal de questions. Une fois que vous avez terminé l'installation, vous devez effectuer plusieurs étapes de configuration post-installation avant de pouvoir la déployer dans un environnement de production. Ces étapes vous permettent de préparer le serveur pour le rôle qu'il exécutera dans le réseau de votre organisation.

Cette leçon explique notamment comment effectuer diverses tâches de configuration post-installation, y compris la configuration des informations d'adressage réseau, la définition d'un nom de serveur et sa jonction au domaine, ainsi que la compréhension des options d'activation de produit.

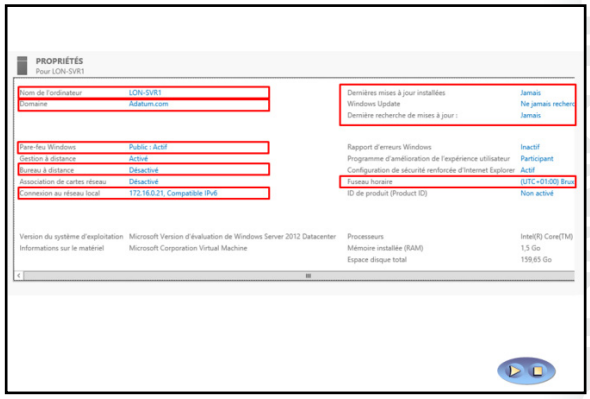
Objectifs de la leçon

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

- expliquer comment utiliser le Gestionnaire de serveur pour effectuer les tâches de configuration post-installation ;
- expliquer comment configurer les paramètres réseau du serveur ;
- expliquer comment joindre un domaine Active Directory ;
- expliquer comment effectuer une jonction de domaine hors connexion ;
- expliquer comment activer Windows Server 2012 ;
- expliquer comment configurer une installation minimale.

Vue d'ensemble de la configuration post-installation

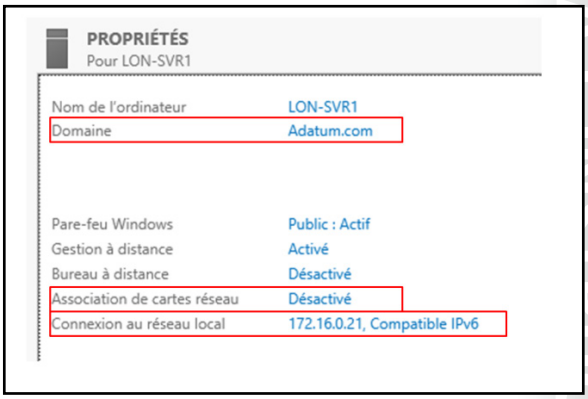
Le processus d'installation de Windows Server 2012 réduit au maximum le nombre de questions auxquelles vous devez répondre pendant l'installation. Les seules informations que vous fournissez au cours du processus d'installation correspondent au mot de passe du compte d'administrateur local par défaut. La procédure post installation implique la configuration de tous les autres paramètres dont le serveur a besoin pour pouvoir être déployé dans un environnement de production.



Vous utilisez le nœud Serveur local dans la console du Gestionnaire de serveur pour effectuer les tâches suivantes :

- configurer l'adresse IP ;
- définir le nom de l'ordinateur ;
- joindre un domaine Active Directory ;
- configurer le fuseau horaire ;
- activer les mises à jour automatiques ;
- ajouter des rôles et des fonctionnalités ;
- activer le Bureau à distance ;
- configurer les paramètres du Pare-feu Windows.

Configuration des paramètres réseau du serveur



Pour communiquer sur le réseau, un serveur a besoin d'informations correctes d'adresse IP. Une fois que vous avez terminé l'installation, vous devez définir ou vérifier la configuration des adresses IP du serveur. Par défaut, un serveur nouvellement déployé tente d'obtenir les informations d'adresse IP auprès d'un serveur DHCP. Vous pouvez afficher la configuration des adresses IP d'un serveur en cliquant sur le nœud **Serveur local** dans le Gestionnaire de serveur.

Si le serveur a une adresse IPv4 comprise dans la plage d'adressage IP privé automatique de 169.254.0.1 à 169.254.255.254, le serveur n'a pas encore été configuré avec une adresse IP provenant d'un serveur DHCP. Peut-être qu'un serveur DHCP n'a pas encore été configuré dans le réseau, ou, si un serveur DHCP est présent, il peut y avoir un problème avec l'infrastructure réseau qui empêche l'adaptateur de recevoir une adresse.

Remarque : Si vous utilisez uniquement un réseau IPv6, une adresse IPv4 comprise dans cette plage n'est pas problématique, et les informations d'adresse IPv6 sont encore configurées automatiquement.

Configuration à l'aide du Gestionnaire de serveur

Vous pouvez configurer manuellement les informations d'adresse IP pour un serveur en procédant comme suit :

1. Dans la console du Gestionnaire de serveur, cliquez sur l'adresse à côté de la carte réseau que vous souhaitez configurer.
2. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur la carte réseau pour laquelle vous souhaitez configurer une adresse, puis cliquez sur **Propriétés**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Propriétés de la carte**, cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de Protocole : Internet version 4 (TCP/IPv4)**, entrez les informations d'adresse IPv4 qui suivent, puis cliquez sur **OK** à deux reprises :
   - Adresse IP
   - Masque de sous-réseau
   - Passerelle par défaut
   - Serveur DNS préféré
   - Serveur DNS auxiliaire

Configuration des adresses IPv4 par l'intermédiaire de la ligne de commande

Vous pouvez définir manuellement les informations d'adresse IPv4 à partir d'une invite de commandes avec élévation de privilèges en utilisant la commande netsh.exe issue du contexte IPv4 (Internet Protocol version 4) ou Windows PowerShell.

Par exemple, pour configurer la carte nommée Connexion au réseau local avec l'adresse IPv4 10.10.10.10 et le masque de sous-réseau 255.255.255.0, tapez les commandes suivantes :

```
Netsh interface ipv4 set address “Connexion au réseau local” static 10.10.10.10
255.255.255.0
New-NetIPAddress –InterfaceIndex 12 –IPAddress 10.10.10.10 –PrefixLength 24
```

Vous pouvez utiliser le même contexte de la commande netsh.exe pour configurer la configuration DNS.

Par exemple, pour configurer la carte nommée Connexion au réseau local pour qu'elle utilise le serveur DNS à l'adresse IP 10.10.10.5 en tant que serveur DNS principal, tapez la commande suivante :

```
Netsh interface ipv4 set dnsservers “Connexion au réseau local” static 10.10.10.5 primary
Set-DNSClientServerAddress –InterfaceIndex 12 –ServerAddresses 10.10.10.5
```

Dans les commandes Windows PowerShell, la valeur InterfaceIndex identifie la carte que vous configurez. Pour obtenir la liste complète des cartes avec les valeurs InterfaceIndex correspondantes, exécutez l'applet de commande Get-NetIPInterface.

Association de cartes réseau

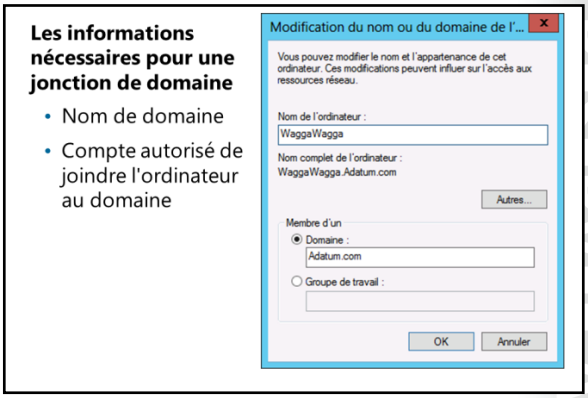
L' association de cartes réseau vous permet d'augmenter la disponibilité d'une ressource réseau. Lorsque vous configurez la fonctionnalité d'association de cartes réseau, un ordinateur utilise une adresse réseau pour plusieurs cartes. En cas de défaillance d'une des cartes, l'ordinateur est en mesure de maintenir la communication avec les autres hôtes sur le réseau qui utilisent cette adresse partagée. L'association de cartes réseau n'exige pas que les cartes réseau soient du même modèle ou utilisent le même pilote. Pour associer des cartes réseau, procédez comme suit :

1. Assurez-vous que le serveur possède plus d'une carte réseau.
2. Dans le Gestionnaire de serveur, cliquez sur le nœud **Serveur local**.
3. En regard de la fonction Association de cartes réseau, cliquez sur **Désactivé**. Ceci lancera la boîte de dialogue **Association de cartes réseau**.
4. Dans la boîte de dialogue **Association de cartes réseau**, maintenez enfoncée la touche Ctrl, puis cliquez sur chaque carte réseau que vous souhaitez ajouter à l'association.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Cliquez avec le bouton droit sur les cartes réseau sélectionnées, puis cliquez sur **Ajouter à une nouvelle équipe**.
6. Dans la boîte de dialogue **Nouvelle équipe**, spécifiez un nom pour l'équipe, puis cliquez sur **OK**.

Procédure de jonction d'un domaine



Quand vous installez Windows Server 2012, un nom aléatoire est attribué à l'ordinateur. Avant de joindre un domaine, vous devriez configurer le serveur avec le nom que vous souhaitez qu'il ait dans le domaine. Il est recommandé d'utiliser un schéma de noms cohérent lors de la conception d'un nom d'ordinateur. Les ordinateurs doivent recevoir des noms qui reflètent leur fonction et emplacement, et non pas des noms avec des liens personnels, tels que des noms d'animaux domestiques ou de personnages fictifs ou historiques. Il est globalement plus aisé de déterminer qu'un serveur nommé MEL-DNS1 est un serveur DNS situé à Melbourne, que de déterminer qu'un serveur nommé Copernic détient le rôle DNS dans le bureau de Melbourne.

Vous pouvez modifier ce nom à l'aide de la console du Gestionnaire de serveur en procédant comme suit :

1. Dans le Gestionnaire de serveur, cliquez sur le nœud **Serveur local**.
2. Dans la fenêtre Propriétés, cliquez sur le texte actif à côté de Nom de l'ordinateur. Ceci lancera la boîte de dialogue **Propriétés système**.
3. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom d'ordinateur**, cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, entrez le nouveau nom que vous souhaitez attribuer à l'ordinateur.
5. Redémarrez l'ordinateur pour implémenter le changement de nom.

Avant de joindre le domaine, veillez à terminer la procédure suivante pour vérifier que le nouveau serveur est prêt à être joint à un domaine :

- Assurez-vous que vous pouvez résoudre l'adresse IP du contrôleur de domaine et que vous pouvez contacter ce contrôleur de domaine. Utilisez le protocole PING pour effectuer un test ping du contrôleur de domaine par nom d'hôte afin d'accomplir ces deux objectifs.
- Terminez l'une des tâches suivantes :
  - Créez un compte d'ordinateur dans le domaine qui correspond au nom de l'ordinateur que vous souhaitez joindre au domaine. Ceci a souvent lieu lorsqu'un grand nombre d'ordinateurs doivent être joints automatiquement au domaine.
  - Joignez l'ordinateur au domaine en utilisant un compte de sécurité qui a le droit d'exécuter des opérations de jonction de domaine.
- Vérifiez que le compte de sécurité qui est utilisé pour l'opération de domaine existe déjà dans le domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

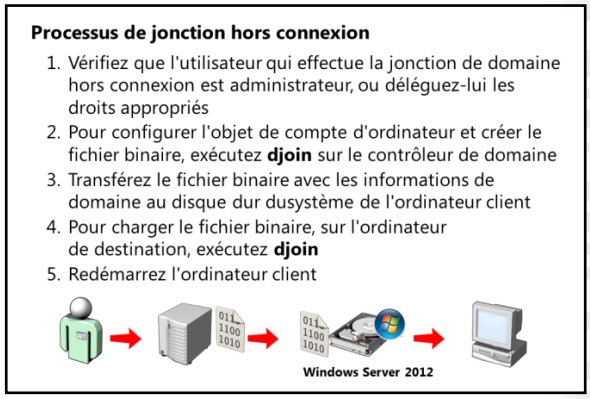
Maintenant que vous avez renommé votre serveur Windows Server 2012 et que vous avez vérifié qu'il est prêt à être joint à un domaine, vous pouvez joindre le serveur au domaine.

Pour joindre le domaine à l'aide du Gestionnaire de serveur, procédez comme suit :

1. Dans le Gestionnaire de serveur, cliquez sur le nœud Serveur local.
2. Dans la fenêtre Propriétés, à côté de Groupe de travail, cliquez sur **WORKGROUP**.
3. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom d'ordinateur**, cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, dans la zone **Membre de**, cliquez sur l'option **Domaine**. Entrez le nouveau nom du domaine, puis cliquez sur **O**.
5. Dans la boîte de dialogue **Sécurité de Windows**, entrez les informations d'identification du domaine qui vous permettent de joindre l'ordinateur au domaine.
6. Redémarrez l'ordinateur.

Exécution d'une jonction de domaine hors connexion

La jonction de domaine hors connexion est une fonctionnalité que vous pouvez utiliser pour joindre un ordinateur au domaine quand cet ordinateur n'a pas de connexion réseau active. Cette fonctionnalité peut être utile dans les situations où la connectivité est intermittente, par exemple lorsque vous déployez un serveur sur un site distant qui est connecté via une liaison montante satellite.



Utilisez l'outil en ligne de commande djoin.exe pour effectuer une jonction de domaine hors connexion. Vous pouvez effectuer une jonction de domaine hors connexion en procédant comme suit :

1. Connectez-vous au contrôleur de domaine avec un compte d'utilisateur doté des droits appropriés pour joindre d'autres ordinateurs au domaine.
2. Ouvrez une invite de commandes avec élévation de privilèges et utilisez la commande **djoin.exe** avec l'option **/provision**. Vous devez également spécifier le domaine auquel vous souhaitez joindre l'ordinateur, le nom de l'ordinateur à joindre au domaine et le nom du fichier savefile que vous allez transférer à la cible de la jonction de domaine hors connexion.

   Par exemple, pour joindre l'ordinateur Canberra au domaine adatum.com en utilisant le fichier savefile Canberra-join.txt, tapez la commande suivante :

```
djoin.exe /provision /domain adatum.com /machine canberra /savefile c:\canberra-join.txt
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Transférez le fichier savefile généré sur le nouvel ordinateur, puis exécutez la commande **djoin.exe** avec l'option **/requestODJ**.

   Par exemple, pour effectuer la jonction de domaine hors connexion, après le transfert du fichier savefile Canberra-join.txt sur l'ordinateur Canberra, vous pouvez exécuter la commande suivante à partir d'une invite de commandes avec élévation de privilèges sur Canberra :

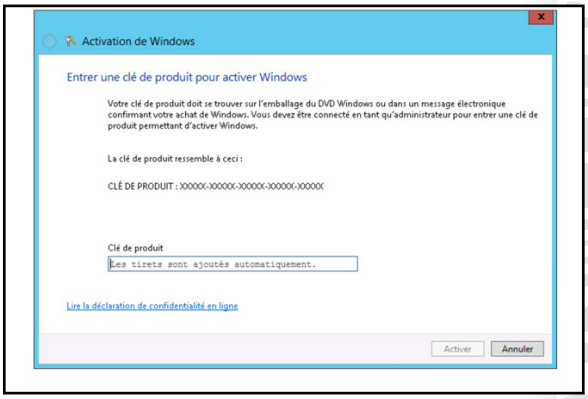
   ```
   djoin.exe /requestODJ /loadfile canberra-join.txt /windowspath %systemroot% /localos
   ```

4. Redémarrez l'ordinateur pour terminer l'opération de jonction de domaine.

   Question : Dans quelle situation préfèreriez-vous effectuer une jonction de domaine hors connexion à une jonction de domaine standard ?

Activation de Windows Server 2012

Pour vous assurer que votre organisation bénéficie de licences correctes et pour recevoir des informations préalables sur les mises à jour du produit, vous devez activer chaque copie de Windows Server 2012 que vous installez. Windows Server 2012 requiert une activation après installation. À la différence des versions précédentes du système d'exploitation Windows Server, il n'y a plus de période de grâce d'activation. Si vous n'effectuez pas l'activation, vous ne pouvez pas effectuer la personnalisation du système d'exploitation.



Pour activer Windows Server 2012, vous pouvez utiliser deux stratégies générales au choix :

- Activation manuelle. Appropriée quand vous déployez un nombre réduit de serveurs.
- Activation automatique. Appropriée quand vous déployez un nombre élevé de serveurs.

Activation manuelle

Avec l'activation manuelle, vous entrez la clé de produit et le serveur contacte Microsoft. Alternativement, un administrateur peut effectuer l'activation par téléphone ou via un site Web Clearinghouse spécial.

Vous pouvez effectuer l'activation manuelle à partir de la console du Gestionnaire de serveur en procédant comme suit :

1. Cliquez sur le nœud Serveur local.
2. Dans la fenêtre Propriétés, à côté de l'ID de produit, cliquez sur **Non activé**.
3. Dans la boîte de dialogue **Activation de Windows**, entrez la clé de produit, puis cliquez sur **Activer**.
4. Si une connexion directe ne peut pas être établie avec les serveurs d'activation Microsoft, des détails s'afficheront concernant la manière d'effectuer l'activation à l'aide d'un site Web à partir d'un périphérique doté d'une connexion Internet ou à l'aide d'un numéro de téléphone local.

Puisque les ordinateurs qui exécutent l'option d'installation minimale ne possèdent pas la console du Gestionnaire de serveur, vous pouvez également effectuer l'activation manuelle à l'aide de la commande **slmgr.vbs**. Utilisez la commande **slmgr.vbs /ipk** pour entrer la clé de produit et **slmgr.vbs /ato** pour effectuer l'activation une fois que la clé de produit a été installée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez effectuer l'activation manuelle à l'aide de la clé de produit commercialisée ou de la clé d'activation multiple. Vous pouvez utiliser une clé de produit commercialisée uniquement pour activer un seul ordinateur. Cependant, une clé d'activation multiple possède un nombre donné d'activations que vous pouvez utiliser. Une clé d'activation multiple vous permet d'activer plusieurs ordinateurs jusqu'à la limite d'activation définie.

Les clés OEM représentent un type particulier de clé d'activation. Elles sont fournies à un fabricant et permettent l'activation automatique lors de la première mise sous tension d'un ordinateur. Ce type de clé d'activation est généralement utilisé avec des ordinateurs qui exécutent des systèmes d'exploitation clients tels que Windows 7 et Windows 8. Les clés OEM sont rarement utilisées avec des ordinateurs qui exécutent des systèmes d'exploitation serveurs.

La réalisation manuelle de l'activation dans des déploiements de serveurs à grande échelle peut être lourde. Microsoft fournit une méthode permettant d'activer un grand nombre d'ordinateurs automatiquement sans avoir à entrer manuellement de clé de produit sur chaque système.

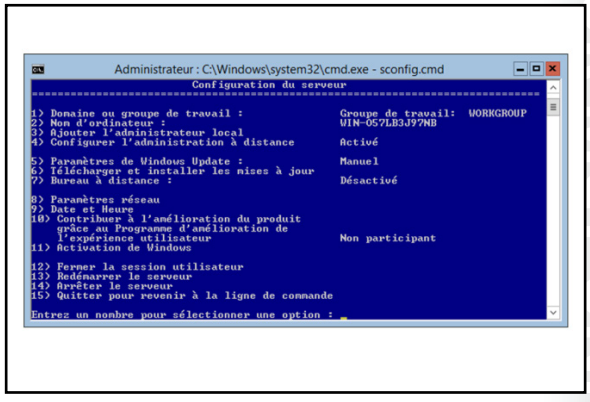
Activation automatique

Dans les versions précédentes du système d'exploitation Windows Server, vous pouviez utiliser KMS pour effectuer une activation centralisée de plusieurs clients. Le rôle serveur Services d'activation en volume dans Windows Server 2012 vous permet de gérer un serveur KMS via une nouvelle interface. Ceci simplifie le processus d'installation d'une clé KMS sur le serveur KMS. Quand vous installez les services d'activation en volume, vous pouvez également configurer une activation basée sur Active Directory. L'activation basée sur Active Directory permet l'activation automatique des ordinateurs joints à un domaine. Quand vous utilisez les services d'activation en volume, chaque ordinateur activé doit régulièrement contacter le serveur KMS pour renouveler son statut d'activation.

Vous utilisez l'outil Volume Activation Management Tool (VAMT) 3.0 en association avec les services d'activation en volume pour effectuer l'activation de plusieurs ordinateurs sur des réseaux qui ne sont pas connectés directement à Internet. Vous pouvez utiliser VAMT pour générer des rapports de licence et gérer l'activation des clients et des serveurs dans des réseaux d'entreprise.

Configuration d'une installation minimale

La procédure post-installation sur un ordinateur exécutant l'option d'installation minimale du système d'exploitation peut être intimidante pour les administrateurs qui n'ont encore jamais effectué cette tâche. Au lieu de disposer d'outils basés sur l'interface graphique utilisateur qui simplifient la procédure de configuration post-installation, les professionnels de l'informatique sont tenus d'effectuer des tâches de configuration complexes via une interface de ligne de commande.



Fort heureusement, vous pouvez effectuer la majorité des tâches de configuration post-installation à l'aide de l'outil en ligne de commande sconfig.cmd. Cet outil réduit au maximum le risque d'effectuer des erreurs de syntaxe lors de l'utilisation d'outils en ligne de commande plus compliqués.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez utiliser **sconfig.cmd** pour effectuer les tâches suivantes :

- configurer les informations de domaine et de groupe de travail ;
- configurer le nom de l'ordinateur ;
- ajouter des comptes d'administrateur local ;
- configurer WinRM ;
- activer Windows Update ;
- télécharger et installer des mises à jour ;
- activer le Bureau à distance ;
- configurer les informations d'adresse réseau ;
- régler la date et l'heure ;
- effectuer l'activation de Windows ;
- activer l'interface graphique utilisateur de Windows Server ;
- se déconnecter ;
- redémarrer le serveur ;
- arrêter le serveur.

Configurer les informations d'adresse IP

Vous pouvez configurer les informations d'adresse IP et DNS à l'aide de **sconfig.cmd** ou de **netsh.exe**. Pour configurer les informations d'adresse IP à l'aide de **sconfig.cmd**, procédez comme suit :

1. À partir d'une ligne de commande, exécutez la commande **sconfig.cmd**.
2. Choisissez l'**option 8** pour configurer les paramètres réseau.
3. Choisissez le numéro d'index de la carte réseau à laquelle vous souhaitez attribuer une adresse IP.
4. Dans la zone Paramètres de carte réseau, choisissez l'une des options suivantes :
    - Définir l'adresse de la carte réseau
    - Définir les serveurs DNS
    - Effacer les paramètres du serveur DNS
    - Retourner au menu principal

Modifier le nom du serveur

Vous pouvez modifier le nom d'un serveur en utilisant la commande **netdom** avec l'option **renamecomputer**.

Par exemple, pour renommer un ordinateur Melbourne, tapez la commande suivante :

```
Netdom renamecomputer %nom_ordinateur% /newname:Melbourne
```

Vous pouvez modifier le nom d'un serveur à l'aide de **sconfig.cmd** en procédant comme suit :

1. À partir d'une ligne de commande, exécutez la commande **sconfig.cmd**.
2. Choisissez l'**option 2** pour configurer le nouveau nom de l'ordinateur.
3. Tapez le nouveau nom de l'ordinateur et appuyez sur Entrée.

Vous devez redémarrer le serveur pour que la modification prenne effet.

Jonction à un domaine

Vous pouvez joindre un ordinateur avec installation minimale à un domaine à l'aide de la commande **netdom** avec l'option **join**.

Par exemple, pour joindre le domaine adatum.com en utilisant le compte Administrateur et être invité à entrer un mot de passe, tapez la commande suivante :

```
Netdom join %nom_ordinateur% /domain:adatum.com /UserD:Administrateur /PasswordD:*
```

Remarque : Avant de joindre le domaine, vérifiez que vous êtes en mesure d'effectuer un test ping du serveur DNS à l'aide du nom d'hôte.

Pour joindre un ordinateur avec installation minimale au domaine à l'aide de **sconfig.cmd**, procédez comme suit :

1. À partir d'une ligne de commande, exécutez la commande **sconfig.cmd**.
2. Choisissez l'**option 1** pour configurer le domaine/groupe de travail.
3. Pour choisir l'option Domaine, tapez **D** et appuyez sur Entrée.
4. Tapez le nom du domaine auquel vous voulez joindre l'ordinateur.
5. Fournissez les détails au format *domaine**nom d'utilisateur* d'un compte autorisé à joindre le domaine.
6. Tapez le mot de passe associé à ce compte.

Pour terminer l'opération de jonction de domaine, il convient de redémarrer l'ordinateur.

Ajout de rôles et de fonctionnalités

Vous pouvez ajouter et supprimer des rôles et des fonctionnalités sur un ordinateur qui exécute l'option d'installation minimale à l'aide des applets de commande Windows PowerShell **Get-WindowsFeature**, **Install-WindowsFeature** et **Remove-WindowsFeature**. Ces applets de commande sont disponibles une fois que vous avez chargé le module Windows PowerShell ServerManager.

Par exemple, vous pouvez afficher la liste des rôles et fonctionnalités qui sont installés en tapant la commande suivante :

```
Get-WindowsFeature | Where-Object {$_.InstallState -eq “Installed”}
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez également installer un rôle ou une fonctionnalité Windows en utilisant l'applet de commande **Install-WindowsFeature**. Par exemple, pour installer la fonctionnalité d'équilibrage de la charge réseau, exécutez la commande :

```
Install-WindowsFeature NLB
```

Toutes les fonctionnalités ne sont pas disponibles directement pour l'installation sur un ordinateur exécutant l'installation minimale du système d'exploitation. Vous pouvez déterminer quelles fonctionnalités ne sont pas directement disponibles pour l'installation en exécutant la commande suivante :

```
Get-WindowsFeature | Where-Object {$_.InstallState -eq “Removed”}
```

Vous pouvez ajouter un rôle ou une fonctionnalité qui n'est pas directement disponible pour l'installation en utilisant le paramètre **-Source** de l'applet de commande **Install-WindowsFeature**. Vous devez spécifier un emplacement source qui héberge une image d'installation montée incluant la version complète de Windows Server 2012. Vous pouvez monter une image d'installation à l'aide de l'outil en ligne de commande **DISM.exe**. Si vous ne spécifiez pas de chemin source lors de l'installation d'un composant qui n'est pas disponible et que le serveur dispose d'une connexion Internet, l'applet de commande **Install-WindowsFeature** tente de récupérer les fichiers sources à partir de Windows Update.

Ajouter l'interface graphique utilisateur

Vous pouvez configurer un ordinateur avec installation minimale avec l'interface graphique utilisateur en utilisant l'outil en ligne de commande **sconfig.cmd**. Pour cela, choisissez l'**option 12** dans le menu Configuration du serveur de sconfig.cmd.

Remarque : Vous pouvez ajouter ou supprimer le composant graphique du système d'exploitation Windows Server 2012 à l'aide de l'applet de commande **Install-WindowsFeature**.

Vous pouvez également utiliser l'outil en ligne de commande **dism.exe** pour ajouter et supprimer des rôles et des fonctionnalités Windows d'un déploiement avec installation minimale, même si cet outil est utilisé principalement pour la gestion des fichiers image.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 5
Présentation de Windows PowerShell

Windows PowerShell est une technologie d'interface de ligne de commande et de script basé sur les tâches, intégrée dans le système d'exploitation Windows Server 2012. Windows PowerShell simplifie l'automatisation des tâches courantes d'administration de systèmes. Windows PowerShell vous permet d'automatiser les tâches, ce qui vous laisse plus de temps pour les tâches plus complexes d'administration de systèmes.

Dans cette leçon, vous allez découvrir Windows PowerShell et pourquoi Windows PowerShell représente un composant essentiel du kit de ressources d'un administrateur de serveur.

Cette leçon explique comment utiliser les fonctionnalités de découverte intégrées de Windows PowerShell pour apprendre à utiliser des applets de commande spécifiques et rechercher les applets de commande associées. Cette leçon présente également comment tirer profit de l'environnement d'écriture de scripts intégré de Windows PowerShell (Windows PowerShell ISE) pour qu'il vous aide à créer des scripts Windows PowerShell efficaces.

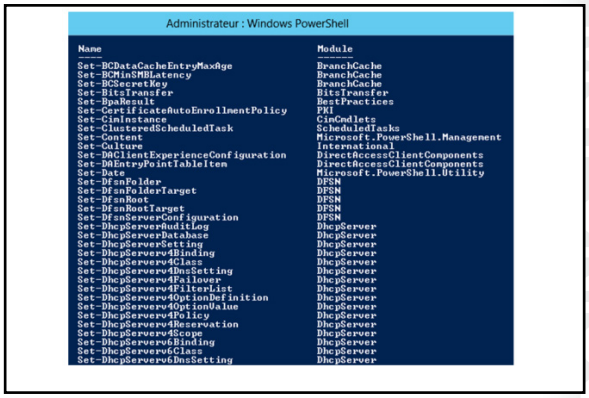
Objectifs de la leçon

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

- décrire la fonction de Windows PowerShell ;
- décrire la syntaxe des applets de commande Windows PowerShell et expliquer comment déterminer les commandes associées à une applet de commande particulière ;
- décrire les applets de commande Windows PowerShell courantes permettant de gérer les services, les processus, les rôles et les fonctionnalités ;
- décrire les fonctionnalités de Windows PowerShell ISE ;
- expliquer comment utiliser Windows PowerShell ;
- expliquer comment utiliser Windows PowerShell ISE.

Qu'est-ce que Windows PowerShell ?

Windows PowerShell est un langage de script et une interface de ligne de commande qui est conçue pour vous aider à effectuer des tâches d'administration quotidiennes. Windows PowerShell se compose d'applets de commande que vous exécutez à une invite de commandes Windows PowerShell ou que vous associez en scripts Windows PowerShell. À la différence d'autres langages de script qui ont été conçus initialement dans un autre but et ont été adaptés pour des tâches d'administration système, Windows PowerShell a été conçu avec les tâches d'administration système à l'esprit.

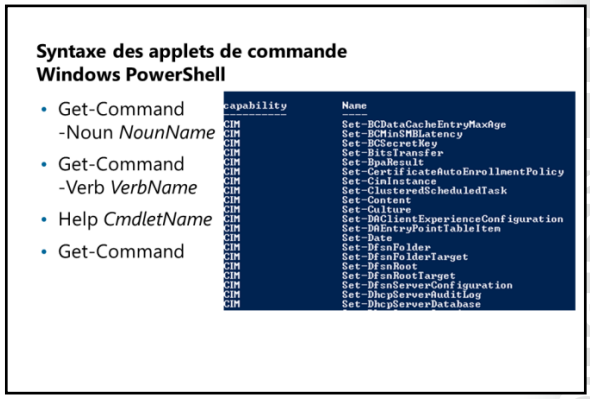


Un nombre croissant de produits Microsoft (tels qu'Exchange Server 2010) ont des interfaces graphiques qui établissent les commandes Windows PowerShell. Ces produits vous permettent de visualiser le script Windows PowerShell généré pour que vous puissiez exécuter la tâche ultérieurement sans avoir à terminer toutes les étapes dans l'interface graphique utilisateur. La capacité à automatiser les tâches complexes simplifie le travail d'un administrateur de serveur et lui permet d'économiser du temps.

Vous pouvez étendre les fonctionnalités de Windows PowerShell en ajoutant des modules. Par exemple, le module Active Directory inclut des applets de commande Windows PowerShell spécifiquement utiles pour effectuer des tâches de gestion liées à Active Directory. Le module Serveur DNS inclut des applets de commande Windows PowerShell spécifiquement utiles pour effectuer des tâches de gestion liées au serveur DNS. Windows PowerShell inclut des fonctionnalités telles que la saisie semi-automatique via la touche Tab, qui permet aux administrateurs de compléter des commandes en appuyant sur la touche Tab au lieu de taper la commande complète. Vous pouvez découvrir les fonctionnalités de toute applet de commande Windows PowerShell à l'aide de l'applet de commande **Get-Help**.

Syntaxe des applets de commande Windows PowerShell

Les applets de commande Windows PowerShell utilisent une syntaxe verbe-nom. Chaque nom possède une collection de verbes associés. Les verbes disponibles diffèrent avec chaque nom d'applet de commande.



Exemples de verbes courants d'applets de commande Windows PowerShell :

- Get
- New
- Set
- Restart
- Resume
- Stop
- Suspend
- Clear
- Limit
- Remove
- Add
- Show
- Write

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez connaître les verbes disponibles pour un nom Windows PowerShell en exécutant la commande suivante :

```
Get-Command -Noun NounName
```

Vous pouvez connaître les noms Windows PowerShell disponibles pour un verbe spécifique en exécutant la commande suivante :

```
Get-Command -Verb VerbName
```

Les paramètres Windows PowerShell commencent par un tiret. Chaque applet de commande Windows PowerShell possède son propre jeu de paramètres associé. Vous pouvez connaître les paramètres correspondant à une applet de commande Windows PowerShell particulière en exécutant la commande suivante :

```
Get-Command CmdletName
```

Vous pouvez déterminer les applets de commande Windows PowerShell disponibles en exécutant l'applet de commande **Get-Command**. Les applets de commande Windows PowerShell disponibles dépendent des modules chargés.

Applets de commande courantes pour l'administration de serveur

En tant qu'administrateur de serveur, il existe certaines applets de commande que vous êtes plus susceptibles d'utiliser. Ces applets de commande se rapportent principalement aux services, aux journaux d'événements, aux processus et au module ServerManager qui s'exécutent sur le serveur.

- Applets de commande de service
  - Utiliser le nom Service
- Applets de commande des journaux d'événements
  - Utiliser le nom Eventlog
- Applets de commande de processus
  - Utiliser le nom Process
- Module ServerManager
  - Autorise le nom WindowsFeature

Applets de commande de service

Vous pouvez utiliser les applets de commande Windows PowerShell suivantes pour gérer des services sur un ordinateur qui exécute Windows Server 2012 :

- **Get-Service**. Affiche les propriétés d'un service.
- **New-Service**. Crée un nouveau service.
- **Restart-Service**. Redémarre un service existant.
- **Resume-Service**. Reprend l'exécution d'un service interrompu.
- **Set-Service**. Configure les propriétés d'un service.
- **Start-Service**. Démarre un service arrêté.
- **Stop-Service**. Arrête un service en cours d'exécution.
- **Suspend-Service**. Interrompt un service.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Applets de commande des journaux d'événements

Vous pouvez utiliser les applets de commande Windows PowerShell suivantes pour gérer les journaux d'événements sur un ordinateur qui exécute Windows Server 2012 :

- **Get-EventLog**. Affiche les événements dans le journal d'événements spécifié.
- **Clear-EventLog**. Supprime toutes les entrées du journal d'événements spécifié.
- **Limit-EventLog**. Définit les limites d'âge et de taille des journaux d'événements.
- **New-EventLog**. Crée un nouveau journal d'événements et une nouvelle source d'événements sur un ordinateur exécutant Windows Server 2012.
- **Remove-EventLog**. Supprime un journal d'événements personnalisé et annule l'inscription de toutes les sources d'événements du journal.
- **Show-EventLog**. Montre les journaux d'événements d'un ordinateur.
- **Write-EventLog**. Vous permet d'écrire des événements dans un journal d'événements.

Applets de commande de processus

Vous pouvez utiliser les applets de commande Windows PowerShell suivantes pour gérer des processus sur un ordinateur qui exécute Windows Server 2012 :

- **Get-Process**. Fournit des informations sur un processus.
- **Start-Process**. Démarre un processus.
- **Stop-Process**. Arrête un processus.
- **Wait-Process**. Attend l'arrêt du processus avant d'accepter l'entrée.
- **Debug-Process**. Joint un débogueur à un ou plusieurs processus en cours d'exécution.

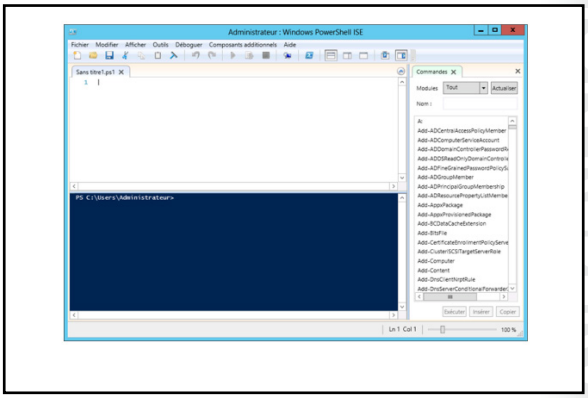
Module ServerManager

Le module ServerManager vous permet d'ajouter trois applets de commande au choix, qui sont utiles pour gérer les fonctionnalités et les rôles. Ces applets de commande sont :

- **Get-WindowsFeature**. Affiche la liste des rôles et des fonctionnalités disponibles. Affiche également si la fonctionnalité est installée et si elle est disponible. Vous pouvez installer une fonctionnalité non disponible uniquement si vous avez accès à une source d'installation.
- **Install-WindowsFeature**. Installe un rôle particulier ou une fonctionnalité particulière de Windows Server. L'applet de commande **Add-WindowsFeature** est associée par des alias à cette commande et est disponible dans les versions antérieures des systèmes d'exploitation Windows.
- **Remove-WindowsFeature**. Supprime un rôle particulier ou une fonctionnalité particulière de Windows Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que Windows PowerShell ISE ?



Windows PowerShell ISE est un environnement de script intégré qui vous fournit une assistance lorsque vous utilisez Windows PowerShell. Il fournit des fonctionnalités pour compléter les commandes et vous permet de voir toutes les commandes disponibles et les paramètres que vous pouvez utiliser avec ces commandes.

Windows PowerShell ISE simplifie le processus d'utilisation de Windows PowerShell car vous pouvez exécuter les applets de commande à partir de l'environnement d'écriture de scripts. Vous pouvez également utiliser une fenêtre de script dans Windows PowerShell ISE pour construire et enregistrer des scripts Windows PowerShell. La capacité à afficher les paramètres des applets de commande vous garantit d'être conscient des fonctionnalités complètes de chaque applet de commande et de pouvoir créer des commandes Windows PowerShell syntaxiquement correctes.

Windows PowerShell ISE fournit des applets de commande avec des codes de couleurs pour faciliter la résolution des problèmes. L'environnement d'écriture de scripts vous fournit également des outils de débogage que vous pouvez utiliser pour déboguer des scripts Windows PowerShell simples et complexes.

Vous pouvez utiliser l'environnement Windows PowerShell ISE pour afficher les applets de commande disponibles par module. Vous pouvez alors déterminer quel module Windows PowerShell vous devez charger pour accéder à une applet de commande particulière.

Démonstration : Utilisation de Windows PowerShell

Dans cette démonstration, vous allez apprendre à utiliser Windows PowerShell pour afficher les services et les processus en cours d'exécution sur un serveur.

Procédure de démonstration

Utiliser Windows PowerShell pour afficher les services et les processus en cours d'exécution sur un serveur

1. Sur LON-DC1, ouvrez une session Windows PowerShell.
2. Exécutez les commandes suivantes et appuyez sur Entrée :

```
Get-Service | where-object {$_.status -eq “Running”}
Get-Command -Noun Service
Get-Process
Get-Help Process
Get-Help –Full Start-Process
```

3. Dans la barre des tâches, cliquez avec le bouton droit sur l'icône **Windows PowerShell**, puis cliquez sur **Exécuter comme administrateur**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Utilisation de Windows PowerShell ISE

Dans cette démonstration, vous allez apprendre à terminer les tâches suivantes :

- utiliser Windows PowerShell ISE pour importer le module ServerManager ;
- afficher les applets de commande proposées dans le module ServerManager ;
- utiliser l'applet de commande **Get-WindowsFeature** à partir de Windows PowerShell ISE.

Procédure de démonstration

Utiliser Windows PowerShell ISE pour importer le module ServerManager

1. Assurez-vous d'être connecté à LON-DC1 en tant qu'Administrateur.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Windows PowerShell ISE**.
3. À l'invite de commandes, tapez **Import-Module ServerManager**.

Afficher les applets de commande proposées dans le module ServerManager

- Dans le volet Commandes, utilisez le menu déroulant **Modules** pour sélectionner le module **ServerManager**.

Utiliser l'applet de commande Get-WindowsFeature à partir de Windows PowerShell ISE

1. Cliquez sur **Get-WindowsFeature**, puis cliquez sur **Afficher les détails**.
2. Dans le champ **ComputerName**, tapez **LON-DC1**, puis cliquez sur **Exécuter**.

Atelier pratique : Déploiement et gestion de Windows Server 2012

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

Vous avez travaillé pour A. Datum pendant plusieurs années en tant que spécialiste du support technique et avez récemment accepté une promotion comme technicien responsable des serveurs.

Le service marketing a acheté une nouvelle application Web. Vous devez installer et configurer les serveurs au centre de données pour cette application. Un serveur dispose d'une interface graphique utilisateur et l'autre serveur est configuré avec une installation minimale.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- déployer Windows Server 2012 ;
- configurer l'installation minimale de Windows Server 2012 ;
- gérer les serveurs à l'aide du Gestionnaire de serveur ;
- gérer les serveurs à l'aide de Windows PowerShell.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-SVR3 22410B-LON-CORE
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 **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 1 à 3 pour **22410B-LON-CORE** et **22410B-LON-SVR3**. 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 : Déploiement de Windows Server 2012

Scénario

Le premier serveur Windows Server 2012 que vous installez pour le service marketing hébergera une instance du moteur de base de données SQL Server 2012. Vous souhaitez configurer ce serveur de sorte qu'il dispose de l'interface graphique utilisateur complète, car ceci permettra au fournisseur de l'application d'exécuter les outils de support directement sur le serveur au lieu de requérir une connexion à distance.

Le premier serveur que vous installez pour la nouvelle application marketing est pour une base de données SQL Server 2012. Ce serveur disposera de l'interface graphique utilisateur complète pour permettre au fournisseur de l'application d'exécuter les outils de support directement sur le serveur.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le serveur Windows Server 2012
2. Modifier le nom du serveur
3. Modifier la date et l'heure
4. Configurer le réseau et l'association de cartes réseau
5. Ajouter le serveur au domaine

▶ Tâche 1 : Installer le serveur Windows Server 2012

1. Dans la console du Gestionnaire Hyper-V, affichez les paramètres pour 22410B-LON-SVR3.
2. Configurez le lecteur de DVD pour utiliser le fichier image Windows Server 2012 nommé **Windows2012_RTM_FR.ISO**. Ce fichier se trouve dans **C:\Program Files\ Microsoft Learning\22410\Drives**.
3. Démarrez **22410B-LON-SVR3**. Dans l'Assistant Installation de Windows, dans la page **Windows Server 2012**, vérifiez les paramètres suivants, cliquez sur **Suivant**, puis sur **Installer maintenant**.
   - Langue à installer : **Français (France)**
   - Format horaire et monétaire : **Français (France)**
   - Clavier ou méthode d'entrée : **Français**
4. Cliquez pour installer le système d'exploitation **Version d'évaluation de Windows Server 2012 Datacenter (serveur avec une interface graphique utilisateur)**.
5. Acceptez le termes du contrat de licence, puis cliquez sur **Personnalisé : installer uniquement Windows (avancé)**.
6. Installez Windows Server 2012 sur **Lecteur 0**.

Remarque: Selon la vitesse du matériel, l'installation prendra approximativement 20 minutes. L'ordinateur virtuel redémarrera plusieurs fois au cours de ce processus.

7. Entrez le mot de passe **Pa$$w0rd** dans les deux zones **Mot de passe** et **Entrer de nouveau le mot de passe**, puis cliquez sur **Terminer** pour terminer l'installation.

▶ Tâche 2 : Modifier le nom du serveur

1. Connectez-vous à LON-SVR3 en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le **Gestionnaire de serveur**, dans le nœud Serveur local, cliquez sur le nom généré aléatoirement à côté de **Nom d'ordinateur**.
3. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom d'ordinateur**, cliquez sur **Modifier**.
4. Dans la zone **Nom d'ordinateur**, tapez **LON-SVR3**, puis cliquez sur **OK**.
5. Cliquez de nouveau sur **OK**, puis sur **Fermer**.
6. Redémarrez l'ordinateur.

▶ Tâche 3 : Modifier la date et l'heure

1. Connectez-vous au serveur LON-SVR3 en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur l'affichage de l'heure, puis cliquez sur **Modifier les paramètres de la date et de l'heure**.
3. Cliquez sur **Changer de fuseau horaire** et définissez le fuseau horaire sur votre fuseau horaire actuel.
4. Cliquez sur **Changer la date et l'heure**, et vérifiez que la date et heure qui s'affichent dans la boîte de dialogue **Réglage de la date et de l'heure** correspondent à la date et l'heure dans la classe.
5. Fermez la boîte de dialogue **Date et Heure**.

▶ Tâche 4 : Configurer le réseau et l'association de cartes réseau

1. Sur LON-SVR3, cliquez sur **Serveur local**, puis à côté d'**Association de cartes réseau**, cliquez sur **Désactivé**.
2. Maintenez enfoncée la touche Ctrl puis, dans la zone **CARTES ET INTERFACES**, cliquez sur **Connexion au réseau local** et sur **Connexion au réseau local 2**.
3. Cliquez avec le bouton droit sur les cartes réseau sélectionnées, puis cliquez sur **Ajouter à une nouvelle équipe**.
4. Entrez **LON-SVR3** dans la zone **Nom de l'équipe**, cliquez sur **OK**, puis fermez la boîte de dialogue **Association de cartes réseau**. Actualisez le volet de la console.
5. À côté de LON-SVR3, cliquez sur **Adresse IPv4 attribuée par DHCP, Compatible IPv6**.
6. Dans la boîte de dialogue **Connexions réseau**, cliquez avec le bouton droit sur **LON-SVR3**, puis cliquez sur **Propriétés**.
7. Cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis cliquez sur **Propriétés**.
8. Entrez les informations d'adresse suivantes, puis cliquez sur **OK** :
   - Adresse IP : **172.16.0.101**
   - Masque de sous-réseau : **255.255.0.0**
   - Passerelle par défaut : **172.16.0.1**
   - Serveur DNS préféré : **172.16.0.10**
9. Fermez toutes les boîtes de dialogue.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À [illegible] INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Ajouter le serveur au domaine

1. Sur LON-SVR3, dans la console du Gestionnaire de serveur, cliquez sur **Serveur local**.
2. À côté de Groupe de travail, cliquez sur **WORKGROUP**.
3. Dans l'onglet **Nom d'ordinateur**, cliquez sur **Modifier**.
4. Cliquez sur l'option **Domaine** et dans la zone **Domaine**, entrez **adatum.com**.
5. Entrez les détails de compte suivants :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
6. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, cliquez sur **OK**.
7. Redémarrez l'ordinateur pour appliquer les modifications.
8. Dans la boîte de dialogue **Propriétés système**, cliquez sur **Fermer**.
9. Après le redémarrage de LON-SVR3, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir déployé Windows Server 2012 sur LON-SVR3. Vous devez également avoir configuré LON-SVR3, notamment le changement de nom, la date et l'heure, la mise en réseau et l'association de cartes réseau.

Exercice 2 : Configuration de l'installation minimale de Windows Server 2012

Scénario

La couche Web de l'application marketing est une application .NET. Pour réduire au maximum l'encombrement du système d'exploitation et réduire la nécessité d'appliquer des mises à jour logicielles, vous avez choisi d'héberger le composant IIS sur un ordinateur qui exécute l'option d'installation minimale du système d'exploitation Windows Server 2012.

Pour permettre cela, vous devez configurer un ordinateur qui exécute Windows Server 2012 avec l'option d'installation minimale.

Les tâches principales de cet exercice sont les suivantes :

1. Définir le nom de l'ordinateur
2. Changer la date et l'heure de l'ordinateur
3. Configurer le réseau
4. Ajouter le serveur au domaine

▶ Tâche 1 : Définir le nom de l'ordinateur

1. Connectez-vous à LON-CORE en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-CORE, tapez **sconfig.cmd**.
3. Cliquez sur l'option **2** pour sélectionner **Nom d'ordinateur**.
4. Définissez le nom de l'ordinateur sur **LON-CORE**.

5. Dans la boîte de dialogue **Redémarrer**, cliquez sur **Oui** pour redémarrer l'ordinateur.
6. Une fois que l'ordinateur a redémarré, connectez-vous à LON-CORE avec le compte **Administrateur** et le mot de passe **Pa$$w0rd**.
7. À l'invite de commandes, tapez **hostname** et appuyez sur Entrée pour vérifier le nom de l'ordinateur.

▶ Tâche 2 : Changer la date et l'heure de l'ordinateur

1. Vérifiez que vous êtes connecté au serveur LON-CORE en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez **sconfig.cmd**.
3. Pour sélectionner **Date et Heure**, tapez **9**.
4. Cliquez sur **Changer de fuseau horaire**, puis définissez le fuseau horaire sur celui que votre classe utilise.
5. Dans la boîte de dialogue **Date et Heure**, cliquez sur **Changer la date et l'heure** et vérifiez que la date et heure correspondent à la date et l'heure là où vous vous trouvez.
6. Quittez sconfig.cmd.

▶ Tâche 3 : Configurer le réseau

1. Vérifiez que vous êtes connecté au serveur LON-CORE à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez **sconfig.cmd**, puis appuyez sur Entrée.
3. Pour configurer les **paramètres réseau**, tapez **8**.
4. Tapez le numéro de la carte réseau que vous souhaitez configurer.
5. Tapez **1** pour définir l'adresse de la carte réseau.
6. Cliquez sur **configuration d'adresse IP statique**, puis entrez l'adresse **172.16.0.111**.
7. À l'invite **Entrer un masque de sous-réseau**, tapez **255.255.0.0**.
8. À l'invite **Entrez la passerelle par défaut**, tapez **172.16.0.1**.
9. Tapez **2** pour configurer l'adresse du serveur DNS.
10. Définissez le serveur DNS préféré sur **172.16.0.10**.
11. Ne configurez pas d'adresse de serveur DNS auxiliaire.
12. Quittez sconfig.cmd.
13. Vérifiez la connexion réseau à lon-dc1.adatum.com à l'aide de l'outil PING.

▶ Tâche 4 : Ajouter le serveur au domaine

1. Vérifiez que vous êtes connecté au serveur LON-CORE à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez **sconfig.cmd** et appuyez sur Entrée.
3. Tapez **1** pour configurer **Domaine ou groupe de travail**.
4. Tapez **D** pour joindre un domaine.
5. À l'invite **Nom du domaine à joindre**, tapez **adatum.com**.
6. À l'invite **Spécifier un domaine\utilisateur autorisé**, tapez **ADATUM\Administrateur**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. À l'invite **Tapez le mot de passe associé à l'utilisateur du domaine**, tapez **Pa$$w0rd**.
8. À l'invite, cliquez sur **Non**.
9. Redémarrez le serveur.
10. Connectez-vous au serveur LON-CORE à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir configuré un déploiement avec installation minimale de Windows Server 2012 et vérifié le nom du serveur.

Exercice 3 : Gestion des serveurs

Scénario

Après le déploiement des serveurs LON-SVR3 et LON-CORE pour héberger l'application marketing, vous devez installer des rôles et des fonctionnalités de serveur appropriés pour prendre en charge l'application. En gardant cela en tête, vous installerez la fonctionnalité Sauvegarde Windows Server sur LON-SVR3 et LON-CORE. Vous installerez le rôle Serveur Web sur LON-CORE.

Vous devez également configurer le service de publication World Wide Web sur LON-CORE.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un groupe de serveurs
2. Déployer des fonctionnalités et des rôles sur les deux serveurs
3. Examiner les services et modifier un paramètre de service

▶ Tâche 1 : Créer un groupe de serveurs

1. Connectez-vous à LON-DC1 à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans la console du Gestionnaire de serveur, cliquez sur **Tableau de bord**, puis cliquez sur **Créer un groupe de serveurs**.
3. Cliquez sur l'onglet **Active Directory**, puis sur **Rechercher maintenant**.
4. Dans la zone **Nom du groupe de serveurs**, tapez **LAB-1**.
5. Ajoutez **LON-CORE** et **LON-SVR3** au groupe de serveurs.
6. Cliquez sur **LAB-1**. Sélectionnez **LON-CORE** et **LON-SVR3**.
7. Faites défiler la fenêtre vers le bas et, sous la section **PERFORMANCES**, sélectionnez **LON-CORE** et **LON-SVR3**.
8. Cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Démarrer les compteurs de performances**.

▶ Tâche 2 : Déployer des fonctionnalités et des rôles sur les deux serveurs

1. Dans le Gestionnaire de serveur, sur LON-DC1, cliquez sur le groupe de serveurs **LAB-1**, cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**, sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
3. Vérifiez que **LON-CORE.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
4. Sélectionnez le rôle serveur **Rôle Web Server (IIS)**.

5. Sélectionnez la fonctionnalité **Sauvegarde Windows Server**.
6. Ajoutez le service de rôle **Authentification Windows**, puis cliquez sur **Suivant**.
7. Activez la case à cocher **Redémarrer automatiquement le serveur de destination, si nécessaire**, puis cliquez sur **Installer**.
8. Cliquez sur **Fermer**.
9. Cliquez avec le bouton droit sur **LON-SVR3**, cliquez sur **Ajouter des rôles et des fonctionnalités**, puis cliquez sur **Suivant**.
10. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
11. Vérifiez que **LON-SVR3.Adatum.com** est sélectionné, puis cliquez sur **Suivant** à deux reprises.
12. Cliquez sur **Sauvegarde Windows Server**, puis sur **Suivant**.
13. Activez la case à cocher **Redémarrer automatiquement le serveur de destination, si nécessaire**, cliquez sur **Installer**, puis sur **Fermer**.
14. Dans le Gestionnaire de serveur, cliquez sur le nœud **IIS** et vérifiez que LON-CORE est répertorié.

▶ Tâche 3 : Examiner les services et modifier un paramètre de service

1. Connectez-vous à LON-CORE à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans la fenêtre d'invite de commandes, tapez la commande suivante :

```
netsh.exe firewall set service remoteadmin enable ALL
```

3. Connectez-vous à LON-DC1 avec le compte **ADATUM\Administrateur**.
4. Dans le **Gestionnaire de serveur**, cliquez sur **LAB-1**, cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Gestion de l'ordinateur**.
5. Développez **Services et applications**, puis cliquez sur **Services**.
6. Vérifiez que le **Type de démarrage** du **Service de publication World Wide Web** est défini sur **Automatique**.
7. Vérifiez que le service est configuré pour utiliser le **compte système local**.
8. Configurez les paramètres de récupération de service suivants :
   - Première défaillance : **Redémarrer le service**
   - Deuxième défaillance : **Redémarrer le service**
   - Défaillances suivantes : **Redémarrer l'ordinateur**.
   - Réinitialiser le compteur de défaillances après : **1** jours
   - Réinitialiser le service après : **1** minute
9. Configurez l'option Redémarrer l'ordinateur sur **2 minutes**, puis fermez la boîte de dialogue **Propriétés de services**.
10. Fermez la console Gestion de l'ordinateur.

Résultats : À la fin de cet exercice, vous devez avoir créé un groupe de serveurs, déployé des rôles et des fonctionnalités, et configuré les propriétés d'un service.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Utilisation de Windows PowerShell pour gérer les serveurs

Scénario

Le fournisseur de l'application marketing a indiqué qu'il peut fournir quelques scripts Windows PowerShell pour configurer le serveur Web qui héberge l'application. Vous devez vérifier que l'administration à distance est opérationnelle avant d'exécuter les scripts.

Les tâches principales de cet exercice sont les suivantes :

1. Utiliser Windows PowerShell® pour se connecter à distance aux serveurs et afficher les informations
2. Utiliser Windows PowerShell pour installer à distance de nouvelles fonctionnalités
3. Pour préparer le module suivant

▶ Tâche 1 : Utiliser Windows PowerShell® pour se connecter à distance aux serveurs et afficher les informations

1. Connectez-vous à LON-DC1 à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur le groupe de serveurs **LAB-1**.
3. Cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Windows PowerShell**.
4. Tapez **Import-Module ServerManager**.
5. Tapez **Get-WindowsFeature** et examinez les rôles et les fonctionnalités.
6. Utilisez la commande suivante pour examiner les services en cours d'exécution sur LON-CORE :

```
Get-service | where-object {$_.status -eq “Running”}
```

7. Tapez **get-process** pour afficher la liste des processus sur LON-CORE.
8. Examinez les adresses IP attribuées au serveur en tapant la commande suivante :

```
Get-NetIPAddress | Format-table
```

9. Examinez les 10 éléments les plus récents dans le journal de sécurité en tapant la commande suivante :

```
Get-EventLog Security -Newest 10
```

10. Fermez Windows PowerShell.

▶ Tâche 2 : Utiliser Windows PowerShell pour installer à distance de nouvelles fonctionnalités

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. Tapez **import-module ServerManager**.
3. Tapez la commande suivante pour vérifier que la fonctionnalité **Visionneuse XPS** n'a pas été installée sur LON-SVR3 :

```
Get-WindowsFeature -ComputerName LON-SVR3
```

4. Pour déployer la fonctionnalité Visionneuse XPS sur LON-SVR3, tapez la commande suivante et appuyez sur Entrée :

```
Install-WindowsFeature XPS-Viewer -ComputerName LON-SVR3
```

5. Tapez la commande suivante pour vérifier que la fonctionnalité Visionneuse XPS est a présent déployée sur LON-SVR3 :

```
Get-WindowsFeature -ComputerName LON-SVR3
```

6. Dans la console du **Gestionnaire de serveur**, dans le menu déroulant **Outils**, cliquez sur **Windows PowerShell ISE**.

7. Dans le volet de script Untitled1.ps1, tapez ce qui suit :

```
Import-Module ServerManager
Install-WindowsFeature WINS -ComputerName LON-SVR3
Install-WindowsFeature WINS -ComputerName LON-CORE
```

8. Enregistrez le script sous le nom InstallWins.ps1 dans un nouveau dossier nommé **Scripts**.

9. Appuyez sur la touche F5 pour exécuter InstallWins.ps1.

Résultats : À la fin de cet exercice, vous devez avoir utilisé Windows PowerShell pour effectuer une installation à distance des fonctionnalités sur plusieurs serveurs.

▶ 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, basculez vers la console du Gestionnaire Hyper-V.

2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-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 22410B-LON-CORE et 22410B-LON-SVR3.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quel est l'avantage d'utiliser Windows PowerShell pour automatiser des tâches courantes ?

Question : Quels sont les avantages d'un déploiement avec installation minimale par rapport au déploiement complet de l'interface graphique utilisateur ?

Question : Quel outil permet de déterminer quelles applets de commande sont contenues dans un module Windows PowerShell ?

Question : Quel rôle pouvez-vous utiliser pour gérer KMS ?

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Échec des connexions WinRM.	
Applets de commande Windows PowerShell non disponibles.	
Impossible d'installer les fonctionnalités d'interface graphique utilisateur sur les déploiements avec installation minimale.	
Impossible de redémarrer un ordinateur exécutant une installation minimale.	
Impossible de joindre le domaine.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2

Présentation des services de domaine Active Directory

Table des matières :

Vue d'ensemble du module	**2-1**
Leçon 1 : Vue d'ensemble d'AD DS	**2-2**
Leçon 2 : Vue d'ensemble des contrôleurs de domaine	**2-9**
Leçon 3 : Installation d'un contrôleur de domaine	**2-16**
Atelier pratique : Installation de contrôleurs de domaine	**2-22**
Contrôle des acquis et éléments à retenir	**2-26**

Vue d'ensemble du module

Les services de domaine Active Directory® (AD DS) et les services associés constituent une base pour les réseaux d'entreprise qui exécutent des systèmes d'exploitation Windows®. La base de données AD DS est le magasin central de tous les objets de domaine, tels que les comptes d'utilisateur, les comptes d'ordinateur et les groupes. AD DS fournit un répertoire hiérarchisé interrogeable et une méthode pour l'application de la configuration et des paramètres de sécurité aux objets de l'entreprise. Ce module traite de la structure d'AD DS et de ses divers composants, tels qu'une forêt, un domaine et des unités d'organisation (OU).

Le processus d'installation d'AD DS sur un serveur est affiné et amélioré avec Windows Server® 2012. Ce module examine certains des choix proposés avec Windows Server 2012 pour l'installation d'AD DS sur un serveur.

Objectifs

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

- décrire la structure d'AD DS ;
- décrire la fonction des contrôleurs de domaine ;
- expliquer comment installer un contrôleur de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble d'AD DS

La base de données AD DS stocke des informations sur l'identité de l'utilisateur, les ordinateurs, les groupes, les services et les ressources. Les contrôleurs de domaine AD DS hébergent également le service qui authentifie les comptes d'utilisateur et d'ordinateur quand ils se connectent au domaine. Comme AD DS stocke des informations sur tous les objets inclus dans le domaine et que tous les utilisateurs et ordinateurs doivent se connecter aux contrôleurs de domaine AD DS lorsqu'ils se connectent au réseau, AD DS constitue le principal moyen vous permettant de configurer et gérer les comptes d'utilisateur et d'ordinateur dans votre réseau.

Cette leçon couvre les composants logiques de base qui composent un déploiement d'AD DS.

Objectifs de la leçon

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

- décrire les composants AD DS ;
- décrire les domaines AD DS ;
- décrire les unités d'organisation et leur fonction ;
- décrire les forêts et arborescences AD DS et expliquer comment vous pouvez les déployer dans un réseau ;
- expliquer comment un schéma AD DS fournit un ensemble de règles qui gèrent les objets et les attributs qui sont stockés dans la base de données AD DS.

Vue d'ensemble d'AD DS

AD DS se compose à la fois de composants physiques et logiques. Vous devez comprendre la manière dont les composants d'AD DS fonctionnent ensemble de façon à pouvoir gérer efficacement votre réseau et contrôler à quelles ressources vos utilisateurs peuvent accéder. En outre, vous pouvez utiliser de nombreuses autres options AD DS, y compris l'installation et la configuration du logiciel et des mises à jour, la gestion de l'infrastructure de sécurité, l'activation de l'accès à distance et de DirectAccess, ainsi que la gestion des certificats.

AD DS se compose à la fois de composants physiques et logiques

Composants physiques	Composants logiques
• Magasin de données	• Partitions
• Contrôleurs de domaine	• Schéma
• Serveur de catalogue global	• Domaines
• Contrôleur de domaine en lecture seule	• Arborescences de domaines
	• Forêts
	• Sites
	• Unités d'organisation

Une des fonctionnalités d'AD DS est la fonctionnalité Stratégie de groupe qui permet de configurer des stratégies centralisées que vous pouvez utiliser pour gérer la plupart des objets dans AD DS. La compréhension des divers composants AD DS est importante pour pouvoir utiliser correctement la fonctionnalité Stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Composants physiques

Les informations relatives à AD DS sont stockées dans un fichier unique sur le disque dur de chaque contrôleur de domaine. Le tableau suivant répertorie quelques composants physiques et où ils sont stockés.

Composant physique	Description
Contrôleurs de domaine	Contiennent des copies de la base de données AD DS.
Magasin de données	Fichier sur chaque contrôleur de domaine qui stocke les informations AD DS.
Serveurs de catalogue global	Hébergent le *catalogue global*, lequel est une copie partielle, en lecture seule, de tous les objets dans la forêt. Un catalogue global accélère les recherches d'objets susceptibles d'être stockés sur des contrôleurs de domaine d'un domaine différent de la forêt.
Contrôleurs de domaine en lecture seule (RODC)	Installation spéciale d'AD DS dans une forme en lecture seule. Elle est souvent utilisée dans les filiales où la sécurité et l'assistance informatique sont souvent moins avancées que dans les centres d'affaires principaux.

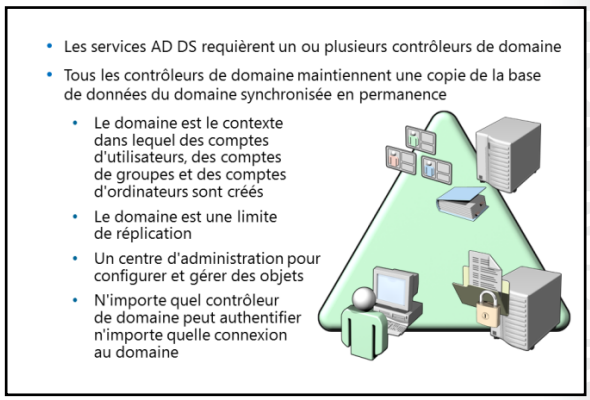
Composants logiques

Les composants logiques AD DS sont des structures utilisées pour l'implémentation d'une conception Active Directory appropriée à une organisation. Le tableau suivant décrit certains types de structures logiques qu'une base de données Active Directory peut contenir.

Composant logique	Description
Partition	Une section de la base de données AD DS. Bien que la base de données soit un seul fichier nommé NTDS.DIT, elle est affichée, gérée et répliquée comme si elle était composée de sections ou d'instances distinctes. Celles-ci sont appelées *partitions* ou encore *contextes d'appellation*.
Schéma	Définit la liste des types d'objets et d'attributs que tous les objets dans AD DS peuvent avoir.
Domaine	Limite d'administration logique pour les utilisateurs et les ordinateurs.
Arborescence de domaine	Collection des domaines qui partagent un domaine racine commun et un espace de noms DNS (Domain Name System).
Forêt	Collection des domaines qui partagent un service AD DS commun.
Site	Collection d'utilisateurs, de groupes et d'ordinateurs, tels qu'ils sont définis par leurs emplacements physiques. Les sites sont utiles dans des tâches d'administration de la planification telles que la réplication des modifications apportées à la base de données AD DS.
Unité d'organisation	Les unités d'organisation (OU) sont des conteneurs dans AD DS qui fournissent une infrastructure pour déléguer des droits d'administration et pour lier des objets de stratégie de groupe (GPO).

Documentation supplémentaire : Pour plus d'informations sur les domaines et les forêts, voir Domains and Forests Technical Reference (Guide de référence technique Domaines et forêts) à l'adresse http://go.microsoft.com/fwlink/?LinkId=104447.

Que sont les domaines AD DS ?



Un domaine AD DS est un regroupement logique d'objets utilisateur, ordinateur et groupe, effectué pour des raisons de gestion et de sécurité. Tous ces objets sont enregistrés dans la base de données AD DS et une copie de cette base de donnée est enregistrée sur chaque contrôleur de domaine dans le domaine AD DS.

Plusieurs types d'objets peuvent être stockés dans la base de données AD DS, y compris des comptes d'utilisateur. Les comptes d'utilisateur fournissent un mécanisme que vous pouvez utiliser pour authentifier puis autoriser des utilisateurs à accéder à des ressources sur le réseau. Chaque ordinateur joint à un domaine doit avoir un compte dans AD DS. Ceci permet aux administrateurs de domaine d'utiliser les stratégies qui sont définies dans le domaine pour gérer les ordinateurs. Le domaine stocke également des groupes, qui représentent le mécanisme de regroupement d'objets pour des raisons administratives ou de sécurité (par exemple, des comptes d'utilisateur et des comptes d'ordinateur).

Le domaine AD DS est également une limite de réplication. Quand des changements sont apportés à n'importe quel objet du domaine, ces changements sont répliqués automatiquement sur tous les autres contrôleurs de domaine du domaine.

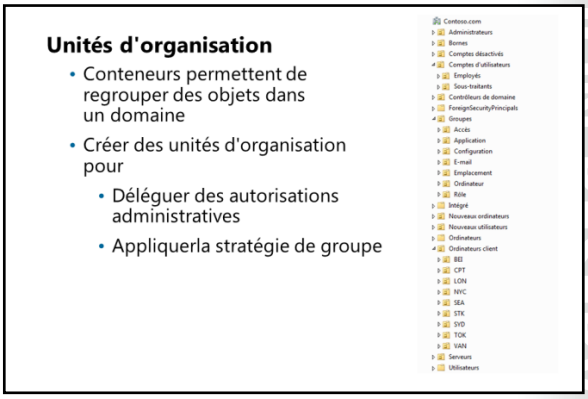
Un domaine AD DS est un centre d'administration. Il contient un compte Administrateur et un groupe Administrateurs du domaine ; chacun a le contrôle total sur chaque objet du domaine. À moins qu'ils ne soient dans le domaine racine de la forêt, leur plage de contrôle est toutefois limitée au domaine. Des règles de mot de passe et de compte sont gérées au niveau du domaine par défaut. Le domaine AD DS fournit un centre d'authentification. Tous les comptes d'utilisateur et comptes d'ordinateur dans le domaine sont stockés dans la base de données du domaine, et les utilisateurs et les ordinateurs doivent se connecter à un contrôleur de domaine pour s'authentifier.

Un domaine individuel peut contenir plus de 1 million d'objets, si bien que la plupart des organisations ont besoin de déployer un seul domaine. Les organisations qui ont des structures administratives décentralisées, ou qui sont distribuées entre plusieurs emplacements, peuvent implémenter plusieurs domaines dans la même forêt.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les unités d'organisation ?



Une *unité d'organisation* (OU) est un objet conteneur dans un domaine, que vous pouvez utiliser pour consolider des utilisateurs, des groupes, des ordinateurs et d'autres objets. Vous pouvez créer des unités d'organisation pour deux raisons :

- Pour configurer des objets contenus dans l'unité d'organisation. Vous pouvez attribuer des objets GPO à l'unité d'organisation, et les paramètres s'appliquent à tous les objets dans l'unité d'organisation. Les objets GPO sont des stratégies que les administrateurs créent pour gérer et configurer les comptes d'ordinateur et d'utilisateur. La manière la plus courante de déployer ces stratégies est de les lier aux unités d'organisation.
- Pour déléguer le contrôle administratif d'objets présents dans l'unité d'organisation. Vous pouvez attribuer des autorisations de gestion sur une unité d'organisation, déléguant de ce fait le contrôle de cette unité d'organisation à un utilisateur ou à un groupe dans AD DS autre que l'administrateur.

Vous pouvez utiliser des unités d'organisation pour représenter les structures hiérarchiques et logiques au sein de votre organisation. Par exemple, vous pouvez créer des unités d'organisation qui représentent les différents services de votre organisation, les régions géographiques de votre organisation ou une combinaison des services et des régions géographiques. Vous pouvez utiliser des unités d'organisation pour gérer la configuration et l'utilisation des comptes d'utilisateur, de groupe et d'ordinateur en fonction de votre modèle d'organisation.

Chaque domaine AD DS contient un ensemble standard de conteneurs et d'unités d'organisation qui sont créés quand vous installez AD DS, dont notamment :

- Conteneur du domaine. Sert de conteneur racine à la hiérarchie.
- Conteneur Builtin. Stocke plusieurs groupes par défaut.
- Conteneur Utilisateurs. Emplacement par défaut pour les nouveaux comptes d'utilisateur et groupes que vous créez dans le domaine. Le conteneur Utilisateurs contient également les comptes d'administrateur et d'invité du domaine, et quelques groupes par défaut.
- Conteneur Ordinateurs. Emplacement par défaut pour les nouveaux comptes d'ordinateur que vous créez dans le domaine.
- Unité d'organisation Contrôleurs de domaine. Emplacement par défaut des comptes d'ordinateur pour les comptes d'ordinateur du contrôleur de domaine. Il s'agit de la seule unité d'organisation présente dans une nouvelle installation d'AD DS.

Remarque : Aucun des conteneurs par défaut dans le domaine AD DS ne peut avoir d'objets GPO liés à lui, à l'exception de l'unité d'organisation Contrôleurs de domaine par défaut et du domaine lui-même. Tous les autres conteneurs sont de simples dossiers. Pour lier des objets GPO afin d'appliquer des configurations et des restrictions, créez une hiérarchie des unités d'organisation, puis liez-leur les objets GPO.

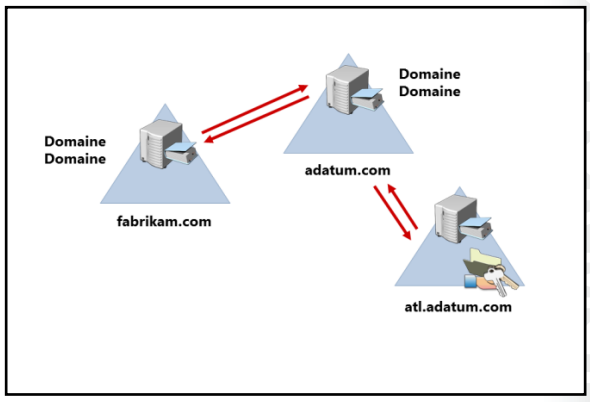
Conception d'une hiérarchie

La conception d'une hiérarchie d'unités d'organisation est dictée par les besoins administratifs de l'organisation. Cette conception peut reposer sur des classifications géographiques, fonctionnelles, de ressources ou d'utilisateurs. Quel que soit l'ordre, la hiérarchie doit permettre d'administrer les ressources AD DS d'une façon aussi souple et efficace que possible. Par exemple, si tous les ordinateurs utilisés par les administrateurs informatiques doivent être configurés d'une certaine façon, vous pouvez regrouper tous les ordinateurs dans une unité d'organisation, puis attribuer un objet GPO pour les gérer. Pour simplifier l'administration, vous pouvez également créer des unités d'organisation dans d'autres unités d'organisation.

Par exemple, votre organisation peut disposer de plusieurs bureaux, et chaque bureau peut avoir un ensemble d'administrateurs chargés de gérer les comptes d'utilisateur et d'ordinateur du bureau. De plus, chaque bureau peut avoir des services différents avec des exigences différentes de configuration des ordinateurs. Dans ce cas, vous pouvez créer une unité d'organisation pour ce bureau permettant de déléguer l'administration, puis créer une unité d'organisation de service dans l'unité d'organisation Bureau pour attribuer les configurations des postes de travail.

Bien qu'il n'y ait aucune limite technique au nombre de niveaux dans votre structure d'unité d'organisation, afin de faciliter la gestion, limitez votre structure d'unité d'organisation à une profondeur maximale de 10 niveaux. La plupart des organisations utilisent cinq niveaux ou moins pour simplifier l'administration. Notez que les applications prenant en charge Active Directory peuvent avoir des restrictions quant à la profondeur des unités d'organisation dans la hiérarchie. Ces applications peuvent également avoir des restrictions sur le nombre de caractères pouvant être utilisés dans le nom unique, qui constitue le chemin d'accès LDAP (Lightweight Directory Access Protocol) complet de l'objet dans le répertoire.

Qu'est-ce qu'une forêt AD DS ?



Une *forêt* est une collection d'une ou plusieurs arborescences de domaines. Une *forêt* est une collection d'un ou de plusieurs domaines.
Le premier domaine qui est créé dans la forêt est appelé le *domaine racine de la forêt.* Le *domaine racine de la forêt* contient quelques objets qui n'existent pas dans d'autres domaines de la forêt. Par exemple, le domaine racine de la forêt contient deux rôles de contrôleur de domaine spéciaux, le contrôleur de schéma et le maître d'opérations des noms de domaine. En outre, le groupe Administrateurs de l'entreprise et le groupe Administrateurs du schéma existent seulement dans le domaine racine de la forêt. Le groupe Administrateurs de l'entreprise a le contrôle total sur chaque domaine de la forêt.

La forêt AD DS est une limite de sécurité. Ceci signifie que, par défaut, aucun utilisateur provenant de l'extérieur de la forêt ne peut accéder à une ressource située à l'intérieur de la forêt. Cela signifie également que des administrateurs provenant de l'extérieur de la forêt n'ont aucun accès d'administration à l'intérieur de la forêt. Une des raisons principales pour lesquelles une organisation peut déployer plusieurs forêts est qu'elle doit isoler les autorisations administratives entre ses différentes parties.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

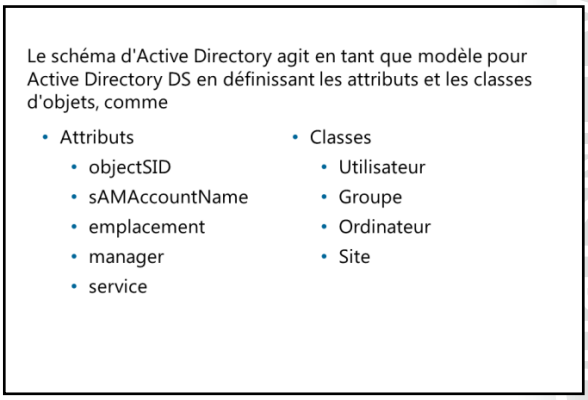
La forêt AD DS est également la limite de réplication pour les partitions de configuration et de schéma dans la base de données AD DS. Ceci signifie que tous les contrôleurs de domaine de la forêt doivent partager le même schéma. Une deuxième raison pour laquelle une organisation peut déployer plusieurs forêts est qu'elle doit déployer des schémas incompatibles dans deux de ses parties.

La forêt AD DS est également la limite de réplication du catalogue global. Ceci facilite la plupart des formulaires de collaboration entre les utilisateurs de différents domaines. Par exemple, tous les destinataires Microsoft® Exchange Server 2010 sont répertoriés dans le catalogue global, ce qui facilite l'envoi de courrier électronique aux utilisateurs de la forêt, même aux utilisateurs figurant dans des domaines différents.

Par défaut, tous les domaines d'une forêt approuvent automatiquement les autres domaines de la forêt. Ceci facilite l'activation de l'accès à des ressources telles que des partages de fichiers et des sites Web pour tous les utilisateurs dans une forêt, indépendamment du domaine dans lequel le compte d'utilisateur est situé.

Qu'est-ce que le schéma AD DS ?

Le *schéma AD DS* est le composant AD DS qui définit tous les types d'objet et attributs qu'AD DS utilise pour stocker des données. Il est parfois désigné en tant que modèle pour AD DS.



AD DS stocke et récupère les informations d'une grande variété d'applications et de services. Le service AD DS normalise la manière dont les données sont stockées dans l'annuaire AD DS afin qu'il puisse stocker et répliquer des données à partir de ces diverses sources. En normalisant la manière dont les données sont stockées, AD DS peut récupérer, mettre à jour et répliquer des données, tout en vérifiant que l'intégrité des données est maintenue.

AD DS utilise des objets comme unités de stockage. Tous les types d'objet sont définis dans le schéma. Chaque fois que l'annuaire traite des données, il interroge le schéma pour obtenir une définition d'objet appropriée. Selon la définition de l'objet dans le schéma, l'annuaire crée l'objet et stocke les données.

Les définitions d'objet contrôlent les types de données que les objets peuvent stocker et la syntaxe des données. En utilisant ces informations, le schéma garantit que tous les objets sont conformes à leurs définitions standard. En conséquence, le service AD DS peut stocker, récupérer et valider les données qu'il gère, indépendamment de l'application constituant la source originale des données. Seules des données ayant une définition d'objet existante dans le schéma peuvent être stockées dans l'annuaire. Si un nouveau type de données doit être stocké, une nouvelle définition d'objet pour ces données doit d'abord être créée dans le schéma.

Dans AD DS, le schéma définit les éléments suivants :

- les objets qui sont utilisés pour stocker des données dans l'annuaire ;
- les règles qui définissent quels types d'objet vous pouvez créer, quels attributs doivent être définis (obligatoire) quand vous créez l'objet et quels attributs sont facultatifs ;
- la structure et le contenu de l'annuaire lui-même.

Vous pouvez utiliser un compte qui est un membre des administrateurs de schéma pour modifier les composants de schéma sous forme de graphique. Les exemples des objets qui sont définis dans le schéma comprennent l'utilisateur, l'ordinateur, le groupe et le site. Parmi les nombreux attributs sont compris les suivants : **location**, **accountExpires**, **buildingName**, **company**, **manager** et **displayName**.

Le contrôleur de schéma est l'un des contrôleurs de domaine des opérations à maître unique dans AD DS. Puisque c'est un maître unique, vous devez apporter des modifications au schéma en ciblant le contrôleur de domaine qui détient le rôle des opérations du contrôleur de schéma.

Le schéma est répliqué sur tous les contrôleurs de domaine de la forêt. Tout changement qui est apporté au schéma est répliqué sur chaque contrôleur de domaine de la forêt à partir du titulaire du rôle du maître d'opérations de schéma, en général le premier contrôleur de domaine de la forêt.

Puisque le schéma dicte la manière dont les informations sont stockées et puisque toute modification apportée au schéma affecte chaque contrôleur de domaine, les modifications apportées au schéma doivent être réalisées seulement si cela est nécessaire. Avant d'apporter des modifications, vous devez examiner les modifications via un processus bien contrôlé, puis les implémenter seulement après avoir réalisé l'essai pour vérifier que les modifications ne compromettront pas le reste de la forêt ni aucune application qui utilise AD DS.

Bien que vous ne puissiez pas apporter de modification au schéma directement, quelques applications apportent des modifications au schéma pour prendre en charge des fonctionnalités supplémentaires. Par exemple, quand vous installez Exchange Server 2010 dans votre forêt AD DS, le programme d'installation étend le schéma pour prendre en charge de nouveaux types d'objet et attributs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Vue d'ensemble des contrôleurs de domaine

Puisque les contrôleurs de domaine authentifient tous les utilisateurs et ordinateurs dans le domaine, le déploiement des contrôleurs de domaine est essentiel au fonctionnement correct du réseau.

Cette leçon porte sur les contrôleurs de domaine, le processus de connexion et l'importance du serveur DNS dans ce processus. En outre, cette leçon présente la fonction du catalogue global.

Tous les contrôleurs de domaine sont essentiellement les mêmes, à deux exceptions près. Les contrôleurs de domaine en lecture seule contiennent une copie en lecture seule de la base de données AD DS, alors que les autres contrôleurs de domaine ont une copie en lecture-écriture. Il existe également certaines opérations qui peuvent être exécutées uniquement sur des contrôleurs de domaine spécifiques appelés *maîtres d'opérations*, lesquels sont présentés à la fin de cette leçon.

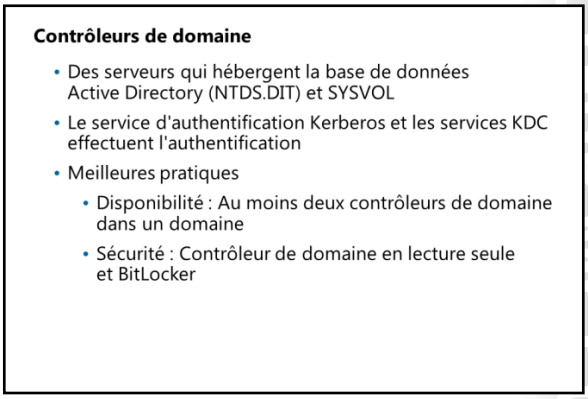
Objectifs de la leçon

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

- décrire la fonction des contrôleurs de domaine ;
- définir la fonction du catalogue global ;
- décrire le processus d'ouverture de session AD DS et l'importance des enregistrements DNS et SRV dans le processus d'ouverture de session ;
- décrire les fonctionnalités des enregistrements SRV ;
- expliquer les fonctions des maîtres d'opérations.

Qu'est-ce qu'un contrôleur de domaine ?

Un *contrôleur de domaine* est un serveur configuré pour stocker une copie de la base de données d'annuaire AD DS (NTDS.DIT) et une copie du dossier SYSVOL. Tous les contrôleurs de domaine, à l'exception des contrôleurs de domaine en lecture seule, stockent une copie en lecture/écriture de NTDS.DIT et du dossier SYSVOL. NTDS.DIT est la base de données elle-même et le dossier SYSVOL contient tous les paramètres de modèle des objets GPO.



Il est possible d'initier des modifications de la base de données AD DS sur n'importe quel contrôleur de domaine d'un domaine, à l'exception des contrôleurs de domaine en lecture seule. Le service de réplication AD DS synchronise alors les modifications et les mises à jour de la base de données AD DS sur tous les autres contrôleurs de domaine du domaine. Les dossiers SYSVOL sont répliqués par le service de réplication de fichiers (FRS) ou par la réplication DFS (Distributed File System) plus récente.

Les contrôleurs de domaine hébergent plusieurs autres services liés à Active Directory, y compris le service d'authentification Kerberos, qui est utilisé par les comptes d'utilisateur et d'ordinateur pour l'authentification des connexions, et le centre de distribution de clés (KDC). Le *centre de distribution de clés* est le service qui émet le ticket TGT (Ticket-Granting Ticket) pour un compte qui se connecte au domaine AD DS. Vous pouvez éventuellement configurer des contrôleurs de domaine pour qu'ils hébergent une copie du catalogue global Active Directory.

Un domaine AD DS doit toujours avoir un minimum de deux contrôleurs de domaine. De cette façon, si l'un des contrôleurs de domaine connaît une défaillance, une instance de secours permet de garantir la continuité des services de domaine AD DS. Quand vous décidez d'ajouter plus de deux contrôleurs de domaine, considérez la taille de votre organisation et les exigences en matière de performances.

Remarque : Deux contrôleurs de domaine doivent être considérés comme un minimum absolu.

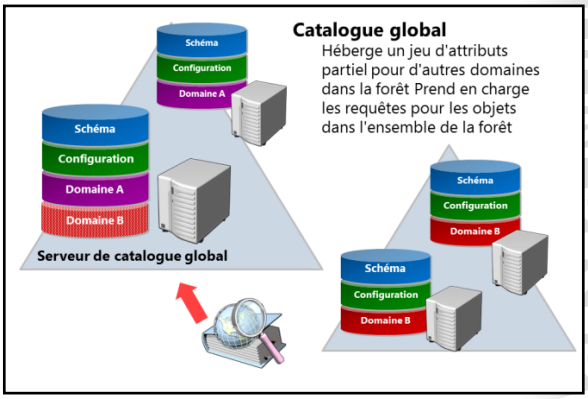
Lorsque vous déployez un contrôleur de domaine dans une filiale où la sécurité physique n'est pas optimale, certaines mesures supplémentaires peuvent être utilisées pour réduire l'impact d'une brèche de sécurité. Une option consiste à déployer un contrôleur de domaine en lecture seule.

Le contrôleur de domaine en lecture seule contient une copie en lecture seule de la base de données AD DS et, par défaut, il ne met en cache aucun mot de passe d'utilisateur. Vous pouvez configurer le contrôleur de domaine en lecture seule pour mettre en cache les mots de passe pour les utilisateurs dans la filiale. Si un contrôleur de domaine en lecture seule est compromis, la perte d'informations potentielle est nettement inférieure à ce qu'elle serait avec un contrôleur de domaine en lecture-écriture complet. Une autre option consiste à utiliser le chiffrement de lecteur Windows BitLocker® pour chiffrer le disque dur du contrôleur de domaine. Si le disque dur est volé, le chiffrement BitLocker garantit une très faible éventualité qu'un utilisateur malveillant parvienne à obtenir des informations utiles du disque dur.

Remarque : BitLocker est un système de chiffrement de lecteur disponible pour les systèmes d'exploitation Windows Server®, ainsi que pour certaines versions clientes du système d'exploitation Windows. BitLocker chiffre de manière sécurisée le système d'exploitation entier de sorte que l'ordinateur ne puisse pas démarrer sans qu'il lui soit fourni une clé privée et (éventuellement) qu'il réussisse un contrôle d'intégrité. Un disque reste chiffré même si vous le transférez sur un autre ordinateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que le catalogue global ?



Dans un même domaine, la base de données AD DS contient toutes les informations sur chaque objet présent dans ce domaine. Ces informations ne sont pas répliquées en dehors du domaine. Par exemple, une requête pour un objet dans AD DS est dirigée vers l'un des contrôleurs de domaine pour ce domaine. Si la forêt contient plusieurs domaines, cette requête ne fournit aucun résultat pour des objets figurant dans un autre domaine. Pour permettre une recherche sur plusieurs domaines, vous pouvez configurer un ou plusieurs contrôleurs de domaine pour stocker une copie du catalogue global. Le *catalogue global* est une base de données distribuée qui contient une représentation pouvant faire l'objet d'une recherche de tous les objets issus de tous les domaines d'une forêt de plusieurs domaines. Par défaut, le seul serveur de catalogue global qui est créé est le premier contrôleur de domaine dans le domaine racine de la forêt.

Le catalogue global ne contient pas tous les attributs pour chaque objet. Au lieu de cela, le catalogue global conserve le sous-ensemble des attributs qui sont le plus susceptibles d'être utiles dans les recherches inter-domaines. Ces attributs peuvent inclure **firstname**, **displayname** et **location**. Il existe de nombreuses raisons pour lesquelles vous pouvez effectuer une recherche dans un catalogue global plutôt que sur un contrôleur de domaine qui n'est pas un catalogue global. Par exemple, quand un serveur Exchange reçoit un courrier électronique entrant, il doit rechercher le compte du destinataire afin de pouvoir décider comment router le message. En interrogeant automatiquement un catalogue global, le serveur Exchange peut localiser le destinataire dans un environnement à plusieurs domaines. Lorsqu'un utilisateur se connecte à son compte Active Directory, le contrôleur de domaine qui effectue l'authentification doit entrer en contact avec un catalogue global pour vérifier l'appartenance aux groupes universels avant d'authentifier l'utilisateur.

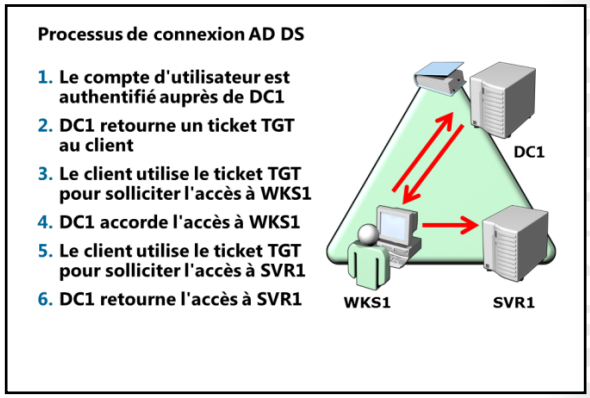
Dans un domaine unique, tous les contrôleurs de domaine doivent être configurés comme détenteurs du catalogue global. Toutefois, dans un environnement à plusieurs domaines, le maître d'infrastructure ne doit pas être un serveur de catalogue global. Quels contrôleurs de domaine sont configurés pour détenir une copie du catalogue global dépend du trafic de réplication et de la bande passante réseau. De nombreuses organisations choisissent de configurer chaque contrôleur de domaine comme serveur de catalogue global.

Question : Un contrôleur de domaine doit-il être un catalogue global ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Processus de connexion AD DS

Lorsque vous ouvrez une session AD DS, votre système examine le service DNS pour trouver des enregistrements de ressource de service (SRV) permettant de localiser le contrôleur de domaine approprié le plus proche. Les *enregistrements SRV* sont des enregistrements qui spécifient des informations sur les services disponibles et qui sont enregistrés dans DNS par tous les contrôleurs de domaine. À l'aide des recherches DNS, les clients peuvent localiser un contrôleur de domaine approprié pour traiter leurs demandes d'ouverture de session.



Si l'ouverture de session a réussi, l'autorité de sécurité locale (LSA) crée un jeton d'accès pour l'utilisateur, qui contient les identificateurs de sécurité (SID) pour l'utilisateur et tous les groupes dont l'utilisateur est membre. Le jeton fournit les informations d'identification d'accès pour tout processus initié par l'utilisateur. Par exemple, après avoir ouvert une session AD DS, un utilisateur exécute Microsoft Office Word et tente d'ouvrir un fichier. Office Word utilise les informations d'identification figurant dans le jeton d'accès de l'utilisateur pour vérifier le niveau des autorisations de l'utilisateur pour ce fichier.

Remarque : Un SID est un numéro unique présentant la forme suivante : S-1-5-21-4130086281-3752200129-271587809-500, où :

- les quatre premiers blocs de lettres et de chiffres (S-1-5-21) représentent le type d'identificateur ;
- les trois blocs de chiffres suivants (4130086281-3752200129-271587809) correspondent au numéro de la base de données où le compte est stocké (habituellement le domaine AD DS) ;
- la dernière section (500) est l'identificateur relatif (RID), lequel correspond à la partie de l'identificateur SID qui identifie de manière unique ce compte dans la base de données.

Chaque compte d'utilisateur et d'ordinateur et chaque groupe que vous créez ont un SID unique. Ils diffèrent les uns des autres uniquement en vertu de identificateur RID unique. Vous pouvez constater que cet identificateur SID particulier est le SID du compte administrateur, car il se termine par un identificateur RID égal à 500.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sites

Les sites sont utilisés par un système client quand il doit entrer en contact avec un contrôleur de domaine. Il commence par rechercher des enregistrements SRV dans DNS. Le système client essaie ensuite de se connecter à un contrôleur de domaine situé dans le même site avant d'essayer ailleurs.

Les administrateurs peuvent définir des sites dans AD DS. Les sites s'alignent habituellement sur les parties du réseau qui disposent d'une connectivité et d'une bande passante satisfaisantes. Par exemple, si une filiale est connectée au centre de données principal par une liaison WAN peu fiable, il est préférable de définir le centre de données et la filiale en tant que sites distincts dans AD DS.

Les enregistrements SRV sont inscrits dans DNS par le service Net Logon qui s'exécute sur chaque contrôleur de domaine. Si les enregistrements SRV ne sont pas entrés correctement dans DNS, vous pouvez imposer au contrôleur de domaine de réinscrire ces enregistrements en redémarrant le service Net Logon sur ce contrôleur de domaine. Ce processus réinscrit uniquement les enregistrements SRV. Si vous souhaitez réinscrire les informations sur les enregistrements d'hôte (A) dans DNS, vous devez exécuter **ipconfig /registerdns** dans une invite de commandes, comme vous le feriez pour tout autre ordinateur.

Bien que le processus d'ouverture de session apparaisse à l'utilisateur comme un événement unique, il comporte en fait deux parties :

- L'utilisateur fournit des informations d'identification, habituellement un nom de compte d'utilisateur et un mot de passe, qui sont ensuite vérifiées dans la base de données AD DS. Si le nom du compte d'utilisateur et le mot de passe correspondent aux informations stockées dans la base de données AD DS, l'utilisateur devient un utilisateur authentifié et un ticket TGT lui est remis par le contrôleur de domaine. À ce stade, l'utilisateur n'a encore accès à aucune ressource dans le réseau.
- Un processus secondaire en arrière-plan soumet le ticket TGT au contrôleur de domaine et demande l'accès à l'ordinateur local. Le contrôleur de domaine remet un ticket de service à l'utilisateur, lequel est alors en mesure d'interagir avec l'ordinateur local. À ce stade du processus, l'utilisateur est authentifié auprès d'AD DS et connecté à l'ordinateur local.

Quand un utilisateur essaie ultérieurement de se connecter à un autre ordinateur du réseau, le processus secondaire est exécuté de nouveau et le ticket TGT est soumis au contrôleur de domaine le plus proche. Lorsque le contrôleur de domaine retourne un ticket de service, l'utilisateur peut accéder à l'ordinateur sur le réseau, lequel génère un événement de connexion à cet ordinateur.

Remarque : Un ordinateur joint à un domaine ouvre également une session AD DS lorsqu'il démarre, ce qui est souvent négligé. Vous ne voyez pas la transaction quand l'ordinateur utilise le nom de son compte d'ordinateur et un mot de passe pour ouvrir une session AD DS. Une fois authentifié, l'ordinateur devient membre du groupe Utilisateurs authentifiés. Bien que le processus de connexion à un ordinateur n'ait aucune confirmation visuelle sous forme d'interface graphique utilisateur, des événements consignés enregistrent cette activité. En outre, si l'audit est activé, des événements supplémentaires sont visualisables dans le journal de sécurité de l'Observateur d'événements.

Démonstration : Affichage des enregistrements SRV dans DNS

Cette démonstration vous montre comment afficher les divers types d'enregistrements SRV que les contrôleurs de domaine inscrivent dans DNS. Ces enregistrements sont cruciaux pour l'opérabilité d'AD DS, parce qu'ils permettent de rechercher des contrôleurs de domaine pour les ouvertures de sessions, les changements de mot de passe et la modification des objets GPO. Les enregistrements SRV sont également utilisés par les contrôleurs de domaine pour rechercher des partenaires de réplication.

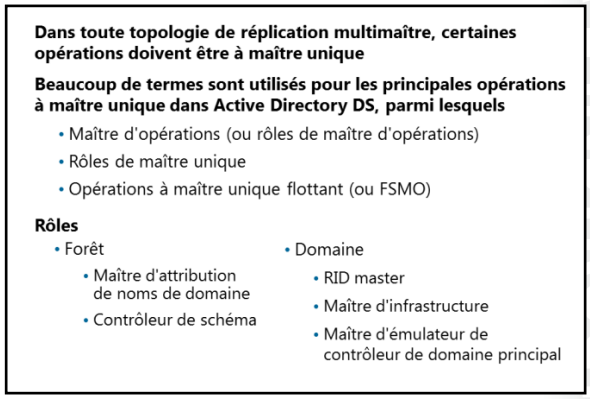
Procédure de démonstration

Afficher les enregistrements SRV à l'aide du Gestionnaire DNS

1. Ouvrez la fenêtre Gestionnaire DNS et explorez les domaines DNS avec trait de soulignement.
2. Consultez les enregistrements SRV inscrits par les contrôleurs de domaine. Ces enregistrements fournissent des chemin d'accès de substitution pour que les clients puissent les découvrir.

Que sont les maîtres d'opérations ?

Bien que tous les contrôleurs de domaine soient essentiellement égaux, certaines tâches peuvent être effectuées uniquement en ciblant un contrôleur de domaine particulier. Par exemple, si vous devez ajouter un domaine supplémentaire à la forêt, vous devez être en mesure de vous connecter au maître d'opérations des noms de domaine. Les contrôleurs de domaine dotés de ces rôles sont :



- les maîtres d'opérations ;
- les rôles de maître unique ;
- les opérations à maître unique flottant (FSMO).

Ces rôles sont distribués comme suit :

- Chaque forêt possède un contrôleur de schéma et un maître d'opérations des noms de domaine.
- Chaque domaine AD DS possède un maître RID, un maître d'infrastructure et un émulateur de contrôleur de domaine principal (PDC).

Maîtres d'opérations de forêt

Les rôles suivants sont les rôles de maître unique présents dans une forêt :

- *Maître d'attribution de noms de domaine*. Il s'agit du contrôleur de domaine qui doit être contacté lorsque vous ajoutez ou supprimez un domaine, ou lorsque vous apportez des modifications de nom à des domaines.
- *Contrôleur de schéma*. Il s'agit du contrôleur de domaine sur lequel toutes les modifications de schéma sont effectuées. Pour effectuer des modifications, vous pouvez en général vous connecter au contrôleur de schéma en tant que membre des groupes Administrateurs du schéma et Administrateurs de l'entreprise. Un utilisateur qui est un membre de ces deux groupes et qui dispose des autorisations appropriées peut également modifier le schéma à l'aide d'un script.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Maîtres d'opérations de domaine

Les rôles suivants sont les rôles de maître unique présents dans un domaine :

- *Maître RID*. Chaque fois qu'un objet est créé dans AD DS, le contrôleur de domaine sur lequel l'objet est créé attribue à l'objet un numéro d'identification unique appelé identificateur SID. Pour garantir que deux contrôleurs de domaine ne peuvent pas attribuer le même SID à deux objets différents, le maître RID alloue des blocs de RID à chaque contrôleur de domaine dans le domaine.
- *Maître d'infrastructure*. Ce rôle est responsable de la conservation des références d'objets inter-domaines, par exemple lorsqu'un groupe dans un domaine contient un membre issu d'un autre domaine. Dans cette situation, le maître d'infrastructure est responsable du maintien de l'intégrité de cette référence. Par exemple, lorsque vous regardez l'onglet de sécurité d'un objet, le système recherche les SID qui sont répertoriés et les traduit en noms. Dans une forêt à plusieurs domaines, le maître d'infrastructure recherche les SID dans les autres domaines.

  Le rôle d'infrastructure ne doit pas résider sur un serveur de catalogue global. Une exception à cette règle est faite lorsque vous suivez les meilleures pratiques et configurez chaque contrôleur de domaine comme catalogue global. Dans ce cas, le rôle d'infrastructure est désactivé parce que chaque contrôleur de domaine connaît chaque objet dans la forêt.
- *Maître d'émulateur de contrôleur de domaine principal* Le contrôleur de domaine qui détient le rôle d'émulateur de contrôleur de domaine principal (émulateur PDC) représente la source de temps pour le domaine. Les contrôleurs de domaine qui détiennent le rôle d'émulateur PDC dans chaque domaine d'une forêt synchronisent leur temps avec le contrôleur de domaine qui a le rôle d'émulateur PDC dans le domaine racine de la forêt. Vous définissez l'émulateur PDC dans le domaine racine de la forêt pour synchroniser son horloge avec une source de temps atomique externe.

  L'émulateur PDC est également le contrôleur de domaine qui reçoit les changements de mot de passe urgents. Si le mot de passe d'un utilisateur est modifié, ces informations sont envoyées immédiatement au contrôleur de domaine détenant le rôle d'émulateur PDC. Ceci signifie que si l'utilisateur essaie ultérieurement de se connecter et qu'il est authentifié par un contrôleur de domaine dans un emplacement différent qui n'a pas encore reçu une mise à jour concernant le nouveau mot de passe, le contrôleur de domaine dans l'emplacement où l'utilisateur essaie de se connecter contacte le contrôleur de domaine détenant le rôle d'émulateur PDC et vérifie les modifications récentes.

  L'émulateur PDC est également utilisé lors de la modification d'objets GPO. Lorsqu'un objet GPO autre qu'un objet GPO local est ouvert pour être modifié, la copie qui est modifiée est celle qui est stockée sur l'émulateur PDC.

Remarque : Le catalogue global n'est pas l'un des rôles de maître d'opérations.

Question : Pourquoi configurer un contrôleur de domaine comme serveur de catalogue global ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Installation d'un contrôleur de domaine

Parfois, vous devez installer des contrôleurs de domaine supplémentaires sur votre système d'exploitation Windows Server 2012. Cela peut être dû au fait que les contrôleurs de domaine existants sont surchargés et que vous avez besoin de ressources supplémentaires. Vous envisagez peut-être d'installer un nouveau bureau distant, ce qui vous oblige à déployer un ou plusieurs contrôleurs de domaine. Vous installez peut-être également un environnement de test ou un site auxiliaire. La méthode d'installation à utiliser varie selon les circonstances.

Cette leçon dévoile plusieurs manières d'installer des contrôleurs de domaine supplémentaires. Elle montre également comment utiliser le Gestionnaire de serveur pour installer AD DS sur un ordinateur local et sur un serveur distant. Cette leçon présente également l'installation d'AD DS sur une installation minimale et sur un ordinateur utilisant une capture instantanée de la base de données AD DS qui est stockée sur un média amovible. Enfin, elle décrit le processus de mise à niveau d'un contrôleur de domaine d'un système d'exploitation Windows antérieur vers Windows Server 2012.

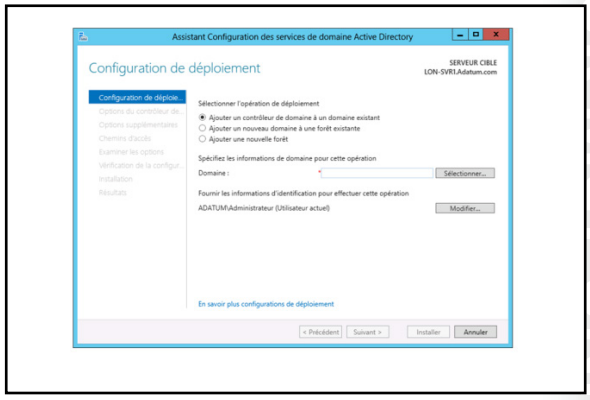
Objectifs de la leçon

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

- expliquer comment installer un contrôleur de domaine à l'aide de l'interface utilisateur graphique ;
- expliquer comment installer un contrôleur de domaine sur une installation minimale de Windows Server 2012 ;
- expliquer comment mettre à niveau un contrôleur de domaine en utilisant l'installation à partir du support ;
- expliquer comment installer un contrôleur de domaine en utilisant l'installation à partir du support.

Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Avant Windows Server 2012, il était courant d'utiliser l'outil dcpromo.exe pour installer des contrôleurs de domaine. Si vous tentez d'exécuter dcpromo.exe sur un serveur Windows Server 2012, vous recevrez le message d'erreur suivant : « L'Assistant Installation des services de domaine Active Directory a été déplacé dans le Gestionnaire de serveur. Pour plus d'informations, voir http://go.microsoft.com/fwlink/?LinkId=220921 ».



Remarque : L'outil dcpromo.exe est un outil que vous exécutez sur un serveur pour faire de ce dernier un contrôleur de domaine AD DS. Jusqu'à Windows Server 2012, dcpromo.exe était la méthode recommandée pour installer AD DS et il s'exécutait habituellement en mode GUI. Dans Windows Server 2012, cet outil est remplacé par le Gestionnaire de serveur. Dcpromo.exe est encore disponible, mais il peut être utilisé uniquement pour des installations sans assistance à partir de l'interface de ligne de commande.

Quand vous exécutez le Gestionnaire de serveur, vous pouvez choisir si l'opération est exécutée sur l'ordinateur local, sur un ordinateur distant ou par des membres d'un pool de serveurs. Ensuite, vous ajoutez le rôle AD DS. À la fin du processus d'installation initial, les binaires AD DS sont installés, mais AD DS n'est pas encore configuré sur ce serveur. Un message à cet effet s'affiche dans le Gestionnaire de serveur.

Vous pouvez sélectionner le lien pour **Promouvoir ce serveur en contrôleur de domaine** et l'Assistant Configuration des services de domaine Active Directory s'exécute. Vous pouvez alors fournir les informations répertoriées dans le tableau suivant au sujet de la structure proposée.

Informations requises	Description
Ajouter un contrôleur de domaine à un domaine existant	Décidez s'il convient d'ajouter un contrôleur de domaine supplémentaire à un domaine.
Ajouter un nouveau domaine dans une forêt existante	Créez un nouveau domaine dans la forêt.
Ajouter une nouvelle forêt	Créez une nouvelle forêt.
Spécifier les informations de domaine pour cette opération	Fournissez des informations sur le domaine existant auquel le nouveau contrôleur de domaine se connectera.
Fournir les informations d'identification pour effectuer cette opération	Entrez le nom d'un compte d'utilisateur doté des droits d'effectuer cette opération.

Certaines informations supplémentaires dont vous devez disposer avant d'exécuter la promotion de contrôleur de domaine sont répertoriées dans le tableau suivant.

Informations requises	Description
Nom DNS pour le domaine AD DS	Par exemple, adatum.com
Nom NetBIOS pour le domaine AD DS	Par exemple, adatum
Si la nouvelle forêt doit prendre en charge des contrôleurs de domaine exécutant des versions antérieures des systèmes d'exploitation Windows (affecte le choix du niveau fonctionnel)	Par exemple, si vous envisagez de déployer des contrôleurs de domaine Windows Server 2008 R2, vous devez sélectionner le niveau fonctionnel de la forêt et du domaine Windows Server 2008 R2.
Si ce contrôleur de domaine sera également un serveur DNS	Votre DNS doit fonctionner correctement pour prendre en charge AD DS.
Emplacement pour stocker les fichiers de base de données, tels que NTDS.DIT, edb.log et edb.chk.	Par défaut, ces fichiers seront stockés dans C:\Windows\NTDS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'Assistant Configuration des services de domaine Active Directory comporte plusieurs pages différentes qui vous permettent d'entrer des éléments prérequis tels que le nom de domaine NetBIOS, la configuration DNS, si ce contrôleur de domaine doit être un serveur de catalogue global, ainsi que le mot de passe du mode de restauration des services d'annuaire. Enfin, vous devez effectuer un redémarrage pour compléter l'installation.

Remarque : Si vous devez restaurer la base de données AD DS à partir d'une sauvegarde, redémarrez le contrôleur de domaine dans le mode de restauration des services d'annuaire.

Lorsque le contrôleur de domaine démarre, il n'exécute pas les services AD DS. Au lieu de cela, il s'exécute en tant que serveur membre dans le domaine. Pour se connecter à ce serveur en l'absence d'AD DS, connectez-vous en utilisant le mot de passe du mode de récupération des services d'annuaire.

Installation d'un contrôleur de domaine sur une installation minimale de Windows Server 2012

La configuration d'un serveur Windows Server 2012 qui exécute une installation minimale en tant que contrôleur de domaine est plus difficile car vous ne pouvez pas exécuter l'Assistant Configuration des services de domaine Active Directory sur le serveur. Pour installer les binaires AD DS sur le serveur, vous pouvez utiliser le Gestionnaire de serveur pour vous connecter à distance au serveur exécutant l'installation minimale. Vous pouvez également utiliser la commande Windows PowerShell **Install-Windowsfeature -name AD-Domain-Services** pour installer les binaires.

Utilisez la commande **dcpromo /unattend:"D:\answerfile.txt"** pour exécuter l'installation sans assistance. Voici un exemple de texte à partir du fichier de réponses

```
[DCINSTALL]
UserName=<Compte d'administrateur dans le domaine du nouveau contrôleur de domaine>
UserDomain=<Nom du domaine du nouveau contrôleur de domaine>
Password=<Mot de passe du compte UserName>
SiteName=<Nom du site AD DS dans lequel se trouve ce contrôleur de domaine résidera> Ce site doit être créé à l'avance dans le composant logiciel enfichable Dssites.msc.
ReplicaOrNewDomain=réplica
ReplicaDomainDNSName=<Nom de domaine complet du domaine dans lequel vous souhaitez ajouter un contrôleur de domaine supplémentaire>
DatabasePath="<Chemin d'accès à un dossier sur un volume local>"
LogPath="<Chemin d'accès à un dossier sur un volume local>"
SYSVOLPath="<Chemin d'accès à un dossier sur un volume local>"
InstallDNS=yes
ConfirmGC=yes
SafeModeAdminPassword=<Mot de passe pour un compte administrateur hors connexion>
RebootOnCompletion=oui
```

Une fois que vous avez installé les binaires AD DS, vous pouvez terminer l'installation et la configuration d'une des quatre manières suivantes :

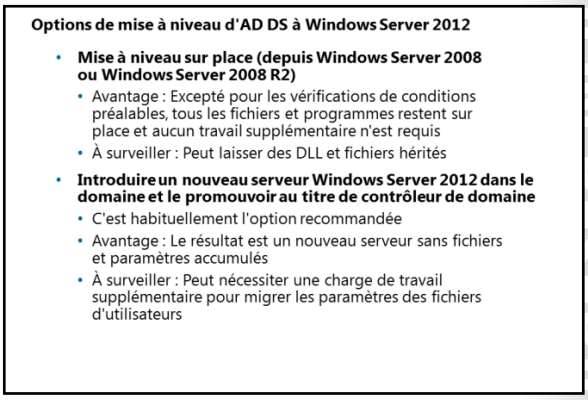
- Dans le Gestionnaire de serveur, cliquez sur l'icône de notification pour terminer la configuration post-déploiement. Ceci démarre la configuration et l'installation du contrôleur de domaine.
- Exécutez la commande Windows PowerShell **Install-ADDSDomainController –domainname "Adatum.com"** avec d'autres arguments, selon les besoins.
- Créez un fichier de réponses et exécutez **dcpromo /unattend:"D:\answerfile.txt"** à une invite de commandes où "D:\answerfile.txt" est le chemin d'accès au fichier de réponses.

Exécutez **dcpromo /unattend** à une invite de commandes avec les commutateurs appropriés, par exemple :

```
dcpromo /unattend /InstallDns:yes /confirmglobal catalog:yes /replicaOrNewDomain:replica
/replicadomaindnsname:"nouveau_domaine.com" /databasePath:"c:\ntds"
/logPath:"c:\ntdslogs" /sysvolpath:"c:\sysvol" /safeModeAdminPassword:Pa$$w0rd
/rebootOnCompletion:yes
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Mise à niveau d'un contrôleur de domaine



Vous pouvez mettre à niveau un contrôleur de domaine Windows Server 2012 de deux manières. Vous pouvez mettre à niveau le système d'exploitation sur les contrôleurs de domaine existants qui exécutent Windows Server 2008 ou Windows Server 2008 R2. Vous pouvez également introduire des serveurs Windows Server 2012 comme contrôleurs de domaine dans un domaine contenant des contrôleurs de domaine qui exécutent des versions antérieures de Windows Server. Des deux manières, la seconde est la méthode recommandée car elle vous permet de disposer à la fin sur le serveur d'une nouvelle installation du système d'exploitation Windows Server 2012 et de la base de données AD DS.

Mise à niveau vers Windows Server 2012

Pour mettre à niveau un domaine AD DS qui s'exécute à un niveau fonctionnel de Windows Server plus ancien vers un domaine AD DS qui s'exécute au niveau fonctionnel de Windows Server 2012, vous devez commencer par mettre à niveau tous les contrôleurs de domaine vers le système d'exploitation Windows Server 2012. Vous pouvez accomplir ceci en mettant à niveau tous les contrôleurs de domaine existants vers Windows Server 2012 ou en introduisant de nouveaux contrôleurs de domaine qui exécutent Windows Server 2012, puis en retirant progressivement les contrôleurs de domaine existants.

Pour effectuer une mise à niveau sur place d'un ordinateur doté du rôle AD DS, vous devez commencer par utiliser les commandes de ligne de commande **Adprep.exe /forestprep** et **Adprep.exe /domainprep** pour préparer la forêt et le domaine. Une mise à niveau sur place du système d'exploitation n'effectue pas une préparation automatique du schéma et du domaine. Adprep.exe est inclus sur le support d'installation dans le dossier \Support\Adprep. Aucune étape supplémentaire de configuration ne figure après ce point et vous pouvez continuer à exécuter la mise à niveau du système d'exploitation Windows Server 2012.

Lorsque vous effectuez la promotion d'un serveur Windows Server 2012 en contrôleur de domaine dans un domaine existant et si vous êtes connecté en tant que membre des groupes Administrateurs du schéma et Administrateurs de l'entreprise, le schéma AD DS sera mis à jour automatiquement vers Windows Server 2012. Dans ce scénario, vous n'avez pas besoin d'exécuter les commandes Adprep.exe avant de commencer l'installation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Déploiement de contrôleurs de domaine Windows Server 2012

Pour mettre à niveau le système d'exploitation d'un contrôleur de domaine Windows Server 2008 vers Windows Server 2012, procédez comme suit :

1. Insérez le disque d'installation de Windows Server 2012, puis exécutez **Setup**.
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 voulez-vous effectuer ?, cliquez sur **Mise à niveau : installer Windows et conserver les fichiers, les paramètres et les applications**.

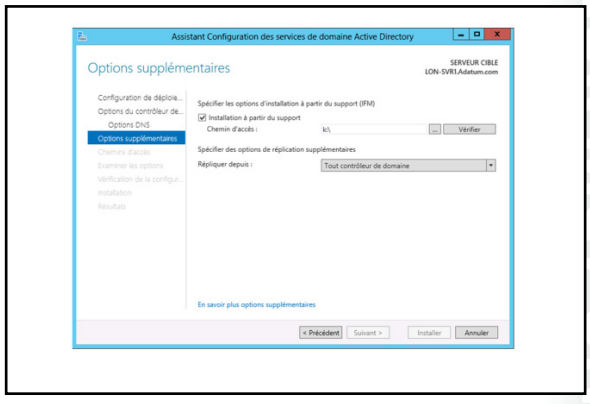
Remarque : Avec ce type de mise à niveau, il n'est pas nécessaire de conserver les paramètres des utilisateurs ni de réinstaller les applications ; tout est mis à niveau sur place. Veillez à vérifier la compatibilité matérielle et logicielle avant d'effectuer une mise à niveau.

Pour introduire une nouvelle installation de Windows Server 2012 en tant que contrôleur de domaine, procédez comme suit :

1. Déployez et configurez une nouvelle installation de Windows Server 2012 et joignez-la au domaine.
2. Effectuez la promotion du nouveau serveur en tant que contrôleur de domaine dans le domaine en utilisant la version 2012 du Gestionnaire de serveur ou l'une des autres méthodes décrites précédemment.

Remarque : Vous pouvez mettre à niveau directement Windows Server 2008 et Windows Server 2008 R2 vers Windows Server 2012.

Installation d'un contrôleur de domaine en utilisant l'installation à partir du support



Si vous possédez un réseau d'intervention qui est lent, peu fiable ou coûteux, il peut vous sembler nécessaire d'ajouter un autre contrôleur de domaine à un emplacement distant ou dans une filiale. Dans ce scénario, il vaut souvent mieux déployer AD DS sur un serveur à l'aide de l*a méthode* Installation à partir du support (IFM).

Par exemple, si vous vous connectez à un serveur dans un bureau distant et utilisez le Gestionnaire de serveur pour installer AD DS, vous devez copier la base de données AD DS complète et le dossier SYSVOL sur le nouveau contrôleur de domaine. Ce processus doit avoir lieu via une connexion WAN potentiellement peu fiable. Comme alternative, pour réduire de manière significative la quantité de trafic copiée via la liaison WAN, vous pouvez effectuer une copie de sauvegarde d'AD DS à l'aide de l'outil Ntdsutil. Quand vous exécutez le Gestionnaire de serveur pour installer AD DS, vous pouvez sélectionner l'option **Installation à partir du support**. La majeure partie de la copie s'effectue alors localement (par exemple à partir d'un lecteur USB) et la liaison WAN est utilisée seulement pour le trafic de sécurité et pour garantir que le nouveau contrôleur de domaine reçoit toutes les modifications effectuées après la création de la sauvegarde IFM.

Pour installer un contrôleur de domaine en utilisant l'installation à partir du support, accédez à un contrôleur de domaine qui n'est pas en lecture seule. Utilisez l'outil Ntdsutil pour créer une capture instantanée de la base de données AD DS, puis copiez la capture instantanée sur le serveur qui sera promu comme contrôleur de domaine. Utilisez le Gestionnaire de serveur pour promouvoir le serveur comme contrôleur de domaine en sélectionnant l'option **Installation à partir du support**, puis en fournissant le chemin d'accès local au répertoire IFM que vous avez créé auparavant.

La procédure complète est la suivante :

1. Sur le contrôleur de domaine complet, ouvrez une invite de commandes d'administration, tapez les commandes suivantes (où *C:\IFM* est le répertoire de destination qui contiendra la capture instantanée de la base de données AD DS) et appuyez sur Entrée après chaque ligne :

```
Ntdsutil
activate instance ntds
ifm
create SYSVOL full C:\IFM
```

2. Sur le serveur dont vous effectuez la promotion en tant que contrôleur de domaine, procédez comme suit :
   a. Utilisez le Gestionnaire de serveur pour ajouter le rôle AD DS.
   b. Patientez pendant que les binaires AD DS s'installent.
   c. Dans le Gestionnaire de serveur, cliquez sur l'icône de notification pour terminer la configuration post-déploiement. L'Assistant Configuration des services de domaine Active Directory s'exécute.
   d. Au moment opportun pendant l'exécution de l'Assistant, sélectionnez l'option d'installation à partir du support (IFM), puis fournissez le chemin d'accès local au répertoire de capture instantanée.

AD DS s'installe alors à partir de la capture instantanée. Lorsque le contrôleur de domaine redémarre, il contacte les autres contrôleurs de domaine dans le domaine et met à jour AD DS avec toutes les modifications qui ont été apportées depuis la création de la capture instantanée.

Documentation supplémentaire : Pour plus d'informations sur les étapes nécessaires pour installer AD DS, voir Installer les services de domaine Active Directory (niveau 100) à l'adresse http://go.microsoft.com/fwlink/?LinkID=266739.

Question : Pour quelle raison spécifier le mot de passe pour le mode de restauration des services d'annuaire ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Installation de contrôleurs de domaine

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

Votre responsable vous a demandé d'installer un nouveau contrôleur de domaine dans le centre de données pour améliorer les performances de connexion. Il vous a également été demandé de créer un nouveau contrôleur de domaine pour une filiale en utilisant une installation à partir du support (IFM).

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- installer un contrôleur de domaine.
- installer un contrôleur de domaine selon la méthode IFM ;

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	22410B-LON-DC1 (à démarrer en premier) 22410B-LON-SVR1 22410B-LON-RTR 22410B-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 débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 : **Administrateur**
    - Mot de passe : **Pa$$w0rd**
    - Domaine : **ADATUM**
5. Répétez les étapes 1 à 3 pour **22410B-LON-SVR1**, **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Installation d'un contrôleur de domaine

Scénario

Les utilisateurs connaissent des lenteurs de connexion à Londres aux heures de pleine activité. L'équipe serveurs a déterminé que les contrôleurs de domaine sont submergés lorsque de nombreux utilisateurs s'authentifient simultanément. Pour améliorer les performances de connexion, vous ajoutez un nouveau contrôleur de domaine dans le centre de données de Londres.

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter un rôle Services de domaine Active Directory (AD DS) sur un serveur membre
2. Configurer un serveur en tant que contrôleur de domaine
3. Configurer un serveur en tant que serveur de catalogue global

▶ Tâche 1 : Ajouter un rôle Services de domaine Active Directory (AD DS) sur un serveur membre

1. Sur LON-DC1, dans le Gestionnaire de serveur, ajoutez **LON-SVR1** dans la liste des serveurs.
2. Ajoutez le rôle serveur **Services AD DS** à **LON-SVR1**. Ajoutez toutes les fonctionnalités requises lorsque vous y êtes invité.
3. L'installation dure quelques minutes. Une fois l'installation terminée, cliquez sur **Fermer** pour fermer l'Assistant Ajout de rôles et de fonctionnalités.

▶ Tâche 2 : Configurer un serveur en tant que contrôleur de domaine

- Sur LON-DC1, utilisez le Gestionnaire de serveur pour promouvoir LON-SVR1 comme contrôleur de domaine, et choisissez les options suivantes :
  - Ajoutez un contrôleur de domaine au domaine Adatum.com existant.
  - Utilisez les informations d'identification **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
  - Pour Options du contrôleur de domaine, installez **DNS (Domain Name System)**, mais supprimez la sélection pour installer le catalogue global.
  - Le mot de passe du mode de restauration des services d'annuaire est **Pa$$w0rd**.
  - Pour toutes les autres options, utilisez les options par défaut.

▶ Tâche 3 : Configurer un serveur en tant que serveur de catalogue global

1. Connectez-vous à LON-SVR1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Utilisez **Sites et services Active Directory** pour configurer LON-SVR1 comme serveur de catalogue global.

Résultats : À la fin de cet exercice, vous devez avoir exploré le Gestionnaire de serveur et promu un serveur membre en tant que contrôleur de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Installation d'un contrôleur de domaine selon la méthode IFM

Scénario

Vous avez été chargé par la direction de gérer une des nouvelles filiales en cours de configuration. La mise en place d'une connexion réseau plus rapide est planifiée quelques semaines plus tard. D'ici là, la connectivité réseau est très lente.

Il a été déterminé que la filiale requiert un contrôleur de domaine pour prendre en charge les connexions locales. Pour éviter des problèmes avec la connexion réseau lente, vous utilisez l'installation à partir du support (IFM) pour installer le contrôleur de domaine dans la filiale.

Les tâches principales de cet exercice sont les suivantes :

1. Utiliser l'outil Ntdsutil pour générer IFM
2. Ajouter le rôle AD DS sur le serveur membre
3. Utilisez l'option IFM pour configurer un serveur membre comme nouveau contrôleur de domaine
4. Pour préparer le module suivant

▶ Tâche 1 : Utiliser l'outil Ntdsutil pour générer IFM

1. Sur LON-DC1, ouvrez une interface de ligne de commande d'administration et utilisez **Ntdsutil** pour créer une copie de sauvegarde IFM de la base de données AD DS et du dossier SYSVOL. Les commandes permettant de créer la copie de sauvegarde sont les suivantes :

```
Ntdsutil
Activate instance ntds
Ifm
Create sysvol full c:\ifm
```

▶ Tâche 2 : Ajouter le rôle AD DS sur le serveur membre

1. Basculez vers LON-SVR2 et connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Ouvrez une invite de commandes et mappez la lettre de lecteur **K:** à **\\LON-DC1\C$\IFM**.
3. Utilisez le Gestionnaire de serveur pour installer le rôle serveur AD DS sur LON-SVR2.

▶ Tâche 3 : Utilisez l'option IFM pour configurer un serveur membre comme nouveau contrôleur de domaine

1. Sur LON-SVR2, ouvrez une invite de commandes puis copiez la copie de sauvegarde IFM à partir de **K:** vers **C:\ifm**.
2. Sur LON-SVR2, utilisez le Gestionnaire de serveur avec les options suivantes pour effectuer la configuration post-déploiement d'AD DS :
   - Ajoutez un contrôleur de domaine au domaine Adatum.com existant.
   - Utilisez **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd** comme informations d'identification.
   - Utilisez **Pa$$w0rd** comme mot de passe du mode de restauration des services d'annuaire.

- Utilisez le support IFM pour installer et configurer AD DS. Utilisez l'emplacement **C:\IFM** comme support IFM.
- Acceptez tous les autres paramètres par défaut.

3. Redémarrez **LON-SVR2** pour terminer l'installation d'AD DS.

Résultats : À la fin de cet exercice, vous devez avoir installé un contrôleur de domaine supplémentaire pour la filiale en utilisant l'option IFM.

▶ 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 **22410B-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 **22410B-LON-SVR1**, **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quelles sont les deux fonctions principales des unités d'organisation ?

Question : Pourquoi auriez-vous besoin de déployer une arborescence supplémentaire dans la forêt AD DS ?

Question : Quelle méthode de déploiement utiliseriez-vous si vous deviez installer un contrôleur de domaine supplémentaire dans un emplacement distant doté d'une connexion WAN limitée ?

Question : Si vous aviez besoin de promouvoir une installation minimale de Windows Server 2012 comme contrôleur de domaine, quel outil ou quels outils utiliseriez-vous ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3

Gestion des objets de services de domaine Active Directory

Table des matières :

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

Leçon 1 : Gestion de comptes d'utilisateurs **3-3**

Leçon 2 : Gestion des comptes de groupes **3-12**

Leçon 3 : Gestion des comptes d'ordinateurs **3-20**

Leçon 4 : Délégation de l'administration **3-26**

Atelier pratique : Gestion des objets de services de domaine Active Directory **3-30**

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

Vue d'ensemble du module

Les comptes d'utilisateurs sont des composants fondamentaux de la sécurité du réseau. Enregistrés dans les services de domaine Active Directory® (AD DS), les comptes d'utilisateurs identifient les utilisateurs à des fins d'authentification et d'autorisation. En raison de leur importance, une compréhension des comptes d'utilisateurs et des tâches liées à leur prise en charge est un aspect essentiel de l'administration d'un réseau d'entreprise avec système d'exploitation Windows® Server.

Bien que les utilisateurs et les ordinateurs, et même les services, évoluent dans le temps, les rôles et règles métier tendent à se stabiliser. Votre entreprise a probablement un rôle financier, qui requiert certaines fonctions dans l'entreprise. L'utilisateur ou les utilisateurs qui tiennent ce rôle peuvent changer, mais le rôle change relativement peu. C'est pourquoi il n'est pas raisonnable de gérer un réseau d'entreprise en attribuant des droits et des autorisations aux utilisateurs, aux ordinateurs ou aux identités de service. Au lieu de cela, associez des tâches de gestion à des groupes. Par conséquent, il est important que vous sachiez utiliser les groupes pour identifier les rôles administratifs et utilisateur, filtrer la stratégie de groupe, attribuer des stratégies de mot de passe unique, et attribuer des droits et des autorisations.

Les ordinateurs, comme les utilisateurs, sont des entités de sécurité :

- Ils ont un compte avec un nom de connexion et un mot de passe que Windows Server modifie automatiquement et régulièrement.
- Ils s'authentifient auprès du domaine.
- Ils peuvent appartenir aux groupes, ont accès aux ressources, et vous pouvez les configurer à l'aide de la stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La gestion des ordinateurs (tant les objets dans AD DS et les périphériques physiques) est l'une des tâches quotidiennes de la plupart des professionnels de l'informatique. De nouveaux ordinateurs sont ajoutés à votre organisation, mis hors connexion pour réparation, échangés entre utilisateurs ou rôles, et supprimés ou mis à niveau. Chacune de ces activités requiert de gérer l'identité de l'ordinateur, qui est représentée par son objet, ou compte, et AD DS. Par conséquent, il est important que vous sachiez créer et gérer des objets ordinateur.

Dans les petites organisations, une personne peut être responsable de toutes ces tâches d'administration quotidiennes. Cependant, dans les réseaux de grandes entreprises, avec des milliers d'utilisateurs et d'ordinateurs, cela n'est pas possible. Il est important qu'un administrateur d'entreprise sache déléguer des tâches d'administration spécifiques aux utilisateurs ou aux groupes désignés pour garantir une administration d'entreprise efficace.

Objectifs

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

- gérer les comptes d'utilisateurs avec les outils graphiques ;
- gérer les comptes de groupes avec les outils graphiques ;
- gérer les comptes d'ordinateurs ;
- déléguer les autorisations d'exécution de l'administration d'AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Gestion de comptes d'utilisateurs

Un objet utilisateur dans AD DS est bien plus que de simples propriétés liées à l'identité de sécurité, ou compte, de l'utilisateur. Il constitue la pierre angulaire de l'identité et de l'accès dans les services de domaine Active Directory. Par conséquent, les processus cohérents, efficaces et sécurisés concernant l'administration des comptes d'utilisateurs constituent la pierre angulaire de la gestion de la sécurité d'entreprise.

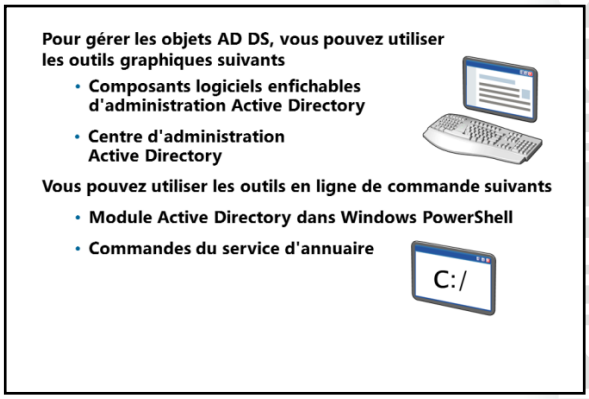
Objectifs de la leçon

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

- afficher les objets AD DS à l'aide de divers outils d'administration d'AD DS ;
- expliquer comment créer des comptes d'utilisateurs que vous pouvez utiliser dans un réseau d'entreprise ;
- décrire comment configurer des attributs de compte d'utilisateur importants ;
- décrire comment créer des profils utilisateur ;
- expliquer comment gérer des comptes d'utilisateurs.

Outils d'administration d'AD DS

Avant de pouvoir commencer à créer et gérer des comptes d'utilisateurs, de groupes et d'ordinateurs, il est important que vous compreniez quels outils vous pouvez utiliser pour effectuer ces diverses tâches de gestion.



Composants logiciels enfichables d'administration Active Directory

La majorité de l'administration d'AD DS est exécutée à l'aide des composants logiciels enfichables et consoles suivants :

- Utilisateurs et ordinateurs Active Directory.
  Ce composant logiciel enfichable gère la plupart des ressources quotidiennes courantes, dont les utilisateurs, les groupes, les ordinateurs et les unités d'organisation. Il s'agit probablement du composant logiciel enfichable le plus utilisé par un administrateur Active Directory.
- Sites et services Active Directory. Ce composant logiciel enfichable gère la réplication, la topologie du réseau et les services connexes.

- Composant Domaines et approbations Active Directory. Ce composant logiciel enfichable configure et maintient les relations d'approbation ainsi que le niveau fonctionnel du domaine et de la forêt.
- Composant logiciel enfichable Schéma Active Directory. Ce composant logiciel enfichable examine et modifie la définition des attributs et des classes d'objets d'Active Directory. Il constitue le modèle pour AD DS. Il est rarement affiché, et encore plus rarement modifié. Par conséquent, le composant logiciel enfichable Schéma Active Directory n'est pas installé par défaut.

Remarque : Pour administrer AD DS à partir d'un ordinateur qui n'est pas un contrôleur de domaine, vous devez installer les Outils d'administration de serveur distant (RSAT). Les Outils d'administration de serveur distant (RSAT) sont une fonctionnalité qui peut être installée à partir du nœud Fonctionnalités du Gestionnaire de serveur sur Windows Server® 2012.

Vous pouvez également installer RSAT sur des clients Windows, y compris Windows Vista® Service Pack 1 (ou version ultérieure), Windows 7 et Windows 8. Après avoir téléchargé les fichiers d'installation de RSAT à partir du site Web de Microsoft, exécutez l'Assistant Installation, qui vous guide tout au long de l'installation. Après avoir installé RSAT, vous devez activer l'outil ou les outils que vous souhaitez utiliser. Pour ce faire, dans le Panneau de configuration, dans l'application Programmes et fonctionnalités, utilisez la commande **Activer ou désactiver des fonctionnalités Windows**.

Documentation supplémentaire : Pour télécharger les fichiers d'installation de RSAT, consultez le Centre de téléchargement Microsoft à l'adresse http://go.microsoft.com/fwlink/?LinkID=266735.

Centre d'administration Active Directory

Windows Server 2012 fournit une autre option pour gérer des objets AD DS. Le Centre d'administration Active Directory fournit une interface utilisateur graphique (GUI) reposant sur Windows PowerShell®. Cette interface améliorée vous permet d'effectuer la gestion d'objets AD DS à l'aide de la navigation orientée vers les tâches. Les tâches que vous pouvez effectuer à l'aide du Centre d'administration Active Directory comprennent :

- créer et gérer des comptes d'utilisateurs, d'ordinateurs et de groupes ;
- créer et gérer des unités d'organisation ;
- se connecter à plusieurs domaines, et les gérer, dans une instance unique du Centre d'administration Active Directory ;
- rechercher et filtrer des données d'Active Directory en générant des requêtes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows PowerShell

Vous pouvez utiliser le module Active Directory pour Windows PowerShell (module Active Directory) pour créer et gérer des objets dans AD DS. Windows PowerShell est non seulement un langage de script, mais il permet également d'exécuter les commandes qui effectuent des tâches d'administration, telles que la création de comptes d'utilisateurs, la configuration de services, la suppression de boîtes aux lettres, et autres fonctions similaires.

Windows PowerShell est installé par défaut sur Windows Server 2012, mais le module Active Directory est seulement présent lorsque :

- vous installez les rôles de serveur AD DS ou des services AD LDS (Active Directory Lightweight Directory Services) ;
- vous exécutez Dcpromo.exe pour promouvoir un ordinateur dans un contrôleur de domaine ;
- vous installez RSAT.

Outils de ligne de commande du service d'annuaire

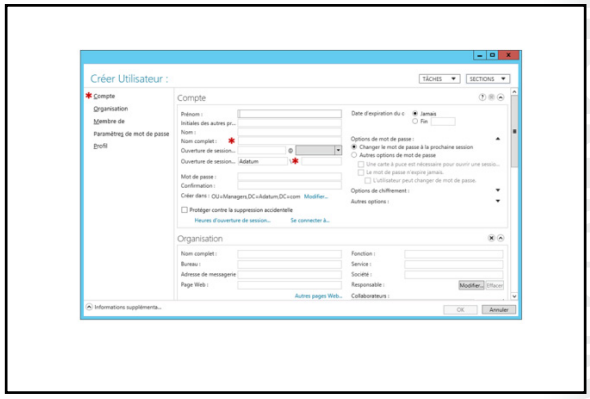
Vous pouvez également utiliser les outils de ligne de commande du service d'annuaire, en plus de Windows PowerShell. Ces outils permettent de créer, modifier, gérer et supprimer des objets AD DS, tels que des utilisateurs, des groupes et des ordinateurs. Vous pouvez utiliser les commandes suivantes :

- **Dsadd**. Pour créer des objets.
- **Dsget**. Pour afficher des objets et leurs propriétés.
- **Dsmod**. Pour modifier des objets et leurs propriétés.
- **Dsmove**. Pour déplacer des objets.
- **Dsquery**. Pour demander à AD DS des objets qui correspondent à des critères que vous fournissez.
- **Dsrm**. Pour supprimer des objets.

Remarque : Il est possible de diriger les résultats de la commande **Dsquery** vers d'autres commandes du service d'annuaire. Par exemple, la saisie de la commande suivante à une invite de commandes retourne le numéro de téléphone de bureau de tous les utilisateurs dont le nom commence par John :

```
dsquery user –name John* | dsget user –office
```

Création de comptes d'utilisateurs



Dans AD DS, tous les utilisateurs qui ont besoin d'accéder aux ressources réseau doivent être configurés avec un compte d'utilisateur. Grâce à ce compte d'utilisateur, les utilisateurs peuvent s'authentifier auprès du domaine AD DS et recevoir l'accès aux ressources réseau.

Dans Windows Server 2012, un *compte d'utilisateur* est un objet qui contient toutes les informations qui définissent un utilisateur. Un compte d'utilisateur inclut le nom d'utilisateur et le mot de passe, ainsi que les appartenances aux groupes. Un compte d'utilisateur contient également de nombreux autres paramètres que vous pouvez configurer en fonction de la configuration requise de votre organisation.

Avec un compte d'utilisateur, vous pouvez effectuer les tâches suivantes :

- accorder ou refuser aux utilisateurs des autorisations d'ouverture de session sur un ordinateur en fonction de l'identité de leur compte d'utilisateur ;
- autoriser les utilisateurs à accéder à des processus et à des services dans un contexte de sécurité spécifique ;
- gérer l'accès des utilisateurs aux ressources, telles que les objets AD DS et leurs propriétés, les dossiers partagés, les fichiers, les annuaires et les files d'attente d'impression.

Un compte d'utilisateur permet à un utilisateur d'ouvrir une session sur les ordinateurs et domaines avec une identité que le domaine peut authentifier. Lorsque vous créez un compte d'utilisateur, vous devez fournir un nom d'ouverture de session d'utilisateur, qui doit être unique dans le domaine/la forêt dans lesquels le compte d'utilisateur est créé.

Pour optimiser la sécurité, évitez que plusieurs utilisateurs partagent un même compte, et vérifiez plutôt que chaque utilisateur qui ouvre une session sur le réseau dispose d'un compte d'utilisateur et d'un mot de passe uniques.

Remarque : Bien que les comptes AD DS soient le sujet principal de ce cours, vous pouvez également enregistrer des comptes d'utilisateurs dans la base de données du Gestionnaire de comptes de sécurité locale de chaque ordinateur, ce qui permet d'ouvrir une session locale et d'accéder aux ressources locales. Les comptes d'utilisateurs locaux, pour la plupart, sortent du cadre de ce cours.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Création de comptes d'utilisateurs

Un compte d'utilisateur comprend le nom d'utilisateur et le mot de passe, qui servent d'informations d'ouverture de session pour l'utilisateur. Un objet utilisateur comprend également plusieurs autres attributs qui permettent de décrire et de gérer l'utilisateur.

Vous pouvez utiliser le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, le Centre d'administration Active Directory, Windows PowerShell ou l'outil de ligne de commande **dsadd.exe** pour créer un objet utilisateur.

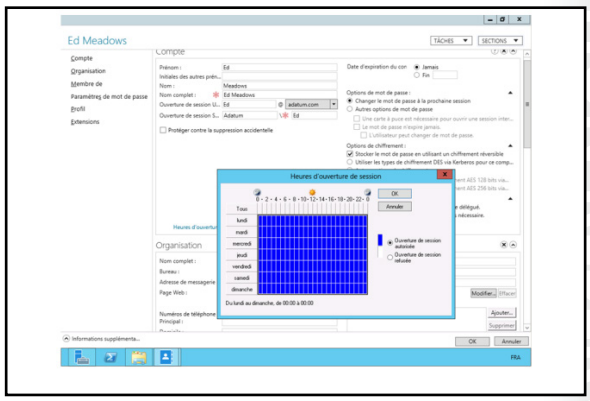
Lorsque vous créez des comptes d'utilisateurs, prenez en compte les propriétés suivantes :

- La propriété Nom complet du compte d'utilisateur permet de créer plusieurs attributs d'un objet utilisateur, et particulièrement le nom commun (CN) et les propriétés du nom complet. Le nom complet d'un utilisateur est le nom affiché dans le volet d'informations du composant logiciel enfichable. Il doit être unique dans le conteneur ou l'unité d'organisation. Si vous créez un objet utilisateur pour une personne portant le même nom qu'un utilisateur existant dans la même unité d'organisation ou le même conteneur, vous devez entrer un nom unique dans le champ **Nom complet**.
- La propriété Ouverture de session UPN de l'utilisateur se compose d'un préfixe de nom d'ouverture de session de l'utilisateur et d'un suffixe de nom d'utilisateur principal (UPN) qui seront ajoutés au nom d'ouverture de session de l'utilisateur après le symbole @.
    - Les noms d'utilisateurs dans AD DS peuvent contenir des caractères spéciaux, dont des points, des traits d'union et des apostrophes. Ces caractères spéciaux vous permettent de générer des noms d'utilisateur exacts, tels que O'Hare et Smith-Bates. Cependant, certaines applications peuvent présenter d'autres restrictions, nous vous recommandons donc d'utiliser uniquement des lettres et chiffres standard jusqu'à ce que vous ayez testé entièrement les applications dans votre environnement d'entreprise à des fins de compatibilité avec des caractères spéciaux.
    - Vous pouvez gérer la liste des suffixes UPN disponibles à l'aide du composant logiciel enfichable Domaines et approbations Active Directory. Cliquez avec le bouton droit sur la racine du composant logiciel enfichable, cliquez sur **Propriétés**, puis utilisez l'onglet **Suffixes UPN** pour ajouter ou supprimer des suffixes. Le nom DNS de votre domaine d'AD DS est toujours disponible comme suffixe ; vous ne pouvez pas le supprimer.

Remarque : Il est important que vous implémentiez une stratégie d'affectation de noms pour les comptes d'utilisateurs, en particulier dans de grands réseaux où les utilisateurs peuvent partager le même nom complet. Une combinaison du nom et du prénom, et si nécessaire, de caractères spéciaux, devrait permettre d'obtenir un nom de compte d'utilisateur unique. Plus particulièrement, seul le nom UPN doit être unique dans votre forêt AD DS. Le nom complet doit être unique uniquement dans l'unité d'organisation dans laquelle il réside, alors que le nom SamAccountName de l'utilisateur doit être unique dans ce domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des attributs de compte d'utilisateur



Lorsque vous créez un compte d'utilisateur dans AD DS, configurez également toutes les propriétés associées au compte, ou attributs.

Remarque : Les attributs associés à un compte d'utilisateur sont définis dans le cadre du schéma AD DS, que les membres du groupe de sécurité Administrateurs du schéma peuvent modifier.

En général, le schéma ne change pas fréquemment. Cependant, quand une application de niveau d'entreprise (telle que Microsoft® Exchange Server 2010) est ajoutée, de nombreuses modifications de schéma sont requises. Ces modifications permettent à des objets, y compris les objets utilisateur, d'avoir des attributs supplémentaires.

Lorsque vous créez un objet utilisateur, vous n'êtes pas obligé de définir de nombreux attributs autres que ceux requis pour permettre à l'utilisateur de se connecter à l'aide du compte. Étant donné que vous pouvez associer un objet utilisateur à de nombreux attributs, il est important que vous compreniez ce que sont ces attributs, et comment vous pouvez les utiliser dans votre organisation.

Catégories d'attributs

Les attributs d'un objet utilisateur peuvent être répartis dans plusieurs grandes catégories. Ces catégories s'affichent dans le volet de navigation de la boîte de dialogue **Propriétés de l'utilisateur** dans le Centre d'administration Active Directory, et incluent :

- **Compte**. Outre les propriétés de nom de l'utilisateur (**Prénom**, **Initiales des autres prénoms**, **Nom**, **Nom complet**) et les divers noms de connexion de l'utilisateur (**Ouverture de session UPN de l'utilisateur**, **Ouverture de session SamAccountName de l'utilisateur**), vous pouvez configurer les propriétés supplémentaires suivantes :
  - **Heures d'ouverture de session**. Cette propriété définit quand le compte peut être utilisé pour accéder à des ordinateurs de domaine. Vous pouvez utiliser l'affichage calendaire hebdomadaire pour définir des heures d'ouvertures de session autorisées et refusées.
  - **Se connecter à**. Utilisez cette propriété pour définir quels ordinateurs un utilisateur peut utiliser pour ouvrir une session sur le domaine. Spécifiez le nom de l'ordinateur et ajoutez-le à la liste des ordinateurs autorisés.
  - **Date d'expiration du compte**. Cette valeur est utile si vous souhaitez créer des comptes d'utilisateurs temporaires. Par exemple, si vous souhaitez créer des comptes d'utilisateurs pour des stagiaires, utilisés pendant un an seulement. Vous pouvez utiliser cette valeur pour définir à l'avance une date d'expiration du compte. Le compte ne peut pas être utilisé après la date d'expiration jusqu'à ce qu'il soit manuellement reconfiguré par un administrateur.
  - **Changer le mot de passe à la prochaine session**. Cette propriété permet pour forcer un utilisateur à réinitialiser son mot de passe la prochaine fois qu'il ouvre une session. En général, vous activez cette option après la réinitialisation du mot de passe d'un utilisateur.

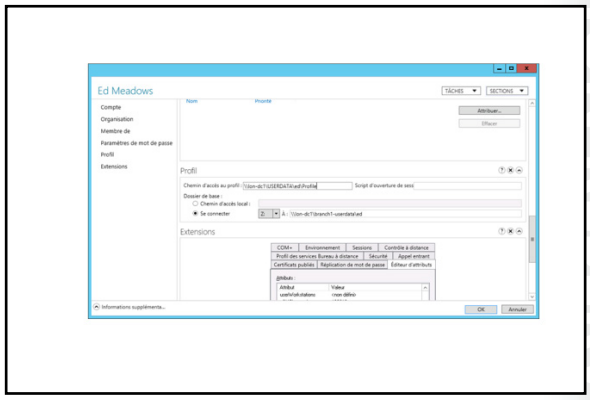
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

  - **La carte est requise pour ouvrir une session interactive**. Cette valeur réinitialise le mot de passe de l'utilisateur sur une séquence de caractères complexe et aléatoire, et définit une propriété qui requiert que l'utilisateur utilise une carte à puce pour s'authentifier à l'ouverture de session.
  - **Le mot de passe n'expire jamais**. Cette propriété est généralement utilisée avec des comptes de service ; c'est-à-dire, des comptes qui ne sont pas utilisés par des utilisateurs normaux mais par des services. Si vous définissez cette valeur, vous devez vous rappeler de régulièrement mettre à jour le mot de passe manuellement ; cependant, vous n'êtes pas obligé de le faire à un intervalle prédéterminé. Par conséquent, le compte ne peut jamais être verrouillé en raison de l'expiration du mot de passe, fonctionnalité particulièrement importante pour les comptes de service.
  - **L'utilisateur ne peut pas changer de mot de passe**. À nouveau, cette option est généralement utilisée pour les comptes de service.
  - **Stocker le mot de passe en utilisant un chiffrement réversible**. Cette stratégie fournit la prise en charge des applications qui utilisent des protocoles qui exigent la connaissance du mot de passe de l'utilisateur pour l'authentification. Le stockage des mots de passe avec un chiffrement réversible est quasiment identique au stockage des mots de passe en texte brut. C'est pourquoi cette stratégie ne devrait jamais être activée, sauf si les besoins de l'application sont supérieurs à la nécessité de protéger les informations de mot de passe. Cette stratégie est requise lors de l'utilisation de l'authentification CHAP (Challenge Handshake Authentication Protocol) via un accès distant ou le service d'authentification Internet (IAS). Elle est également requise pour l'authentification Digest dans les services Internet (IIS).
  - **Le compte est approuvé pour la délégation**. Vous pouvez utiliser cette propriété pour permettre à un compte de service de se faire passer pour un utilisateur standard afin d'accéder à des ressources réseau au nom d'un utilisateur.

- **Organisation**. Ceci comprend des propriétés telles que **Nom complet**, **Bureau**, **Adresse de messagerie** de l'utilisateur, divers numéros de téléphone, la structure hiérarchique, les noms des services et de la société ou les adresses.
- **Membre de**. Cette section permet de définir les appartenances à des groupes pour l'utilisateur.
- **Profil**. Cette section permet de configurer un emplacement pour les données personnelles de l'utilisateur, et de définir un emplacement dans lequel sauvegarder le profil de bureau de l'utilisateur lorsqu'il se déconnecte.
- **Extensions**. Cette section présente de nombreuses propriétés d'utilisateur supplémentaires, dont la plupart ne requiert normalement pas de configuration manuelle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Création des profils utilisateur



Lorsque les utilisateurs ferment une session, leur Bureau et leurs paramètres d'applications sont enregistrés dans un sous-dossier créé dans le dossier C:\Users sur le disque dur, qui correspond à leur nom d'utilisateur. Ce dossier contient leur profil utilisateur. Ce dossier héberge des sous-dossiers qui contiennent les documents et les paramètres qui représentent le profil utilisateur, dont les sous-dossiers Documents, Vidéos, Images et Téléchargements.

Si un utilisateur est susceptible d'ouvrir une session en mode interactif sur plusieurs stations de travail clientes, il est préférable que ces paramètres et documents soient disponibles sur ces autres stations de travail clientes. En tant qu'administrateur, vous pouvez utiliser plusieurs méthodes pour vérifier que les utilisateurs peuvent accéder à leurs profils à partir de plusieurs stations de travail.

Configuration des propriétés de compte d'utilisateur pour gérer des profils

À l'aide des paramètres de compte d'utilisateur dans le Centre d'administration Active Directory, vous pouvez configurer les propriétés suivantes liées au profil de bureau d'un utilisateur :

- **Chemin d'accès au profil**. Ce chemin d'accès est soit un chemin d'accès local soit, plus souvent, un chemin d'accès UNC (Universal Naming Convention). Les paramètres de Bureau de l'utilisateur sont enregistrés dans le profil. Une fois que vous définissez un profil utilisateur à l'aide d'un chemin UNC, quel que soit l'ordinateur du domaine que l'utilisateur utilise pour ouvrir une session, ses paramètres de bureau sont disponibles. Il s'agit d'un *profil itinérant*.

Remarque : Il est recommandé d'utiliser un sous-dossier du dossier de base de l'utilisateur pour le chemin d'accès du profil de l'utilisateur.

- **Script d'ouverture de session**. Ce script est le nom d'un fichier de commandes qui contient les commandes qui s'exécutent lorsque l'utilisateur ouvre une session. En général, vous utilisez ces commandes pour créer des mappages de lecteurs. Plutôt que d'utiliser un fichier de commandes de script d'ouverture de session, les administrateurs implémentent en général des scripts d'ouverture de session à l'aide des objets de stratégie de groupe (GPO) ou de préférences de stratégie de groupe. Si vous utilisez un script de connexion, cette valeur peut uniquement prendre la forme d'un nom de fichier (avec extension). Les scripts doivent être enregistrés dans le dossier C:\Windows\SYSVOL\domain\scripts sur tous les contrôleurs de domaine.
- **Dossier de base**. Cette valeur permet de créer une zone de stockage personnelle dans laquelle les utilisateurs peuvent sauvegarder leurs documents personnels. Vous pouvez spécifier un chemin d'accès local ou, plus souvent, un chemin d'accès UNC au dossier de l'utilisateur. Vous devez également spécifier une lettre de lecteur qui est utilisée pour mapper un lecteur réseau au chemin UNC spécifié. Vous pouvez alors configurer les documents personnels d'un utilisateur à ce dossier de base redirigé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des profils à l'aide de la console Stratégie de groupe

Une alternative à l'utilisation des paramètres des comptes d'utilisateurs individuels consiste à utiliser des objets de stratégie de groupe pour gérer ces paramètres. Vous pouvez configurer des paramètres de redirection de dossiers à l'aide de l'Éditeur de gestion des stratégies de groupe pour ouvrir un objet de stratégie de groupe pour le modifier, puis accéder au nœud Configuration utilisateur\Stratégies\Paramètres Windows.

Ces paramètres contiennent les sous-nœuds repris dans le tableau suivant.

Sous-nœuds dans le nœud Paramètres Windows		
• AppData (Roaming) • Bureau • Menu Accueil • Document	• Images • Musique • Vidéos • Favoris • Contacts	• Téléchargements • Liens • Recherches • Parties enregistrées

Vous pouvez utiliser ces sous-nœuds pour configurer tous les aspects des paramètres de profil de bureau et d'application d'un utilisateur. Pour un sous-nœud donné, tel que Documents, vous pouvez choisir entre la redirection de base et la redirection avancée. Dans la redirection de base, tous les utilisateurs affectés par l'objet de stratégie de groupe voient leur dossier Documents redirigé vers un sous-dossier nommé individuel sous un dossier racine commun défini par un nom UNC, par exemple \\LON-SVR1\Users\. La redirection avancée permet d'utiliser l'appartenance au groupe de sécurité pour déterminer où stocker les paramètres et les documents d'un utilisateur.

Démonstration : Gestion des comptes d'utilisateurs

Cette démonstration vous explique également comment :

- ouvrir le Centre d'administration Active Directory ;
- supprimer un compte d'utilisateur ;
- créer un compte d'utilisateur ;
- déplacer le compte d'utilisateur.

Procédure de démonstration

Ouvrir le Centre d'administration Active Directory

- Sur LON-DC1, ouvrez le **Centre d'administration Active Directory**.

Supprimer un compte d'utilisateur

- Localisez Ed Meadows dans l'unité d'organisation des gestionnaires, et supprimez le compte.

Créer un compte d'utilisateur

- Créez un compte d'utilisateur nommé **Ed Meadows**. Assurez-vous que le compte est créé avec un mot de passe fort.

Déplacer le compte d'utilisateur

- Déplacez le compte Ed Meadows vers l'unité d'organisation relative au service informatique IT.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Gestion des comptes de groupes

Bien que l'attribution des autorisations et des capacités aux comptes d'utilisateurs individuels dans de petits réseaux puisse être pratique, elle devient impossible et inefficace dans de grands réseaux d'entreprise. Par exemple, si de nombreux utilisateurs ont besoin du même niveau d'accès à un dossier, il est plus efficace de créer un groupe qui contient les comptes d'utilisateurs requis, puis d'attribuer au groupe les autorisations requises. Ceci a l'avantage de vous permettre de modifier les autorisations d'accès aux fichiers d'un utilisateur en l'ajoutant ou le supprimant des groupes, plutôt qu'en modifiant les autorisations d'accès aux fichiers directement.

Avant d'implémenter des groupes dans votre organisation, vous devez comprendre l'étendue des différents types de groupes Windows Server, et comment les utiliser au mieux pour gérer l'accès aux ressources ou pour attribuer des droits et des capacités de gestion.

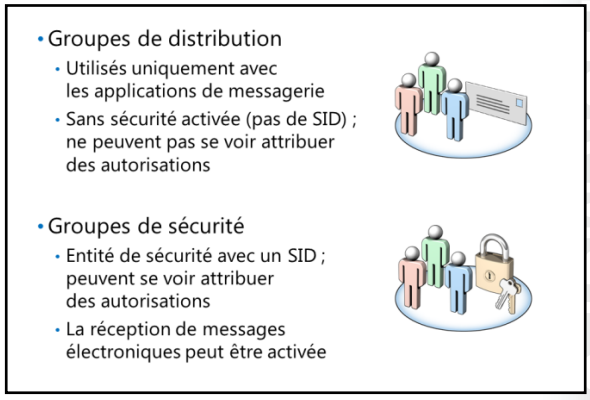
Objectifs de la leçon

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

- décrire les types de groupes ;
- décrire les étendues de groupes ;
- expliquer comment implémenter la gestion des groupes ;
- décrire les groupes par défaut ;
- décrire les identités spéciales ;
- gérer des groupes dans Windows Server.

Types de groupes

Dans un réseau d'entreprise Windows Server 2012, il y a deux types de groupes : les groupes de sécurité et les groupes de distribution. Lorsque vous créez un groupe, vous choisissez le type et l'étendue du groupe.



Les groupes de distribution, sur lesquels la sécurité n'est pas activée, sont principalement utilisés par des applications de messagerie électronique. Cela signifie qu'ils n'ont pas de SID, et qu'ils ne peuvent donc pas être autorisés à accéder aux ressources. L'envoi d'un message à un groupe de distribution permet d'envoyer le message à tous les membres du groupe.

Les groupes de sécurité sont des entités de sécurité avec des SID. Vous pouvez donc utiliser ces groupes dans des entrées d'autorisation dans des listes de contrôle d'accès pour contrôler la sécurité de l'accès aux ressources. Vous pouvez également utiliser des groupes de sécurité à des fins de distribution pour des applications de messagerie électronique. Si vous souhaitez utiliser un groupe pour gérer la sécurité, celui-ci doit être un groupe de sécurité.

Remarque : Le type de groupe par défaut est le groupe de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comme vous pouvez utiliser des groupes de sécurité pour l'accès aux ressources et la distribution des messages électroniques, de nombreuses organisations utilisent uniquement des groupes de sécurité. Cependant, si un groupe est utilisé uniquement pour la distribution des messages électroniques, nous vous recommandons de créer le groupe en tant que groupe de distribution. Dans le cas contraire, un SID est attribué au groupe, et le SID est ajouté au jeton d'accès de sécurité de l'utilisateur, ce qui peut entraîner à une augmentation de taille du jeton de sécurité inutile.

Remarque : Pensez que quand vous ajoutez un utilisateur à un groupe de sécurité, le jeton d'accès de l'utilisateur, qui authentifie les processus jour de l'utilisateur, est mis à jour uniquement quand l'utilisateur se connecte. Par conséquent, si l'utilisateur est connecté, il doit fermer sa session et en ouvrir une autre pour mettre à jour son jeton d'accès avec les modifications d'appartenances aux groupes.

Remarque : L'avantage de l'utilisation des groupes de distribution est encore plus évident dans des déploiements Exchange Server de grande ampleur, en particulier lorsque ces groupes de distribution doivent être imbriqués dans l'entreprise.

Étendues de groupes

Windows Server 2012 prend en charge les étendues de groupes. L'étendue d'un groupe détermine à la fois la plage de capacités ou d'autorisations d'un groupe, et l'appartenance au groupe.

Étendue de groupe	Membres d'un même domaine	Membres d'un domaine dans la même forêt	Membres d'un domaine externe approuvé	Possibilité de se voir attribuer des autorisations aux ressources
Local	U, O, GG, GLD, GU et utilisateurs locaux	U, O, GG, GU	U, O, GG	Sur l'ordinateur local uniquement
Domaine local	U, O, GG, GLD, GU	U, O, GG, GU	U, O, GG	N'importe où dans le domaine
Universel	U, O, GG, GU	U, O, GG, GU	N/A	N'importe où dans la forêt
Global	U, O, GG	N/A	N/A	N'importe où dans le domaine ou dans un domaine approuvé

U Utilisateur
O Ordinateur
GG Groupe global
GLD Groupe local de domaine
GU Groupe universel

Il existe quatre étendues de groupes :

- Local. Ce type de groupe est conçu pour les serveurs ou stations de travail autonomes, sur des serveurs membres du domaine qui ne sont pas des contrôleurs de domaine ou sur des stations de travail membres du domaine. Les groupes locaux sont vraiment locaux, c'est-à-dire qu'ils sont disponibles uniquement sur l'ordinateur sur lequel ils existent. Les principales caractéristiques d'un groupe local sont :
  - Vous pouvez attribuer des capacités et des autorisations uniquement sur les ressources locales, c'est-à-dire sur l'ordinateur local.
  - Les membres peuvent être n'importe où dans la forêt AD DS, et peuvent inclure :
    - des entités de sécurité du domaine : utilisateurs, ordinateurs, groupes globaux ou groupes locaux de domaine ;
    - des utilisateurs, ordinateurs et groupes globaux de n'importe quel domaine dans la forêt ;
    - des utilisateurs, ordinateurs et groupes globaux de n'importe quel domaine approuvé ;
    - des groupes universels définis dans n'importe quel domaine de la forêt.

- Domaine local. Ce type de groupe est principalement utilisé pour gérer l'accès aux ressources ou pour attribuer des responsabilités de gestion (droits). Les groupes locaux de domaine existent sur des contrôleurs de domaine dans une forêt AD DS et, par conséquent, l'étendue des groupes est localisée au domaine dans lequel ils résident. Les principales caractéristiques des groupes locaux de domaine sont :
  - Vous pouvez attribuer des capacités et des autorisations uniquement sur les ressources locales de domaine, c'est-à-dire sur tous les ordinateurs du domaine local.
  - Les membres peuvent être n'importe où dans la forêt AD DS, et peuvent inclure :
    - des entités de sécurité du domaine : utilisateurs, ordinateurs, groupes globaux ou groupes locaux de domaine ;
    - des utilisateurs, ordinateurs et groupes globaux de n'importe quel domaine dans la forêt ;
    - des utilisateurs, ordinateurs et groupes globaux de n'importe quel domaine approuvé ;
    - des groupes universels définis dans n'importe quel domaine de la forêt.
- Global. Ce type de groupe est principalement utilisé pour regrouper les utilisateurs qui présentent des caractéristiques semblables. Par exemple, des groupes globaux sont souvent utilisés pour regrouper les utilisateurs qui font partie d'un service ou d'un emplacement géographique. Les principales caractéristiques des groupes globaux sont :
  - Vous pouvez attribuer des capacités et des autorisations n'importe où dans la forêt.
  - Les membres peuvent uniquement provenir du domaine local et peuvent inclure :
    - des utilisateurs, ordinateurs et groupes globaux du domaine local.
- Universel. Ce type de groupe est le plus utile dans les réseaux multidomaines car qu'il combine les caractéristiques des groupes locaux de domaine et des groupes globaux. Plus particulièrement, les principales caractéristiques des groupes universels sont :
  - Vous pouvez attribuer des capacités et des autorisations n'importe où dans la forêt, comme pour les groupes globaux.
  - Les membres peuvent être n'importe où dans la forêt AD DS, et peuvent inclure :
    - des utilisateurs, ordinateurs et groupes globaux de n'importe quel domaine dans la forêt ;
    - des groupes universels définis dans n'importe quel domaine de la forêt.
  - Les propriétés des groupes universels sont propagées au catalogue global, et rendues disponibles dans le réseau de l'entreprise sur tous les contrôleurs de domaine qui hébergent le rôle de catalogue global. Ceci qui permet d'accéder plus facilement aux listes des membres des groupes universels, ce qui peut être utile dans des scénarios multidomaines. Par exemple, si un groupe universel est utilisé pour la distribution de la messagerie électronique, le processus de détermination de la liste des membres est généralement plus rapide dans les réseaux multidomaines distribués.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

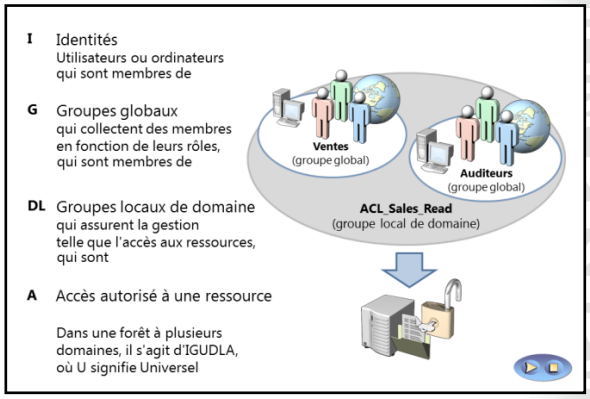
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémentation de la gestion des groupes

L'ajout des groupes à d'autres groupes est un processus appelé *imbrication*. L'imbrication crée une hiérarchie des groupes qui prennent en charge vos rôles métier et règles de gestion.

Il est conseillé d'utiliser l'imbrication de groupes appelée IGDLA, qui est l'acronyme en anglais de :

- Identités
- Groupes globaux
- Groupes locaux de domaine
- Accès



Les identités (comptes d'utilisateurs et comptes d'ordinateurs) sont membres des groupes globaux, qui représentent des rôles métier. Ces groupes de rôles (groupes globaux) sont membres des groupes locaux de domaine, qui représentent les règles de gestion, par exemple, pour déterminer qui dispose de l'autorisation en lecture sur un ensemble spécifique de dossiers. Ces groupes de règles (groupes locaux de domaine) sont autorisés à accéder aux ressources. Dans le cas d'un dossier partagé, l'accès est accordé en ajoutant le groupe local de domaine à la liste de contrôle d'accès du dossier, avec une autorisation qui fournit le niveau d'accès approprié.

Une forêt multidomaine contient également des groupes universels, qui se trouvent entre les groupes globaux et les groupes locaux de domaine. Les groupes globaux de plusieurs domaines sont membres d'un seul groupe universel. Ce groupe universel est membre des groupes locaux de domaine dans de plusieurs domaines. Pensez à l'imbrication en tant qu'IGUDLA.

Exemple IGDLA

L'illustration sur la diapositive représente une implémentation de groupe qui reflète le point de vue technique des méthodes conseillées de gestion des groupes (IGDLA), et le point de vue commercial de la gestion basée sur les rôles et sur les règles.

Prenez le scénario suivant :

Le personnel de vente chez Contoso, Ltd a juste terminé son exercice comptable. Les fichiers de ventes de l'année précédente se trouvent dans un dossier appelé Ventes. Le personnel de vente a besoin de l'accès en lecture sur le dossier Ventes. En outre, une équipe d'auditeurs de Woodgrove Bank, investisseur potentiel, exigent l'accès en lecture au dossier Ventes pour effectuer l'audit. Procédez comme suit pour implémenter la sécurité requise par ce scénario :

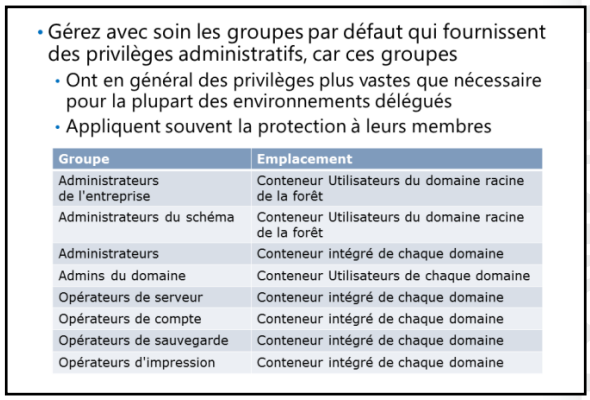
1. Affectez aux utilisateurs des responsabilités professionnelles communes ou d'autres caractéristiques commerciales aux groupes de rôles implémentés comme groupes de sécurité globaux. Faites ceci séparément dans chaque domaine. Le personnel de vente chez Contoso est ajouté à un groupe de rôles Ventes ; les auditeurs chez Woodgrove Bank sont ajoutés à un groupe de rôles Auditeurs.
2. Créez un groupe pour gérer l'accès aux dossiers Ventes avec l'autorisation Lecture. Implémentez ceci dans le domaine qui contient la ressource gérée. Dans ce cas, le dossier Ventes réside dans le domaine Contoso. Par conséquent, vous créez le groupe de règles de gestion de l'accès aux ressources en tant que groupe local de domaine nommé ACL_Sales Folders_Read.

3. Ajoutez les groupes de rôles au groupe de règles de gestion de l'accès aux ressources pour représenter la règle de gestion. Ces groupes peuvent provenir de n'importe quel domaine de la forêt ou d'un domaine de confiance, tel que Woodgrove Bank. Les groupes globaux de domaines externes de confiance, ou de n'importe quel domaine de la même forêt, peuvent être membre d'un groupe local de domaine.
4. Attribuez l'autorisation qui implémente le niveau d'accès requis. Dans ce cas, accordez l'autorisation Autoriser la lecture au groupe local de domaine.

Cette stratégie crée deux points uniques de gestion, réduisant ainsi la charge de gestion. Un point de gestion définit les membres du personnel de vente, l'autre point de gestion définit qui est auditeur. Puisque ces rôles sont susceptibles d'avoir accès à diverses ressources au-delà du dossier Ventes, un autre point de gestion permet de déterminer qui a accès en lecture au dossier Ventes. En outre, le dossier Ventes peut ne pas être un dossier unique sur un serveur unique ; il peut être constitué d'un ensemble de dossiers sur plusieurs serveurs, chacun attribuant l'autorisation Autoriser la lecture au groupe local de domaine unique.

Groupes par défaut

Le serveur Windows Server 2012 crée un certain nombre de groupes automatiquement. Ceux-ci sont appelés *groupes locaux par défaut*, et ils comprennent les groupes réputés tels que Administrateurs, Opérateurs de sauvegarde et Utilisateurs du Bureau à distance. Des groupes supplémentaires sont créés dans un domaine, dans les conteneurs Builtin et Utilisateurs, dont les Admins du domaine, les Administrateurs de l'entreprise et les Administrateurs du schéma.



La liste suivante fournit un résumé des fonctions pour le sous-ensemble de groupes par défaut qui ont des autorisations significatives et des droits d'utilisateur liés à la gestion d'AD DS :

- Administrateurs de l'entreprise (dans le conteneur Utilisateurs du domaine racine de la forêt). Ce groupe est membre du groupe Administrateurs dans tous les domaines dans la forêt, qui lui donne un accès complet à la configuration de tous les contrôleurs de domaine. Il possède également la partition Configuration du répertoire et dispose du contrôle total sur le contexte de dénomination du domaine dans tous les domaines de la forêt.
- Administrateurs du schéma (conteneur Utilisateurs du domaine racine de la forêt). Ce groupe possède le schéma Active Directory, sur lequel il a un contrôle total.
- Administrateurs (conteneur intégré de chaque domaine). Les membres de ce groupe disposent du contrôle total sur tous les contrôleurs de domaine et les données dans le contexte de dénomination de domaine. Ils peuvent modifier l'appartenance à tous les autres groupes administratifs dans le domaine, et le groupe Administrateurs dans le domaine racine de la forêt peut modifier l'appartenance des Administrateurs de l'entreprise, Administrateurs du schéma et Administrateurs du domaine. Le groupe Administrateurs dans le domaine racine de la forêt est sans doute le groupe d'administration de service le plus puissant dans la forêt.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Admins du domaine (conteneur Utilisateurs de chaque domaine). Ce groupe est ajouté au groupe Administrateurs de son domaine. Il hérite donc de toutes les fonctions du groupe Administrateurs. Il est également ajouté par défaut au groupe Administrateurs local de chaque ordinateur membre du domaine, accordant la propriété de tous les ordinateurs du domaine aux Admins du domaine.
- Opérateurs de serveur (conteneur intégré de chaque domaine). Les membres de ce groupe peuvent effectuer des tâches de maintenance sur les contrôleurs de domaine. Ils ont le droit d'ouvrir une session localement, de démarrer et arrêter des services, d'exécuter des opérations de sauvegarde et de restauration, de formater des disques, de créer ou supprimer des partages, et d'arrêter des contrôleurs de domaine. Par défaut, ce groupe ne comprend pas de membres.
- Opérateurs de compte (conteneur intégré de chaque domaine). Les membres de ce groupe peuvent créer, modifier et supprimer les comptes des utilisateurs, des groupes et des ordinateurs situés dans une unité d'organisation du domaine (sauf ceux de l'unité d'organisation Contrôleurs de domaine) et dans le conteneur Utilisateurs et ordinateurs. Les membres du groupe Opérateurs de compte ne peuvent pas modifier les comptes qui sont membres des groupes Administrateurs ou Admins du domaine, ni modifier ces groupes. Les membres du groupe Opérateurs de compte peuvent également ouvrir une session localement sur les contrôleurs de domaine. Par défaut, ce groupe ne comprend pas de membres.
- Opérateurs de sauvegarde (conteneur intégré de chaque domaine). Les membres de ce groupe peuvent exécuter des opérations de sauvegarde et de restauration sur les contrôleurs de domaine, et ouvrir une session localement et arrêter les contrôleurs de domaine. Par défaut, ce groupe ne comprend pas de membres.
- Opérateurs d'impression (conteneur intégré de chaque domaine). Les membres de ce groupe peuvent effectuer la maintenance des files d'attente d'impression sur les contrôleurs de domaine. Ils peuvent aussi ouvrir des sessions localement et arrêter les contrôleurs de domaine.

Vous devez gérer soigneusement les groupes par défaut qui fournissent des privilèges d'administrateur, car ils ont en général des privilèges plus larges que cela est nécessaire pour la plupart des environnements délégués, et car ils appliquent souvent la protection à leurs membres.

Le groupe Opérateurs de compte en est un bon exemple. Si vous examinez les fonctions du groupe Opérateurs de compte dans la liste précédente, vous pouvez voir que les membres de ce groupe ont des droits très larges, ils peuvent même ouvrir une session localement sur un contrôleur de domaine. Dans les très petits réseaux, de tels droits peuvent être appropriés pour une ou deux personnes qui sont généralement les administrateurs de domaine de toute façon. Dans de grandes entreprises, les droits et autorisations accordés aux Opérateurs de compte sont généralement trop larges.

En outre, le groupe Opérateurs de compte est, comme les autres groupes administratifs, un groupe protégé.

Les groupes protégés sont définis par le système d'exploitation et ne peuvent pas être non protégés. Les membres d'un groupe protégé deviennent protégés par l'association. Le résultat de la protection est que les autorisations (listes de contrôle d'accès) des membres sont modifiées de sorte qu'elles n'héritent plus des autorisations de leur unité d'organisation, mais reçoivent plutôt une copie d'une liste de contrôle d'accès qui est beaucoup plus restrictive. Par exemple, si vous ajoutez Jeff Ford au groupe Opérateurs de compte, son compte devient protégé, et l'assistance technique, qui peut réinitialiser tous autres mots de passe d'utilisateur dans l'unité d'organisation Employés, ne peut pas réinitialiser le mot de passe de Jeff Ford.

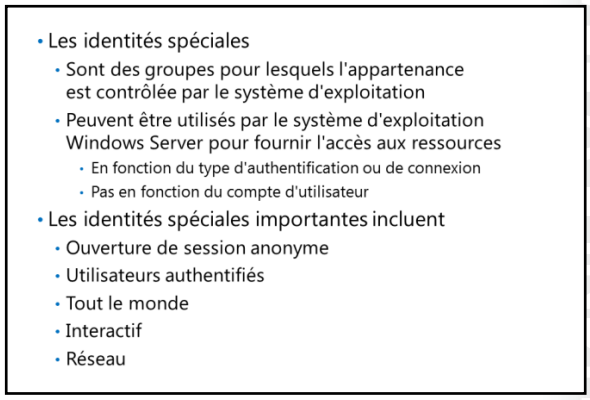
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Évitez d'ajouter des utilisateurs aux groupes qui n'ont pas de membres par défaut (Opérateurs de compte, Opérateurs de sauvegarde, Opérateurs de serveur et Opérateurs d'impression). Au lieu de cela, créez des groupes personnalisés auxquels vous attribuez des autorisations et des droits d'utilisateur qui répondent à vos exigences commerciales et administratives.

Par exemple, si Scott Mitchell doit être en mesure d'exécuter des opérations de sauvegarde sur un contrôleur de domaine, mais qu'il ne doit pas pouvoir exécuter les opérations de restauration qui pourraient entraîner la restauration de la base de données ou l'endommager, ni arrêter un contrôleur de domaine, ne placez pas Scott dans le groupe Opérateurs de sauvegarde. Créez plutôt un groupe et attribuez-lui uniquement le droit d'utilisateur Sauvegarde des fichiers et des répertoires, puis ajoutez Scott en tant que membre.

Identités spéciales

Windows et AD DS prennent également en charge les identités spéciales, qui sont des groupes dont l'appartenance est contrôlée par le système d'exploitation. Vous ne pouvez afficher les groupes dans aucune liste (dans le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, par exemple), vous ne pouvez ni afficher ni modifier l'appartenance de ces identités spéciales, et vous ne pouvez pas les ajouter à d'autres groupes. Vous pouvez, cependant, utiliser ces groupes pour attribuer des droits et des autorisations.



Les identités spéciales les plus importantes, souvent appelées *groupes* (par commodité), sont décrites dans la liste suivante :

- Ouverture de session anonyme. Cette identité représente des connexions à un ordinateur et à ses ressources qui sont établies sans fournir de nom d'utilisateur et de mot de passe. Avant Windows Server 2003, ce groupe était membre du chacun Tout le monde. À partir de Windows Server 2003, ce groupe n'est plus un membre par défaut du groupe Tout le monde.
- Utilisateurs authentifiés. Ceci représente les identités qui ont été authentifiées. Ce groupe n'inclut pas le compte Invité, même si celui-ci a un mot de passe.
- Tout le monde. Cette identité comprend le groupe Utilisateurs authentifiés et le compte Invité. (Sur les ordinateurs qui exécutent des versions du système d'exploitation Windows Server antérieures à Windows Server 2003, ce groupe inclut le groupe Ouverture de session anonyme.)

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Interactif. Ceci représente les utilisateurs qui accèdent à une ressource en étant connectés localement à l'ordinateur qui héberge la ressource, et non via le réseau. Lorsqu'un utilisateur accède à une ressource quelconque sur un ordinateur sur lequel l'utilisateur a ouvert une session localement, l'utilisateur est automatiquement ajouté au groupe Interactif pour cette ressource. Le groupe Interactif comprend également les utilisateurs qui ouvrent une session via une connexion Bureau à distance.
- Réseau. Ceci représente les utilisateurs qui accèdent à une ressource sur le réseau, et non les utilisateurs qui sont connectés localement à l'ordinateur qui héberge la ressource. Lorsqu'un utilisateur accède à une ressource quelconque sur le réseau, l'utilisateur est automatiquement ajouté au groupe Réseau pour cette ressource.

L'importance de ces identités spéciales réside dans le fait que vous pouvez les utiliser pour fournir l'accès aux ressources selon le type d'authentification ou de connexion, plutôt que le compte d'utilisateur. Par exemple, vous pouvez créer un dossier sur un système qui permet aux utilisateurs d'afficher son contenu quand ils ont ouvert une session localement sur le système, mais qui ne permet pas aux mêmes utilisateurs d'afficher le contenu d'un lecteur mappé sur le réseau. Vous pouvez faire ceci en attribuant des autorisations à l'identité spéciale Interactif.

Démonstration : Gestion des groupes

Cette démonstration vous explique également comment :

- créer un groupe ;
- ajouter des membres au groupe ;
- ajouter un utilisateur au groupe ;
- changer le type et l'étendue du groupe ;
- modifier la propriété **Géré par** du groupe.

Procédure de démonstration

Créer un groupe

1. Sur LON-DC1, ouvrez le **Centre d'administration Active Directory**.
2. Créez un groupe de sécurité global dans l'unité d'organisation relative au service informatique IT appelée **Responsables TI**.

Ajouter des membres au groupe

- Ajoutez plusieurs utilisateurs au nouveau groupe.

Ajouter un utilisateur au groupe

- Ajoutez **Ed Meadows** au groupe **Responsables TI**.

Changer le type et l'étendue du groupe

- Dans les propriétés du groupe **Responsables TI**, modifiez l'étendue du groupe à **Universel** et le type à **Distribution**.

Modifier la propriété Géré par du groupe

- Ajoutez **Ed Meadows** à la liste **Géré par**, puis accordez-lui l'autorisation **Le gestionnaire peut mettre à jour la liste des membres**.

Leçon 3
Gestion des comptes d'ordinateurs

Un compte d'ordinateur commence son cycle de vie lorsque vous le créez et le joignez à votre domaine. Ensuite, les tâches d'administration quotidiennes comprennent les tâches suivantes :

- configurer les propriétés de l'ordinateur ;
- déplacer l'ordinateur d'une unité d'organisation à une autre ;
- gérer l'ordinateur lui-même ;
- attribuer un nouveau nom, réinitialiser, désactiver, activer et enfin supprimer l'objet ordinateur.

Il est important que vous sachiez effectuer ces diverses tâches de gestion de l'ordinateur afin de pouvoir configurer et maintenir les objets ordinateur dans votre organisation.

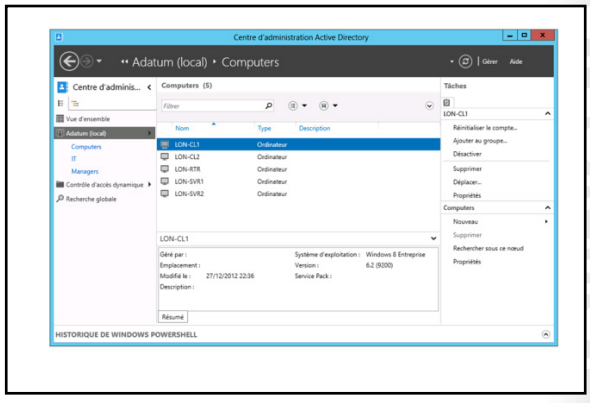
Objectifs de la leçon

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

- Expliquez le rôle du conteneur Ordinateurs AD DS.
- Décrivez comment configurer l'emplacement des comptes d'ordinateurs.
- Expliquez comment contrôler qui est autorisé à créer des comptes d'ordinateurs.
- Décrivez les comptes d'ordinateurs et le canal sécurisé.
- Expliquez comment réinitialiser le canal sécurisé.

Qu'est-ce que le conteneur Ordinateurs ?

Avant de créer un objet ordinateur dans le service d'annuaire, vous devez disposer d'un emplacement où le mettre.



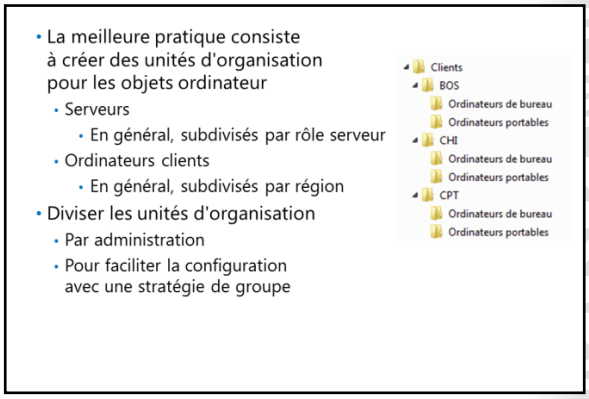
Lorsque vous créez un domaine, le conteneur Ordinateurs est créé par défaut (CN=Computers). Ce conteneur n'est pas une unité d'organisation ; au lieu de cela, c'est un objet de la classe Conteneur.

Il existe des différences subtiles mais importantes entre un conteneur et une unité d'organisation. Vous ne pouvez pas créer une unité d'organisation dans un conteneur, ainsi vous ne pouvez pas subdiviser l'unité d'organisation Ordinateurs. Vous ne pouvez pas non plus lier un objet de stratégie de groupe à un conteneur. Par conséquent, nous vous recommandons de créer des unités d'organisation personnalisées pour héberger les objets ordinateur, au lieu d'utiliser le conteneur Ordinateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Spécification de l'emplacement des comptes d'ordinateurs



La plupart des organisations créent au moins deux unités d'organisation pour les objets ordinateur : une pour les serveurs, et une autre pour héberger les comptes d'ordinateurs pour les ordinateurs clients, tels que des bureaux, des portables et d'autres systèmes utilisateur. Ces deux unités d'organisation s'ajoutent à l'unité d'organisation Contrôleurs de domaine qui est créée par défaut pendant l'installation d'AD DS.

Les objets ordinateur sont créés dans les deux unités d'organisation. Il n'existe aucune différence technique entre un objet ordinateur dans l'unité d'organisation d'un client et un objet ordinateur dans une unité d'organisation du serveur ou du contrôleur de domaine ; les objets ordinateur sont des objets ordinateur. Cependant, des unités d'organisation distinctes sont généralement créées pour fournir des étendues de gestion uniques, de sorte que vous puissiez déléguer la gestion des objets clients à une équipe et la gestion des objets serveur à une autre.

Votre modèle d'administration peut nécessiter une division supplémentaire de vos unités d'organisation client et serveur. De nombreuses organisations créent des sous-unités d'organisation sous une unité d'organisation serveur, pour collecter et gérer les types spécifiques de serveurs. Par exemple, vous pouvez créer une unité d'organisation pour les serveurs de fichiers et d'impression, et une unité d'organisation pour les serveurs de base de données. En procédant ainsi, vous pouvez déléguer des autorisations pour gérer les objets ordinateur dans l'unité d'organisation appropriée à l'équipe d'administrateurs pour chaque type de serveur. De même, les organisations distribuées géographiquement avec des équipes de support technique locales divisent souvent une unité d'organisation parente pour les clients en sous-unités d'organisation pour chaque site. Cette approche permet à l'équipe de support de chaque site de créer des objets ordinateur dans le site pour les ordinateurs clients, et pour joindre les ordinateurs au domaine à l'aide de ces objets ordinateur.

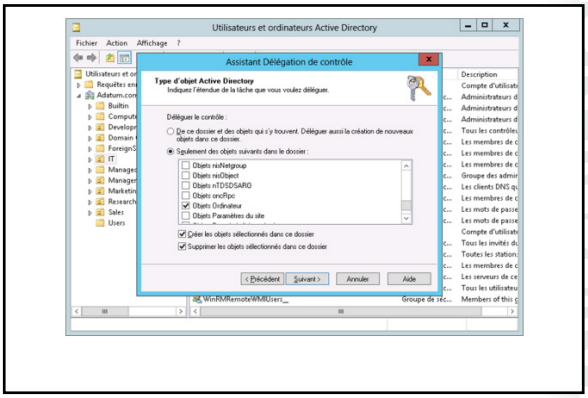
Outre ces exemples spécifiques, le plus important est que votre structure de l'unité d'organisation reflète votre modèle d'administration de sorte que vos unités d'organisation puissent fournir des points de gestion uniques pour la délégation de l'administration.

En outre, à l'aide des unités d'organisation distinctes, vous pouvez créer diverses configurations de base à l'aide des différents objets de stratégie de groupe qui sont liés aux unités d'organisations client et serveur. Avec la stratégie de groupe, vous pouvez spécifier la configuration pour des ensembles d'ordinateurs en liant les objets de stratégies de groupe qui contiennent des instructions de configuration aux unités d'organisation. Les organisations séparent souvent les clients dans les unités d'organisation de l'ordinateur de bureau et de l'ordinateur portable. Vous alors pouvez lier les objets de stratégie de groupe qui spécifient la configuration de l'ordinateur de bureau ou de l'ordinateur portable aux unités d'organisation appropriées.

Remarque : Vous pouvez utiliser l'outil de ligne de commande **Redircmp.exe** pour reconfigurer le conteneur de l'ordinateur par défaut. Par exemple, si vous souhaitez modifier le conteneur d'ordinateur par défaut en une unité d'organisation appelée mycomputers, utilisez la syntaxe suivante :

```
redircmp ou=mycomputers,DC=contoso,dc=com
```

Contrôle des autorisations pour créer des comptes d'ordinateurs



Pour joindre un ordinateur à un domaine Active Directory, quatre conditions doivent être remplies :

- Un objet ordinateur doit exister dans le service d'annuaire.
- Vous devez disposer des autorisations appropriées sur l'objet ordinateur qui vous permettent de joindre un ordinateur physique avec un nom qui correspond à celui de l'objet dans AD DS au domaine.
- Vous devez être membre du groupe Administrateurs local sur l'ordinateur. Vous pouvez ainsi modifier l'appartenance au domaine ou au groupe de travail de l'ordinateur.
- Vous ne devez pas dépasser le nombre maximal de comptes d'ordinateurs que vous pouvez ajouter au domaine. Par défaut, les utilisateurs peuvent uniquement ajouter un maximum de dix ordinateurs au domaine ; cette valeur est appelée *quota de comptes ordinateurs* et est contrôlée par la valeur de MS-DS-MachineQuota. Vous pouvez modifier cette valeur à l'aide du composant logiciel enfichable ADSIEdit.

Remarque : Vous n'avez pas besoin de créer un objet ordinateur dans le service d'annuaire, mais cela est recommandé. De nombreux administrateurs joignent les ordinateurs à un domaine sans d'abord créer un objet ordinateur. Cependant, quand vous faites ceci, Windows Server tente de joindre le domaine à un objet existant. Si Windows Server ne trouve pas l'objet, il est restauré et crée un objet ordinateur dans le conteneur Ordinateur par défaut.

Le processus de création d'un compte d'ordinateur à l'avance est appelé *préinstallation d'un ordinateur*. La préinstallation d'un ordinateur présente deux principaux avantages :

- Le compte est placé dans l'unité d'organisation appropriée, et est donc délégué selon la stratégie de sécurité définie par la liste de contrôle d'accès de l'unité d'organisation.
- L'ordinateur se trouve dans l'étendue des objets de stratégie de groupe liés à l'unité d'organisation, avant que l'ordinateur joigne le domaine.

Pour ce faire, une fois que vous êtes autorisé à créer des objets ordinateur, cliquez avec le bouton droit sur l'unité d'organisation et dans du menu **Nouveau**, cliquez sur **Ordinateur**. Ensuite, entrez le nom de l'ordinateur, conformément à la convention d'affectation de noms de votre entreprise, et sélectionnez l'utilisateur ou le groupe qui seront autorisés pour joindre l'ordinateur au domaine avec ce compte. Le nom des deux ordinateurs (Nom de l'ordinateur et Nom de l'ordinateur, avant Windows 2000) devraient être identiques. Il est très rarement justifié de les configurer séparément.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Délégation des autorisations

Par défaut, les groupes Administrateurs de l'entreprise, Admins du domaine, Administrateurs et Opérateurs de compte sont autorisés à créer des objets ordinateur dans n'importe quelle nouvelle unité d'organisation. Cependant, comme indiqué précédemment, nous vous recommandons de limiter strictement l'appartenance aux trois premiers groupes, et de n'ajouter aucun administrateur au groupe Opérateurs de compte.

À la place, déléguez l'autorisation de création d'objets ordinateur (appelée Créer des objets d'ordinateur) aux administrateurs compétents ou au service de support technique. Cette autorisation, qui est attribuée au groupe d'une unité d'organisation, permet aux membres du groupe de créer des objets ordinateur dans cette unité d'organisation. Par exemple, vous pouvez autoriser votre équipe de support technique à créer des objets ordinateur dans les unités d'organisation clientes, et autoriser vos administrateurs de serveur de fichiers à créer des objets ordinateur dans l'unité d'organisation des serveurs de fichiers. Pour déléguer les autorisations de création de comptes d'ordinateurs, vous pouvez utiliser l'Assistant Délégation de contrôle pour choisir une tâche personnalisée à déléguer.

Lorsque vous déléguez des autorisations de gestion des comptes d'ordinateurs, vous pouvez envisager d'accorder des autorisations supplémentaires à celles requises pour créer des comptes d'ordinateurs. Par exemple, vous pouvez décider d'autoriser un administrateur délégué à gérer les propriétés de comptes d'ordinateurs existants, supprimer le compte d'ordinateur ou déplacer le compte d'ordinateur.

Remarque : Si vous souhaitez autoriser un administrateur délégué à déplacer des comptes d'ordinateurs, n'oubliez pas qu'il a besoin des autorisations appropriées à la fois dans le conteneur AD DS source (où l'ordinateur existe actuellement) et dans le conteneur cible (vers lequel il déplace l'ordinateur). Plus particulièrement, il doit disposer des autorisations de suppression des ordinateurs dans le conteneur de source et de création des ordinateurs dans le conteneur cible.

Comptes d'ordinateurs et canaux sécurisés

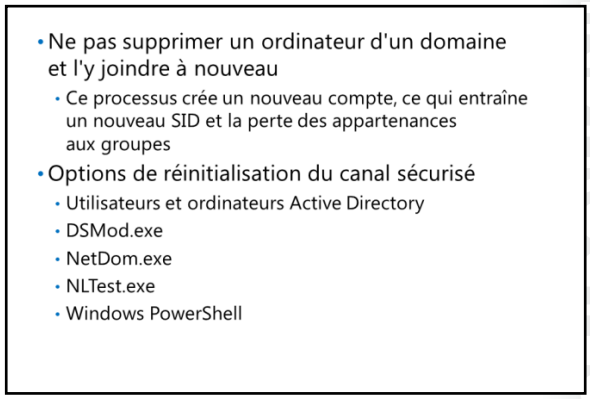
Chaque ordinateur membre d'un domaine AD DS conserve un compte d'ordinateur avec un nom d'utilisateur (SamAccountName) et un mot de passe, tout comme le fait un compte d'utilisateur. L'ordinateur enregistre son mot de passe sous forme de secret d'autorité de sécurité locale, et modifie son mot de passe avec le domaine tous les 30 jours environ. Le service NetLogon utilise les informations d'identification pour ouvrir une session sur le domaine, qui établit le canal sécurisé avec un contrôleur de domaine.

- Les ordinateurs ont des comptes
  - sAMAccountName et mot de passe
  - Utilisés pour créer un canal sécurisé entre l'ordinateur et le contrôleur de domaine
- Scénarios dans lesquels un canal sécurisé peut être rompu
  - La réinstallation d'un ordinateur, même avec le même nom, génère un nouveau SID et un nouveau mot de passe
  - La restauration d'un ordinateur à partir d'une ancienne sauvegarde, ou la restauration d'un ordinateur d'après une capture instantanée ancienne
  - Désaccord entre l'ordinateur et le domaine à propos du mot de passe

Les comptes d'ordinateurs et les relations sécurisées entre les ordinateurs et leur domaine sont fiables. Néanmoins, il peut arriver qu'un ordinateur ne puisse plus s'authentifier auprès du domaine. Voici des exemples de ces scénarios :

- Après la réinstallation du système d'exploitation sur une station de travail, la station de travail ne peut pas s'authentifier, bien que le technicien ait utilisé le même nom d'ordinateur que celui utilisé dans l'installation précédente. Étant donné que la nouvelle installation a généré un nouveau SID et que le nouvel ordinateur ne connaît pas le mot de passe initial du compte d'ordinateur dans le domaine, il n'appartient pas au domaine et ne peut pas s'authentifier auprès du domaine.
- Un ordinateur n'a pas été utilisé pendant une longue période, par exemple parce que l'utilisateur est en vacances ou travaille à distance. Les ordinateurs modifient leurs mots de passe tous les 30 jours, et les services de domaine Active Directory se souviennent du mot de passe actuel et du mot de passe précédent. Si l'ordinateur n'est pas utilisé pendant cette période, l'authentification peut échouer.
- Le secret d'autorité de sécurité locale d'un ordinateur n'est plus synchronisé avec le mot de passe que le domaine connaît. Cela équivaut à un ordinateur oubliant son mot de passe. Bien qu'il n'ait pas oublié son mot de passe, il est en désaccord avec le domaine quant au mot de passe. Lorsque cela se produit, l'ordinateur ne peut pas s'authentifier et le canal sécurisé ne peut pas être créé.

Réinitialisation du canal sécurisé



De temps à autre, les relations de sécurité entre un compte d'ordinateur et son domaine peuvent être interrompues ; ceci entraîne un certain nombre de symptômes et d'erreurs. Les signes les plus courants des problèmes de compte d'ordinateur sont :

- Les messages qui s'affichent à l'ouverture de session indiquent qu'un contrôleur de domaine ne peut pas être contacté, que le compte d'ordinateur est peut-être manquant, que le mot de passe du compte d'ordinateur est incorrect, ou que la relation d'approbation (autre façon de dire *relation sécurisée*) entre l'ordinateur et le domaine a été perdue.
- Les messages d'erreur ou les événements dans le journal des événements indiquent les problèmes semblables ou suggèrent que les mots de passe, les approbations, les canaux sécurisés ou les relations avec le domaine ou un contrôleur de domaine ont échoué. Un exemple de ce type d'erreur est « ID d'événement NETLOGON 3210 : Échec de l'authentification », qui apparaît dans le journal des événements de l'ordinateur.
- Un compte d'ordinateur manque dans AD DS.

Quand le canal sécurisé échoue, vous devez le réinitialiser. Beaucoup d'administrateurs font cela en supprimant l'ordinateur du domaine, en le plaçant dans un groupe de travail, puis en rejoignant le domaine. Cependant, cette procédure n'est pas recommandée car elle risque de supprimer complètement le compte d'ordinateur. La suppression du compte d'ordinateur supprime le SID de l'ordinateur, et plus important encore, ses appartenances aux groupes. Lorsque vous rejoignez le domaine à l'aide de cette procédure, bien que l'ordinateur ait le même nom, le compte a un nouveau SID, et toutes les appartenances aux groupes de l'objet ordinateur précédent doivent être recréées pour inclure le nouveau SID. Par conséquent, si l'approbation avec le domaine a été perdue, ne supprimez pas un ordinateur du domaine pour ensuite le joindre à nouveau. À la place, réinitialisez le canal sécurisé. Ceci permet de vous assurer que le compte d'ordinateur existant peut être réutilisé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour réinitialiser le canal sécurisé entre un membre du domaine et le domaine, utilisez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, DSMod.exe, NetDom.exe ou NLTest.exe. Si vous réinitialisez le compte, le SID de l'ordinateur reste le même et il maintient ses appartenances aux groupes.

Pour réinitialiser le canal sécurisé à l'aide du Centre d'administration Active Directory :

1. Cliquez avec le bouton droit sur un ordinateur, puis cliquez sur **Réinitialiser le compte**.
2. Cliquez sur **Oui** pour confirmer votre choix.
3. Joignez à nouveau l'ordinateur au domaine, puis redémarrez l'ordinateur.

Pour réinitialiser le canal sécurisé à l'aide de DSMod :

4. À l'invite de commandes, tapez la commande suivante :

```
dsmod computer "ComputerDN" –reset
```

5. Joignez à nouveau l'ordinateur au domaine, puis redémarrez l'ordinateur.

Pour réinitialiser le canal sécurisé à l'aide de NetDom.exe, saisissez la commande suivante à une invite de commandes, où les informations d'identification appartiennent au groupe Administrateurs local de l'ordinateur :

```
netdom reset MachineName /domain DomainName /UserO UserName /PasswordO {Password |
*}
```

Cette commande réinitialise le canal sécurisé en essayant de réinitialiser le mot de passe sur l'ordinateur et sur le domaine, afin de ne pas devoir effectuer une nouvelle jonction ou un redémarrage.

Pour réinitialiser le canal sécurisé à l'aide de NLTest.exe, sur l'ordinateur qui a perdu son approbation, saisissez la commande suivante à une invite de commandes :

```
NLTEST /SERVER:SERVERNAME /SC_RESET:DOMAIN\DOMAINCONTROLLER
```

Vous pouvez également utiliser Windows PowerShell avec le module Active Directory pour réinitialiser un compte d'ordinateur. L'exemple suivant montre comment réinitialiser le canal sécurisé entre l'ordinateur local et le domaine auquel il est joint.

Vous devez exécuter cette commande sur l'ordinateur local :

```
Test ComputerSecureChannel –Repair
```

Remarque : Vous pouvez également réinitialiser le mot de passe d'un ordinateur distant avec Windows PowerShell :

invoke-command -*computername* Workstation1 -scriptblock {reset-*computermachinepassword*}

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Délégation de l'administration

Bien qu'une seule personne puisse gérer un petit réseau avec quelques utilisateurs et comptes d'ordinateurs. Au fur et à mesure que le réseau croît, la charge de travail liée à la gestion du réseau fait de même. À un moment donné, les équipes avec des spécialisations particulières évoluent, chacune étant responsable d'un certain aspect spécifique de la gestion du réseau. Dans des environnements AD DS, il est courant de créer des unités d'organisation pour apporter une structure départementale ou géographique aux objets en réseau, et pour activer la configuration de la délégation administrative. Il est important que vous sachiez pourquoi et comment créer des unités d'organisation, et comment déléguer des tâches d'administration aux utilisateurs sur des objets dans ces unités d'organisation.

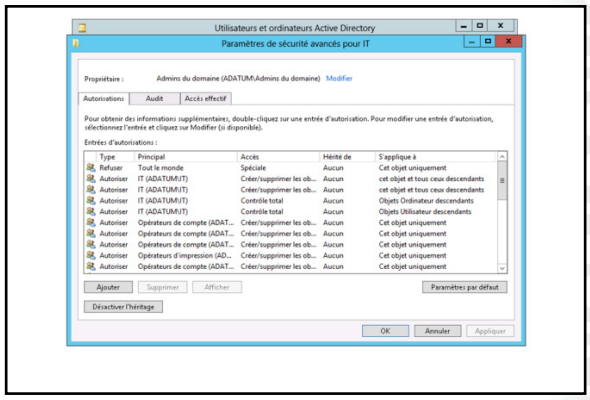
Objectifs de la leçon

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

- Décrivez les autorisations AD DS.
- Déterminez les autorisations AD DS efficaces d'un utilisateur sur un objet AD DS.
- Déléguez le contrôle administratif d'un objet AD DS à un utilisateur ou à un groupe d'utilisateurs spécifique.

Autorisations AD DS

Tous les objets AD DS, tels que des utilisateurs, ordinateurs et groupes, peuvent être sécurisés à l'aide d'une liste d'autorisations. Les autorisations sur un objet sont appelées entrées de contrôle d'accès, et sont attribuées aux utilisateurs, aux groupes ou aux ordinateurs, qui sont également appelés entités de sécurité. Les entrées de contrôle d'accès sont enregistrées dans la liste de contrôle d'accès discrétionnaire (DACL) de l'objet, qui fait partie de la liste de contrôle d'accès de l'objet. La liste de contrôle d'accès contient la liste de contrôle d'accès système (SACL) qui comprend des paramètres d'audit.



Chaque objet dans AD DS dispose de sa propre liste de contrôle d'accès. Si vous disposez des autorisations suffisantes, vous pouvez modifier les autorisations pour contrôler le niveau d'accès sur un objet AD DS spécifique. La délégation du contrôle administratif implique d'affecter les autorisations qui gèrent l'accès aux objets et aux propriétés dans AD DS. Tout comme vous pouvez donner à un groupe la capacité de modifier des fichiers dans un dossier, vous pouvez donner à un groupe la capacité, par exemple, de réinitialiser des mots de passe sur des objets utilisateur.

La liste DACL d'un objet permet également d'attribuer des autorisations à des propriétés spécifiques d'un objet. Par exemple, vous pouvez octroyer (ou refuser) l'autorisation de modifier les options de téléphone et de messagerie électronique. En fait, il ne s'agit pas seulement d'une propriété. C'est un ensemble de propriétés qui regroupe plusieurs propriétés spécifiques. Grâce aux ensembles de propriétés, vous pouvez facilement gérer les autorisations des collections de propriétés couramment utilisées. Cependant, vous pouvez également attribuer des autorisations plus précises et accorder ou refuser l'autorisation de modifier certaines informations, telles que le numéro de téléphone portable ou l'adresse postale.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Accorder à l'assistance technique l'autorisation de réinitialiser les mots de passe pour tous les objets utilisateur est une opération fastidieuse. Néanmoins, dans AD DS, il n'est pas recommandé d'attribuer des autorisations à des objets distincts. Vous devez plutôt attribuer des autorisations au niveau des unités d'organisation.

Les autorisations que vous attribuez à une unité d'organisation sont héritées par tous les objets dans l'unité d'organisation. Par conséquent, si vous autorisez l'assistance technique à réinitialiser les mots de passe pour des objets utilisateur et que vous associez cette autorisation à l'unité d'organisation qui contient les utilisateurs, tous les objets utilisateur dans cette unité d'organisation héritent de cette autorisation. En une seule étape, vous avez délégué cette tâche d'administration.

Les objets enfants héritent des autorisations du conteneur parent ou de l'unité d'organisation parente. Cet conteneur ou cette unité d'organisation hérite des autorisations de son conteneur parent ou de son unité d'organisation parente. S'il s'agit d'un conteneur ou d'une unité d'organisation de premier niveau, il ou elle hérite des autorisations du domaine même. La raison pour laquelle les objets enfant héritent des autorisations de leurs parents est que, par défaut, chaque nouvel objet est créé avec l'option **Inclure les autorisations pouvant être héritées du parent de cet objet** activée.

Autorisations AD DS effectives

Les autorisations effectives sont les autorisations résultantes pour une entité de sécurité (tel qu'un utilisateur ou un groupe), reposant sur l'effet cumulatif de chaque entrée de contrôle d'accès héritée et explicite. Votre capacité à réinitialiser un mot de passe d'utilisateur, par exemple, peut être due à votre appartenance à un groupe qui dispose de l'autorisation Réinitialiser le mot de passe sur une unité d'organisation, plusieurs niveaux au-dessus de l'objet utilisateur. L'autorisation héritée attribuée à un groupe auquel vous appartenez octroie une autorisation effective Autoriser : Réinitialiser le mot de passe. Vos autorisations effectives peuvent être compliquées lorsque vous prenez en compte les autorisations Autoriser et Refuser, les entrées de contrôle d'accès explicites et héritées, et le fait que vous pouvez appartenir à plusieurs groupes, chacun pouvant être doté de différentes autorisations.

Les autorisations attribuées aux utilisateurs et aux groupes se cumulent

La meilleure pratique consiste à affecter des autorisations à des groupes et non à des utilisateurs individuels

En cas de conflits

- Refuser des autorisations est prioritaire par rapport à autoriser des autorisations
- Les autorisations explicites ont priorité sur les autorisations héritées
  - Une autorisation explicite a priorité sur un refus hérité

Pour évaluer les autorisations effectives, vous pouvez utiliser

- L'onglet Autorisations effectives
- L'analyse manuelle

Les autorisations, qu'elles soient attribuées à votre compte d'utilisateur ou à un groupe auquel vous appartenez, sont équivalentes. Cela signifie que, au final, une entrée de contrôle d'accès s'applique à vous, l'utilisateur. La méthode conseillée consiste à gérer des autorisations en les attribuant aux groupes, mais il est également possible d'attribuer des entrées de contrôle d'accès aux utilisateurs ou ordinateurs individuels. Une autorisation qui a été attribuée directement à vous, l'utilisateur, n'est ni plus importante ni moins importante qu'une autorisation attribuée à un groupe auquel vous appartenez.

Les autorisations Autoriser, qui accordent l'accès, sont cumulatives. Si vous appartenez à plusieurs groupes, et que ces groupes se sont vus accorder des autorisations qui autorisent diverses tâches, vous pouvez effectuer toutes les tâches attribuées à tous ces groupes, ainsi que les tâches attribuées directement à votre compte d'utilisateur.

Les autorisations Refuser, qui interdisent l'accès, priment sur les autorisations Autoriser équivalentes. Si vous appartenez à un groupe qui a été autorisé à réinitialiser les mots de passe, et que vous appartenez également un autre groupe qui n'a pas été autorisé à réinitialiser les mots de passe, l'autorisation Refuser vous empêche de réinitialiser les mots de passe.

Remarque : Utilisez les autorisations Refuser avec parcimonie. En effet, il est souvent inutile d'attribuer des autorisations Refuser, car si vous n'attribuez pas d'autorisation Autoriser, les utilisateurs ne peuvent pas effectuer la tâche. Avant d'attribuer une autorisation Refuser, commencez par vérifier si vous pouvez atteindre votre objectif en supprimant une autorisation Autoriser. Par exemple, si vous souhaitez déléguer une autorisation Autoriser à un groupe, mais exclure un seul membre de ce groupe, vous pouvez attribuer une autorisation Refuser à ce compte d'utilisateur spécifique tandis que le groupe dispose d'une autorisation Autoriser.

Toutes les autorisations sont granulaires. Même si vous vous êtes vu refuser la capacité de réinitialiser les mots de passe, vous pouvez encore être en mesure de modifier le nom de connexion ou l'adresse de messagerie de l'utilisateur grâce à d'autres autorisations Autoriser.

Étant donné que les objets enfant héritent des autorisations pouvant être héritées des objets parent par défaut et que les autorisations explicites peuvent remplacer les autorisations Autoriser pouvant être héritées, une autorisation explicite remplace en fait une autorisation Refuser héritée.

Malheureusement, l'interaction complexe des autorisations des utilisateurs, des groupes, explicites, héritées, Autoriser et Refuser peut rendre l'évaluation des autorisations effectives fastidieuse. Vous pouvez utiliser les autorisations retournées par la commande **DSACL**, ou listées dans l'onglet **Accès effectif** de la boîte de dialogue **Paramètres de sécurité avancés** pour commencer à évaluer les autorisations effectives, mais cela reste une tâche manuelle.

Démonstration : Délégation du contrôle administratif

Cette démonstration vous explique également comment :

- déléguer une tâche standard ;
- déléguer une tâche personnalisée ;
- afficher les autorisations AD DS qui résultent de ces délégations.

Procédure de démonstration

Déléguer une tâche standard

1. Ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Utilisez l'Assistant Délégation de contrôle pour accorder au groupe IT les tâches de gestion standard suivantes sur l'unité d'organisation IT :
   - **Créer, supprimer et gérer les comptes d'utilisateurs**
   - **Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session**
   - **Lire toutes les informations sur l'utilisateur**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Déléguer une tâche personnalisée

- Utilisez l'Assistant Délégation de contrôle pour accorder les autorisations suivantes de l'unité d'organisation IT au groupe IT :
  - **Contrôle total sur les objets ordinateur**
  - **Créer des objets ordinateur**
  - **Supprimer des objets ordinateur**

Afficher les autorisations AD DS qui résultent de ces délégations

1. Activez la vue **Fonctions avancées** dans Utilisateurs et ordinateurs Active Directory.
2. Examinez les **propriétés** de l'unité d'organisation IT.
3. Utilisez l'onglet **Sécurité** pour vérifier les autorisations attribuées. Fermez toutes les fenêtres actives.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Gestion des objets de services de domaine Active Directory

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. Un bureau informatique et un centre de données sont situés à Londres pour assister le bureau de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

Vous avez travaillé pour A. Datum en tant que spécialiste du support technique et avez consulté les ordinateurs de bureau pour résoudre les problèmes d'application et de réseau. Vous avez récemment accepté une promotion au sein de l'équipe d'assistance technique des serveurs. L'une de vos premières missions consiste à configurer le service d'infrastructure pour une nouvelle filiale.

Pour commencer le déploiement de la nouvelle filiale, vous préparez des objets AD DS. Dans le cadre de cette préparation, vous devez créer une unité d'organisation pour la filiale et déléguer l'autorisation de la gérer. Ensuite, vous devez créer des utilisateurs et des groupes pour la nouvelle filiale. Enfin, vous devez réinitialiser le canal sécurisé pour un compte d'ordinateur qui a perdu la connectivité au domaine dans la filiale.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- déléguer l'administration pour une filiale ;
- créer et configurer des comptes d'utilisateurs dans AD DS ;
- gérer des objets ordinateur dans AD DS.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-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, dans **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 :
   a. Nom d'utilisateur : **Administrateur**
   b. Mot de passe : **Pa$$w0rd**
   c. Domaine : **ADATUM**
5. Répétez les étapes 2 à 4 pour **22410B-LON-CL1**.

Exercice 1 : Délégation de l'administration pour une filiale

Scénario

A. Datum délègue la gestion de chaque filiale à un groupe spécifique. Ceci permet à un employé qui travaille sur site d'être configuré en tant qu'administrateur, en cas de besoin. Chaque filiale a un groupe des administrateurs de la filiale qui peut exécuter l'administration complète dans l'unité d'organisation de la filiale. Le groupe d'assistance technique de la filiale peut quant à lui gérer des utilisateurs dans l'unité d'organisation de la filiale, mais pas d'autres objets. Vous devez créer ces groupes pour la nouvelle filiale et déléguer des autorisations aux groupes.

Les tâches principales de cet exercice sont les suivantes :

1. Déléguer l'administration pour les administrateurs d'une filiale
2. Déléguer un administrateur pour l'assistance technique de la filiale
3. Ajouter un membre aux Administrateurs de la filiale
4. Ajouter un membre au groupe d'assistance technique de la filiale

▶ Tâche 1 : Déléguer l'administration pour les administrateurs d'une filiale

1. Sur LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory**, puis créez dans le domaine **Adatum.com** une unité d'organisation appelée **Filiale 1**.
2. Créez les groupes de sécurité globaux suivants dans l'unité d'organisation **Filiale 1** :
   - **Assistance technique Filiale 1**
   - **Administrateurs Filiale 1**
   - **Utilisateurs Filiale 1**
3. Déplacez **Holly Dickson** de l'unité d'organisation **IT** vers l'unité d'organisation **Filiale 1**.
4. Déplacez les utilisateurs suivants de l'unité d'organisation **Filiale 1** :
   - **Development\Bart Duncan**
   - **Managers\Ed Meadows**
   - **Marketing\Connie Vrettos**
   - **Research\Barbara Zighetti**
   - **Sales\Arlene Huff**
5. Déplacez l'ordinateur **LON-CL1** vers l'unité d'organisation **Filiale 1**, puis redémarrez l'ordinateur **LON-CL1**.
6. Ouvrez une session sur LON-CL1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Sur LON-DC1, dans Utilisateurs et ordinateurs Active Directory, l'utilisation de l'Assistant Délégation de contrôle pour déléguer l'administration de l'unité d'organisation **Filiale 1** au groupe de sécurité **Administrateurs Filiale 1** en déléguant les tâches courantes et personnalisées suivantes :

   a. Déléguez les tâches courantes suivantes :

      - **créer, supprimer et gérer des comptes d'utilisateurs ;**
      - **réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session ;**
      - **lire toutes les informations sur l'utilisateur ;**
      - **créer, supprimer et gérer les groupes ;**
      - **modifier l'appartenance à un groupe ;**
      - **gérer les liens de stratégie de groupe.**

   b. Déléguez les tâches personnalisées suivantes :

      - **créer et supprimer les objets ordinateur dans l'unité d'organisation actuelle ;**
      - **contrôle total des objets ordinateur dans l'unité d'organisation actuelle.**

▶ Tâche 2 : Déléguer un administrateur pour l'assistance technique de la filiale

1. Sur LON-DC1, dans Utilisateurs et ordinateurs Active Directory, utilisez l'Assistant Délégation de contrôle pour déléguer l'administration de l'unité d'organisation **Filiale 1** au groupe de sécurité **Assistance technique Filiale 1**.
2. Déléguez les tâches courantes suivantes :
   - **Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session**
   - **Lire toutes les informations sur l'utilisateur**
   - **Modifier l'appartenance à un groupe**

▶ Tâche 3 : Ajouter un membre aux Administrateurs de la filiale

1. Sur LON-DC1, ajoutez **Holly Dickson** au groupe global **Administrateurs Filiale 1**.
2. Ajoutez le groupe global **Administrateurs Filiale 1** au groupe local de domaine **Opérateurs de serveurs**. Déconnectez-vous de LON-DC1.
3. Connectez-vous en tant que **ADATUM\Holly** avec le mot de passe **Pa$$w0rd**. Vous pouvez ouvrir une session localement sur un contrôleur de domaine car Holly appartient indirectement au groupe local de domaine Opérateurs de serveur.
4. À partir du Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**. Vérifiez les informations d'identification actuelles de Holly dans la boîte de dialogue **Contrôle de compte d'utilisateur**.
5. Tentez de supprimer **Sales\Aaren Ekelund**. L'opération échoue car Holly ne dispose pas des autorisations requises.
6. Essayez de supprimer **Filiale 1\Ed Meadows**. L'opération réussit car Holly dispose des autorisations requises.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Ajouter un membre au groupe d'assistance technique de la filiale

1. Sur LON-DC1, ajoutez **Bart Duncan** au groupe global **Assistance technique Filiale 1**.
2. Fermez Utilisateurs et ordinateurs Active Directory, puis le Gestionnaire de serveur.
3. Ouvrez le **Gestionnaire de serveur**, puis **Utilisateurs et ordinateurs Active Directory**. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, spécifiez **ADATUM\Administrateur** et **Pa$$w0rd** en tant qu'informations d'identification requises.

Remarque : Pour modifier la liste des membres du groupe Opérateurs de serveur, vous devez disposer des autorisations supérieures à celles du groupe Administrateurs Filiale 1.

4. Ajoutez le groupe global **Assistance technique Filiale 1** au groupe local de domaine **Opérateurs de serveurs**. Déconnectez-vous de LON-DC1.
5. Connectez-vous en tant que **ADATUM\Bart** avec le mot de passe **Pa$$w0rd**. Vous pouvez ouvrir une session localement sur un contrôleur de domaine car Bart appartient, indirectement, au groupe local de domaine Opérateurs de serveur.
6. Ouvrez le **Gestionnaire de serveur**, puis **Utilisateurs et ordinateurs Active Directory**. Vérifiez vos informations d'identification actuelles dans la boîte de dialogue **Contrôle de compte d'utilisateur**.
7. Essayez de supprimer **Filiale 1\Connie Vrettos**. L'opération échoue car Bart ne dispose pas des autorisations requises.
8. Rétablissez le mot de passe de Connie à **Pa$$w0rd**.
9. Après confirmation de la réinitialisation du mot de passe, déconnectez-vous de LON-DC1.
10. Ouvrez une session sur LON-DC1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir créé une unité d'organisation et délégué son administration au groupe compétent.

Exercice 2 : Création et configuration de comptes d'utilisateurs dans AD DS

Scénario

Vous disposez d'une liste de nouveaux utilisateurs pour la filiale et vous avez besoin de leur créer des comptes d'utilisateurs.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un modèle utilisateur pour la filiale
2. Configurer les paramètres du modèle
3. Créer un utilisateur pour la filiale d'après le modèle
4. Se connecter en tant qu'utilisateur pour tester les paramètres de compte

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Créer un modèle utilisateur pour la filiale

1. Sur LON-DC1, créez un dossier appelé **C:\branch1-userdata**, puis partagez-le.
2. Modifiez les autorisations de dossier partagé de sorte que le groupe **Tout le monde** dispose des autorisations **Autoriser Contrôle total**.
3. Dans le Gestionnaire de serveurs, ouvrez **Utilisateurs et ordinateurs Active Directory**, puis créez un utilisateur avec les propriétés suivantes dans l'unité d'organisation **Filiale 1** :
   - Nom complet : **_Branch_template**
   - Nom d'ouverture de session de l'utilisateur : **_Branch_template**
   - Mot de passe : **Pa$$w0rd**
   - **Le compte est désactivé**

▶ Tâche 2 : Configurer les paramètres du modèle

- Sur LON-DC1, modifiez les propriétés suivantes du compte **_Branch_template** :
  - Ville : **Slough**
  - Groupe : **Utilisateurs Filiale 1**
  - Dossier de base : **\\lon-dc1\branch1-userdata\%username%**

▶ Tâche 3 : Créer un utilisateur pour la filiale d'après le modèle

1. Sur LON-DC1, copiez le compte d'utilisateur **_Branch_template**, puis configurez les propriétés suivantes :
   - Prénom : **Ed**
   - Nom : **Meadows**
   - Mot de passe : **Pa$$w0rd**
   - L'option **L'utilisateur devra changer le mot de passe** est désactivée.
   - L'option **Le compte est désactivé** est désactivée.
2. Vérifiez que les propriétés suivantes ont été copiées lors de la création de compte :
   - Ville : **Slough**
   - Chemin d'accès du dossier de base : **\\lon-dc1\branch1-userdata\Ed**
   - Groupe : **Utilisateurs Filiale 1**
3. Déconnectez-vous de LON-DC1.

▶ Tâche 4 : Se connecter en tant qu'utilisateur pour tester les paramètres de compte

1. Basculez vers **LON-CL1** et déconnectez-vous.
2. Ouvrez une session sur **LON-CL1** en tant que **ADATUM\Ed** avec le mot de passe **Pa$$w0rd**. Vous pouvez ouvrir une session correctement.
3. Vérifiez que le lecteur Z est mappé avec le dossier de base d'Ed sur LON-DC1.
4. Déconnectez-vous de LON-CL1.

Résultats : À la fin de cet exercice, vous devez avoir créé et testé un compte d'utilisateur créé à partir d'un modèle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Gestion des objets ordinateur dans AD DS

Scénario

Une station de travail a perdu sa connectivité au domaine et ne peut pas authentifier les utilisateurs correctement. Lorsque les utilisateurs tentent d'accéder à des ressources de cette station de travail, l'accès est refusé. Vous devez réinitialiser le compte d'ordinateur pour recréer la relation d'approbation entre le client et le domaine.

Les tâches principales de cet exercice sont les suivantes :

1. Réinitialiser un compte d'ordinateur
2. Observer le comportement quand un client ouvre une session
3. Joindre à nouveau le domaine pour reconnecter le compte d'ordinateur

▶ Tâche 1 : Réinitialiser un compte d'ordinateur

1. Sur LON-DC1, ouvrez une session en tant que **ADATUM\Holly** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez **Utilisateurs et ordinateurs Active Directory**.
3. Vérifiez vos informations d'identification dans la boîte de dialogue **Contrôle de compte d'utilisateur**.
4. Accédez à **Filiale 1**.
5. Réinitialisez le compte d'ordinateur **LON-CL1**.

▶ Tâche 2 : Observer le comportement quand un client ouvre une session

1. Basculez vers **LON-CL1**, puis essayez d'ouvrir une session en tant que **ADATUM\Ed** avec le mot de passe **Pa$$w0rd**. Un message s'affiche indiquant **La relation d'approbation entre cette station de travail et le domaine principal a échoué**.
2. Cliquez sur **OK** pour accepter le message.

▶ Tâche 3 : Joindre à nouveau le domaine pour reconnecter le compte d'ordinateur

1. Ouvrez une session sur **LON-CL1** en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le Panneau de configuration, basculez vers l'affichage **Grandes icônes**, puis ouvrez **Système**.
3. Affichez les **Paramètres système avancés**, puis cliquez sur l'onglet **Nom d'ordinateur**.
4. Dans la boîte de dialogue **Propriétés système**, utilisez le bouton **Identité sur le réseau...** pour joindre à nouveau l'ordinateur au domaine.
5. Suivez les instructions de l'Assistant avec les paramètres suivants :
   - Nom d'utilisateur : **administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **Adatum**
   - Si vous souhaitez activer un compte d'utilisateur du domaine sur cet ordinateur : Non

6. Lorsque vous y êtes invité, redémarrez l'ordinateur.
7. Ouvrez une session en tant que **ADATUM\Ed** avec le mot de passe **Pa$$w0rd**. L'opération réussit car la jonction de l'ordinateur a été rétablie correctement.

Résultats : À la fin de cet exercice, vous devez avoir réinitialisé avec succès une relation d'approbation.

▶ 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 **22410B-LON-CL1**, 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 22410B-LON-DC1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Dans une entreprise disposant de filiales dans plusieurs villes, les membres d'une équipe de vente voyagent fréquemment entre les domaines. Chacun de ces domaines dispose de ses propres imprimantes qui sont gérées à l'aide de groupes locaux de domaine. Comment pouvez-vous fournir à ces membres l'accès aux diverses imprimantes des domaines ?

Question : Vous êtes chargé de gérer des comptes et l'accès aux ressources pour les membres de votre groupe. Un utilisateur de votre groupe est transféré vers un autre service de la société. Que devez-vous faire du compte de l'utilisateur ?

Question : Quelle est la principale différence entre le conteneur Ordinateur et une unité d'organisation ?

Question : Quand devriez-vous réinitialiser un compte d'ordinateur ? Pourquoi est-il mieux de réinitialiser le compte d'ordinateur plutôt que de supprimer puis recréer la jonction au domaine ?

Question : Un chef de projet de votre service démarre un projet de groupe qui se poursuivra l'année suivante. Plusieurs utilisateurs de votre service et d'autres services seront dédiés à ce projet pendant ce temps. L'équipe du projet doit avoir accès aux mêmes ressources partagées. Le chef de projet doit être en mesure de gérer les comptes d'utilisateurs et les comptes de groupes dans AD DS ; toutefois, vous ne voulez pas lui accorder l'autorisation de gérer autre chose dans AD DS. Quelle est la meilleure façon de procéder ?

Question : Vous travaillez en tant que technicien informatique chez Contoso, Ltd. Vous gérez l'infrastructure basée sur Windows Server. Vous devez trouver une méthode pour joindre de nouveaux ordinateurs Windows 8 à un domaine lors du processus d'installation, sans intervention d'un utilisateur ou d'un administrateur. Quelle est la meilleure façon de procéder ?

Outils

Outil	Utilisation	Emplacement
Utilisateurs et ordinateurs Active Directory	Gestion de groupes	Outils d'administration
Module Active Directory pour Windows PowerShell	Gestion de groupes	Installé comme fonctionnalité Windows
Utilitaires DS	Gestion de groupes	Ligne de commande
Module Active Directory pour Windows PowerShell	Gestion des comptes d'ordinateur	Outils d'administration
Djoin.exe	Jonction de domaine hors connexion	Ligne de commande
Redircmp.exe	Modification du conteneur d'ordinateur par défaut	Ligne de commande
DSACLS	Affichage et modification des autorisations AD DS	Ligne de commande

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Méthode conseillée

Méthodes conseillées pour la gestion des comptes d'utilisateurs

- Ne laissez pas les utilisateurs partager des comptes d'utilisateurs. Créez toujours un compte d'utilisateur pour chaque individu, même si cette personne ne rejoint votre organisation que temporairement.
- Sensibilisez les utilisateurs sur l'importance de la sécurité des mots de passe.
- Assurez-vous de choisir une stratégie d'attribution de noms pour des comptes d'utilisateurs qui permet d'identifier l'utilisateur lié au compte. Assurez-vous également que votre stratégie d'attribution de noms utilise des noms uniques dans votre domaine.

Méthodes conseillées pour la gestion des groupes

- Dans le cadre de la gestion de l'accès aux ressources, essayez d'utiliser le groupe local de domaine et les groupes de rôles.
- Utilisez les groupes universels uniquement lorsque cela est nécessaire car ils alourdissent le trafic de réplication.
- Utilisez Windows PowerShell avec le module Active Directory pour les programmes de commandes sur les groupes.
- Évitez d'ajouter des utilisateurs aux groupes intégrés et par défaut.

Méthodes conseillées concernant la gestion des comptes d'ordinateurs

- Configurez toujours un compte d'ordinateur avant de joindre des ordinateurs à un domaine, puis placez-les dans l'unité d'organisation appropriée.
- Redirigez le conteneur d'ordinateur par défaut vers un autre emplacement.
- Réinitialisez le compte d'ordinateur, au lieu de supprimer puis recréer la jonction.
- Intégrez la fonctionnalité de jonction de domaine hors connexion avec les installations sans assistance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4

Automatisation de l'administration des domaines de services Active Directory

Table des matières :

Vue d'ensemble du module **4-1**

Leçon 1 : Utilisation des outils en ligne de commande pour l'administration d'AD DS **4-2**

Leçon 2 : Utilisation de Windows PowerShell pour l'administration d'AD DS **4-8**

Leçon 3 : Exécution d'opérations en bloc avec Windows PowerShell **4-15**

Atelier pratique : Automatisation de l'administration d'AD DS à l'aide de Windows PowerShell **4-23**

Contrôle des acquis et éléments à retenir **4-28**

Vue d'ensemble du module

Vous pouvez utiliser des outils en ligne de commande et Windows PowerShell® pour automatiser l'administration des services de domaine Active Directory® (AD DS). L'automatisation de l'administration accélère les processus que vous devez normalement exécuter manuellement. Windows PowerShell comprend des applets de commande pour l'administration des services de domaine Active Directory (AD DS) et l'exécution des opérations en bloc. Vous pouvez utiliser des opérations en bloc pour modifier de nombreux objets AD DS en une seule étape au lieu de mettre à jour chaque objet manuellement.

Objectifs

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

- utiliser les outils en ligne de commande pour l'administration d'AD DS ;
- utiliser les applets de commande Windows PowerShell pour l'administration d'AD DS ;
- exécuter des opérations en bloc à l'aide de Windows PowerShell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Utilisation des outils en ligne de commande pour l'administration d'AD DS

Windows Server® 2012 inclut plusieurs outils en ligne de commande que vous pouvez utiliser pour exécuter l'administration d'AD DS. De nombreuses organisations créent des scripts qui utilisent des outils en ligne de commande pour automatiser la création et la gestion des objets AD DS, tels que les comptes d'utilisateurs et les groupes. Vous devez savoir utiliser ces outils en ligne de commande pour vérifier que vous pouvez modifier les scripts utilisés par votre organisation, si nécessaire.

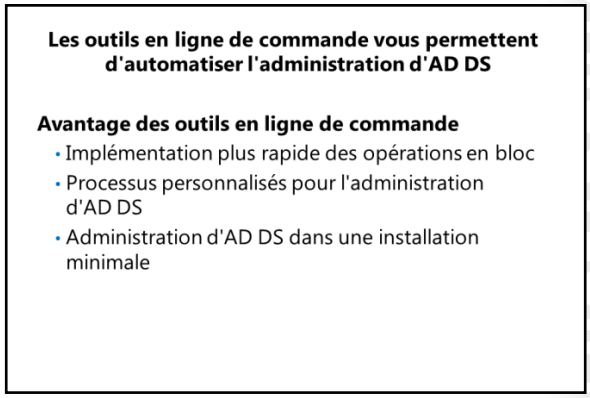
Objectifs de la leçon

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

- décrire les avantages de l'utilisation des outils en ligne de commande pour l'administration d'AD DS ;
- décrire comment et quand utiliser **csvde** ;
- décrire comment et quand utiliser **ldifde** ;
- décrire comment et quand utiliser les commandes DS.

Avantages de l'utilisation des outils en ligne de commande pour l'administration d'AD DS

De nombreux administrateurs préfèrent utiliser les outils graphiques pour l'administration d'AD DS chaque fois que cela est possible. Les outils graphiques, tels que le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory, sont utilisables de manière intuitive parce qu'ils représentent les informations visuellement et fournissent des options sous forme de cases d'option et de boîtes de dialogue. Lorsque les informations sont représentées graphiquement, vous n'avez pas besoin de mémoriser la syntaxe.



Les outils graphiques fonctionnent bien dans de nombreuses situations, mais ils ne peuvent pas être automatisés. Pour automatiser l'administration d'AD DS, vous avez besoin des outils en ligne de commande. Les outils en ligne de commande peuvent être utilisés dans les scripts ou par d'autres applications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

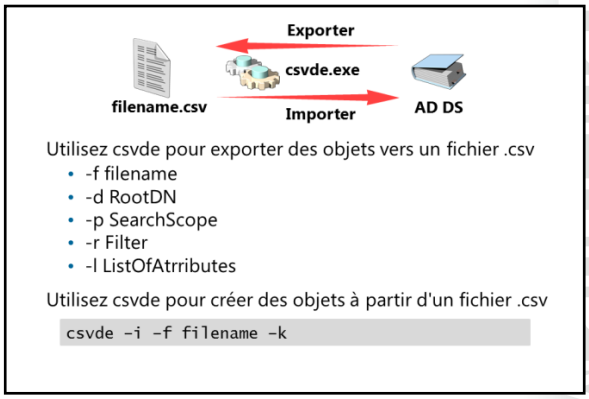
Voici quelques-uns des avantages liés à l'utilisation des outils en ligne de commande :

- Implémentation plus rapide des opérations en bloc. Par exemple, vous pouvez exporter une liste de nouveaux comptes d'utilisateurs à partir d'une application de gestion des ressources humaines. Vous pouvez utiliser un outil en ligne de commande ou un script pour créer des comptes d'utilisateurs en fonction des informations exportées. Ce processus est beaucoup plus rapide que de créer chaque nouveau compte d'utilisateur manuellement.
- Processus personnalisés pour l'administration d'AD DS. Vous pouvez utiliser un programme graphique personnalisé pour rassembler des informations sur un nouveau groupe et créer ensuite le nouveau groupe. Lorsque les informations sont rassemblées, le programme graphique peut vérifier que le format des informations, tel que la convention d'affectation de noms, est correct. Le programme graphique utilise ensuite un outil en ligne de commande pour créer le nouveau groupe. Ce processus permet l'application de règles spécifiques à la société.
- Administration d'AD DS dans une installation minimale. L'installation minimale de Windows Server ne peut pas exécuter les outils d'administration graphiques tels que Utilisateurs et ordinateurs Active Directory. Toutefois, vous pouvez utiliser des outils en ligne de commande sur l'installation minimale.

Remarque : Vous pouvez administrer l'installation minimale à distance à l'aide des outils graphiques.

Qu'est-ce que Csvde ?

Csvde est un outil en ligne de commande qui exporte ou importe des objets Active Directory dans ou à partir d'un fichier de valeurs séparées par une virgule (.csv). De nombreuses applications sont capables d'exporter ou d'importer des données à partir de fichiers .csv. Csvde est alors utile pour l'interopérabilité avec d'autres applications, telles que les bases de données ou les feuilles de calcul.



La principale limite de csvde est qu'il ne peut pas modifier les objets Active Directory existants. Il ne peut que créer de nouveaux objets. Par exemple, vous pouvez utiliser csvde pour créer un ensemble de nouveaux comptes d'utilisateurs, mais vous ne pouvez pas l'utiliser pour modifier les propriétés de comptes d'utilisateurs après leur création. Vous pouvez également l'utiliser pour exporter des propriétés d'objet, telles qu'une liste d'utilisateurs et de leurs adresses de messagerie.

Exporter des objets à l'aide de csvde

Pour exporter des objets à l'aide de csvde, vous devez, au minimum, spécifier le nom du fichier .csv vers lequel les données seront exportées. Avec uniquement le nom de fichier spécifié, tous les objets du domaine seront exportés.

La syntaxe de base permettant d'utiliser csvde pour l'exportation est la suivante :

```
csvde -f filename
```

Les autres options que vous pouvez utiliser avec csvde sont répertoriées dans le tableau suivant.

Option	Description
-d RootDN	Spécifie le nom unique du conteneur à partir duquel l'exportation commencera. La valeur par défaut est le domaine.
-p SearchScope	Spécifie l'étendue de recherche relative au conteneur spécifié par l'option **-d**. L'option **SearchScope** peut avoir la valeur base (cet objet uniquement), **onelevel** (objets de ce conteneur) ou **subtree** (ce conteneur et tous les sous-conteneurs). La valeur par défaut est **subtree**.
-r Filter	Limite les objets retournés à ceux qui correspondent au filtre. Le filtre est basé sur la syntaxe de requête du protocole LDAP (Lightweight Directory Access Protocol).
-l ListOfAtrributes	Spécifie les attributs à exporter. Utilisez le nom LDAP pour chaque attribut et séparez-les par une virgule.

Une fois l'exportation terminée, le fichier .csv contient une ligne d'en-tête et une ligne pour chaque objet exporté. La ligne d'en-tête est une liste contenant les noms des attributs de chaque objet, séparés par une virgule.

Créer des objets à l'aide de csvde

La syntaxe de base permettant d'utiliser csvde pour créer des objets est la suivante :

```
csvde -i -f filename -k
```

Le paramètre **-i** spécifie le mode d'importation. Le paramètre **-f** identifie le nom de fichier à partir duquel l'importation s'effectue. Le paramètre **-k** indique à csvde d'ignorer les messages d'erreur, y compris le message « L'objet existe déjà ». L'option **Supprimer les erreurs** est utile lors de l'importation des objets pour vous assurer que tous les objets possibles sont créés et éviter un arrêt si elle n'est pas complètement terminée.

Le fichier .csv utilisé pour une importation doit avoir une ligne d'en-tête contenant les noms des attributs LDAP des données du fichier .csv. Chaque ligne doit contenir précisément le nombre exact d'éléments tel que spécifié dans la ligne d'en-tête.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

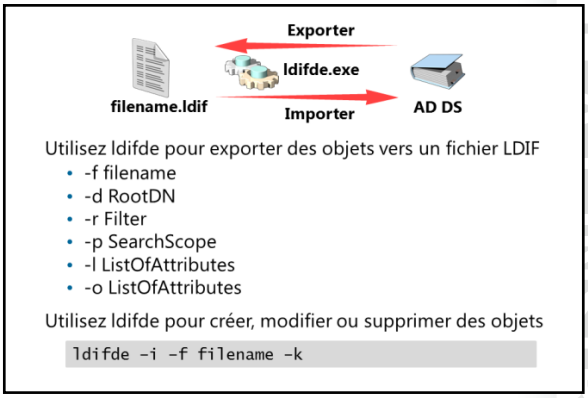
Vous ne pouvez pas utiliser csvde pour importer des mots de passe, car les mots de passe d'un fichier .csv ne sont pas protégés. Par conséquent, les comptes d'utilisateurs crées avec csvde ont un mot de passe vide et sont désactivés.

Remarque : Pour plus d'informations sur les paramètres de csvde, à l'invite de commandes, tapez **csvde / ?**, puis appuyez sur Entrée.

Documentation supplémentaire : Pour plus d'informations sur la syntaxe de requête LDAP, consultez les principes de requête LDAP à l'adresse http://go.microsoft.com/fwlink/?LinkId=168752.

Qu'est-ce que Ldifde ?

Ldifde est un outil en ligne de commande que vous pouvez utiliser pour exporter, créer, modifier ou supprimer des objets AD DS. Comme csvde, ldifde utilise les données enregistrées dans un fichier. Le fichier doit être au format LDIF (LDAP Data Interchange Format). La plupart des applications ne peuvent pas exporter ou importer des données au format LDIF. Vous obtiendrez probablement des données au format LDIF à partir d'un autre service d'annuaire.



Un fichier LDIF est un fichier texte qui contient des blocs de lignes composant une opération unique telle la création ou la modification d'un objet utilisateur. Chaque ligne de l'opération spécifie quelque chose au sujet de l'opération, par exemple un attribut ou le type d'opération. Une ligne vierge sépare plusieurs opérations du fichier LDIF.

Vous trouverez ci-dessous un exemple de fichier LDIF qui crée un simple utilisateur :

```
dn: CN=Bonnie Kearney,OU=Employees,OU=User Accounts,DC=adatum,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Bonnie Kearney
sn: Kearney
title: Opérations
description: Operations (London)
givenName: Bonnie
displayName: Kearney, Bonnie
company: Contoso, Ltd.
sAMAccountName: bonnie.kearney
userPrincipalName: bonnie.kearney@adatum.com
mail: bonnie.kearney@adatum.com
```

Pour chaque opération d'un fichier LDIF, la ligne **changetype** définit l'opération à effectuer. Les valeurs valides sont **add**, **modify** ou **delete**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exporter des objets à l'aide de Ldifde

Lorsque vous utilisez ldifde pour exporter des objets, vous devez fournir au minimum un nom de fichier pour contenir les données. Lorsqu'aucune autre option n'est sélectionnée, tous les objets du domaine sont exportés.

La syntaxe de base pour l'exportation des objets à l'aide de LDIFE est la suivante :

```
ldifde -f filename
```

Certaines des autres options que vous pouvez utiliser lors de l'exportation des objets sont répertoriées dans le tableau suivant.

Option	Description
-d RootDN	Racine de la recherche LDAP. La valeur par défaut est la racine du domaine.
-r Filter	Filtre de recherche LDAP qui limite les résultats retournés.
-p SearchScope	Étendue ou intensité de la recherche. Valeur possible : • **subtree** (conteneur et tous les conteneurs enfants) ; • **base** (objets enfants immédiats du conteneur uniquement) ; • **onelevel** (conteneur et ses conteneurs enfants immédiats).
-l ListOfAttributes	Liste d'attributs à inclure dans l'exportation, séparés par une virgule.
-o ListOfAttributes	Liste d'attributs à exclure de l'exportation, séparés par une virgule.

Importer des objets à l'aide de Ldifde

Lorsque vous utilisez ldifde pour importer des objets, vous devez spécifier l'opération à effectuer sur l'objet. Pour chaque opération d'un fichier LDIF, la ligne **changetype** définit l'opération à effectuer.

La syntaxe de base permettant d'utiliser ldifde pour importer des objets est la suivante :

```
ldifde -i -f filename -k
```

Le paramètre **-i** spécifie le mode d'importation. Le paramètre **-f** identifie le nom de fichier à partir duquel l'importation s'effectue. Le paramètre **-k** indique à ldifde d'ignorer les erreurs, y compris l'erreur « *L'objet existe déjà* ». L'option **Supprimer les erreurs** est utile lors de l'importation des objets pour vous assurer que tous les objets possibles sont créés et éviter un arrêt si elle n'est pas complètement terminée.

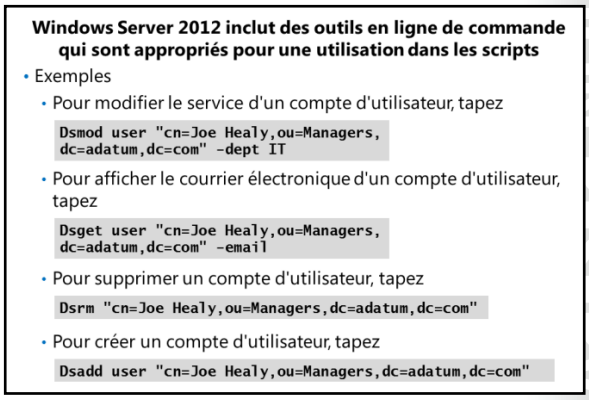
Vous ne pouvez pas utiliser ldifde pour importer des mots de passe, car le fichier LDIF ne serait pas sécurisé. Par conséquent, les comptes d'utilisateurs créés par ldifde ont un mot de passe vide et sont désactivés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que les commandes DS ?

Windows Server 2012 inclut des outils en ligne de commande, appelés *commandes DS*, qui sont appropriées pour une utilisation dans les scripts. Vous pouvez utiliser les outils en ligne de commande DS pour créer, afficher, modifier et supprimer des objets AD DS. Le tableau suivant décrit les outils en ligne de commande DS.



Outil	Description
DSadd	Crée des objets AD DS.
DSget	Affiche les propriétés des objets AD DS.
DSquery	Recherche les objets AD DS.
DSmod	Modifie les objets AD DS.
DSrm	Supprime les objets AD DS.
DSmove	Déplace les objets AD DS.

Exemples de commandes de gestion des utilisateurs

Vous trouverez ci-dessous des exemples de commandes DS que vous pouvez taper à l'invite de commandes.

Pour modifier le service d'un compte d'utilisateur, tapez :

```
dsmod user "cn=Joe Healy,ou=Managers,dc=adatum,dc=com" -dept IT
```

Pour afficher le courrier électronique d'un compte d'utilisateur, tapez :

```
dsget user "cn=Joe Healy,ou=Managers,dc=adatum,dc=com" -email
```

Pour supprimer un compte d'utilisateur, tapez :

```
dsrm "cn=Joe Healy,ou=Managers,dc=adatum,dc=com"
```

Pour créer un compte d'utilisateur, tapez :

```
dsadd user "cn=Joe Healy,ou=Managers,dc=adatum,dc=com"
```

Question : Quels critères utiliseriez-vous pour choisir d'opter pour csvde, ldifde ou les commandes DS ?

Leçon 2
Utilisation de Windows PowerShell pour l'administration d'AD DS

Windows PowerShell est l'environnement d'écriture de scripts par défaut de Windows Server 2012. Il est beaucoup plus facile à utiliser que les langages de script précédents tels que Microsoft® Visual Basic Scripting Edition (VBScript). Windows PowerShell inclut une liste étendue d'applets de commande pour gérer les objets AD DS. Vous pouvez utiliser des applets de commande pour créer, modifier et supprimer des comptes d'utilisateurs, des groupes, des comptes d'ordinateurs et des unités d'organisation (OU).

Objectifs de la leçon

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

- utiliser les applets de commande Windows PowerShell pour gérer les comptes d'utilisateurs ;
- utiliser les applets de commande Windows PowerShell pour gérer les groupes ;
- utiliser les applets de commande Windows PowerShell pour gérer les comptes d'ordinateurs ;
- utiliser les applets de commande Windows PowerShell pour gérer les unités d'organisation.

Utilisation des applets de commande Windows PowerShell pour gérer les comptes d'utilisateurs

Vous pouvez utiliser les applets de commande Windows PowerShell pour créer, modifier et supprimer des comptes d'utilisateurs. Ces applets de commande peuvent être utilisées pour des opérations différentes ou dans le cadre d'un script permettant d'exécuter des opérations en bloc.

Certaines des applets de commande permettant de gérer des comptes d'utilisateurs se trouvent dans le tableau suivant.

Applet de commande	Description
New-ADUser	Crée des comptes d'utilisateurs
Set-ADUser	Modifie les propriétés des comptes d'utilisateurs
Remove-ADUser	Supprime des comptes d'utilisateurs
Set-ADAccountPassword	Réinitialise le mot de passe d'un compte d'utilisateur
Set-ADAccountExpiration	Modifie la date d'expiration d'un compte d'utilisateur
Unlock-ADAccount	Déverrouille un compte d'utilisateur après qu'il soit devenu verrouillé après que trop de tentatives incorrectes d'ouverture de session
Enable-ADAccount	Active un compte d'utilisateur
Disable-ADAccount	Désactive un compte d'utilisateur

```
New-ADUser "Sten Faerch" -AccountPassword (Read-Host
-AsSecureString "Enter password") -Department IT
```

Applet de commande	Description
New-ADUser	Crée des comptes d'utilisateurs.
Set-ADUser	Modifie les propriétés des comptes d'utilisateurs.
Remove-ADUser	Supprime des comptes d'utilisateurs.
Set-ADAccountPassword	Réinitialise le mot de passe d'un compte d'utilisateur.
Set-ADAccountExpiration	Modifie la date d'expiration d'un compte d'utilisateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Applet de commande	Description
Unlock-ADAccount	Déverrouille un compte d'utilisateur lorsqu'il a été verrouillé après le dépassement du nombre autorisé de tentatives incorrectes d'ouverture de session.
Enable-ADAccount	Active un compte d'utilisateur.
Disable-ADAccount	Désactive un compte d'utilisateur.

Créer des comptes d'utilisateurs

Lorsque vous utilisez l'applet de commande **New-ADUser** pour créer des comptes d'utilisateurs, vous pouvez définir la plupart des propriétés d'utilisateur, y compris un mot de passe. Par exemple :

- Si vous n'utilisez pas le paramètre **-AccountPassword**, aucun mot de passe n'est défini et le compte d'utilisateur est désactivé. Le paramètre **-Enabled** ne peut pas être défini comme **$true** lorsqu'aucun mot de passe n'est défini.
- Si vous utilisez le paramètre **-AccountPassword** pour spécifier un mot de passe, vous devez alors spécifier une variable qui contient le mot de passe sous forme de chaîne sécurisée ou choisir d'être invité à entrer le mot de passe. Une chaîne sécurisée est chiffrée dans la mémoire. Si vous avez défini un mot de passe, vous pouvez alors activer le compte d'utilisateur en donnant au paramètre **-Enabled** la valeur **$true**.

Certains paramètres couramment utilisés pour l'applet de commande **New-ADUser** sont répertoriés dans le tableau suivant.

Paramètre	Description
AccountExpirationDate	Définit la date d'expiration du compte d'utilisateur.
AccountPassword	Définit le mot de passe du compte d'utilisateur.
ChangePasswordAtLogon	Requiert le compte d'utilisateur pour modifier les mots de passe à la prochaine connexion.
Service	Définit le service du compte d'utilisateur.
Activé	Définit si le compte d'utilisateur est activé ou désactivé.
HomeDirectory	Définit l'emplacement du répertoire de base d'un compte d'utilisateur.
HomeDrive	Définit les lettres de lecteur mappées au répertoire de base d'un compte d'utilisateur.
GivenName	Définit le prénom d'un compte d'utilisateur.
Surname	Définit le nom d'un compte d'utilisateur.
Chemin d'accès	Définit l'unité d'organisation ou le conteneur dans lequel le compte d'utilisateur est créé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous trouverez ci-dessous un exemple de commande que vous pouvez utiliser pour créer un compte d'utilisateur avec une invite vous demandant d'entrer un mot de passe :

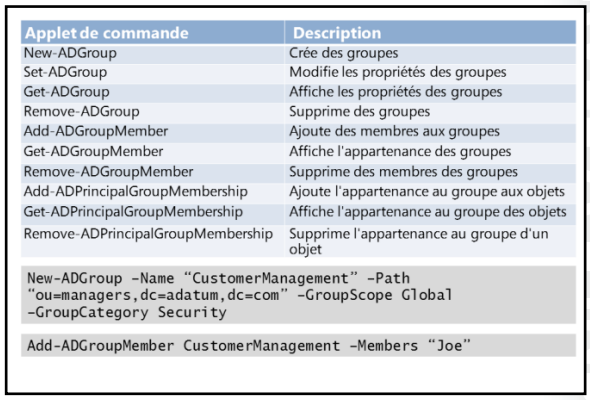
```
New-ADUser "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Entrez le mot de passe")  -Department IT
```

Question : Les paramètres des applets de commande que vous utilisez pour gérer les comptes d'utilisateurs sont-ils identiques ?

Utilisation des applets de commande Windows PowerShell pour gérer les groupes

Vous pouvez utiliser les applets de commande Windows PowerShell pour créer, modifier et supprimer des groupes. Ces applets de commande peuvent être utilisées pour des opérations différentes ou dans le cadre d'un script permettant d'exécuter des opérations en bloc.

Certaines des applets de commande permettant de gérer les groupes se trouvent dans le tableau suivant.



Applet de commande	Description
New-ADGroup	Crée des groupes.
Set-ADGroup	Modifie les propriétés des groupes.
Get-ADGroup	Affiche les propriétés des groupes.
Remove-ADGroup	Supprime des groupes.
Add-ADGroupMember	Ajoute des membres aux groupes.
Get-ADGroupMember	Affiche l'appartenance des groupes.
Remove-ADGroupMember	Supprime des membres des groupes.
Add-ADPrincipalGroupMembership	Ajoute l'appartenance au groupe aux objets.
Get-ADPrincipalGroupMembership	Affiche l'appartenance au groupe des objets.
Remove-ADPrincipalGroupMembership	Supprime l'appartenance au groupe d'un objet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Créer des groupes

Vous pouvez utiliser l'applet de commande **New-ADGroup** pour créer des groupes. Toutefois, lorsque vous créez des groupes à l'aide de l'applet de commande **New-ADGroup**, vous devez utiliser le paramètre **GroupScope** en plus du nom de groupe. C'est le seul paramètre requis. Le tableau suivant répertorie les paramètres couramment utilisés pour **New-ADGroup**.

Paramètre	Description
Nom	Définit le nom du groupe.
GroupScope	Définit l'étendue du groupe comme **DomainLocal**, **Global** ou **Universal**. Vous devez fournir ce paramètre.
DisplayName	Définit le nom complet LDAP de l'objet.
GroupCategory	Définit s'il s'agit d'un groupe de sécurité ou d'un groupe de distribution. Si vous n'en spécifiez aucun, un groupe de sécurité est créé.
ManagedBy	Définit un utilisateur ou un groupe qui peut gérer le groupe.
Chemin d'accès	Définit l'unité d'organisation ou le conteneur dans laquelle ou lequel le groupe est créé.
SamAccountName	Définit un nom qui a une compatibilité descendante avec les systèmes d'exploitation plus anciens.

La commande suivante est un exemple de ce que vous pouvez taper à une invite Windows PowerShell pour créer un groupe :

```
New-ADGroup -Name "CustomerManagement" -Path "ou=managers,dc=adatum,dc=com" -GroupScope
Global -GroupCategory Security
```

Gérer l'appartenance au groupe

Il existe deux ensembles d'applets de commande que vous pouvez utiliser pour gérer l'appartenance au groupe : ***-ADGroupMember** et ***-ADPrincipalGroupMembership**. La distinction entre ces deux ensembles d'applets de commande est la perspective utilisée lors de la modification de l'appartenance au groupe. Les voici :

- Les applets de commande ***-ADGroupMember** modifient l'appartenance à un groupe. Par exemple, vous ajoutez ou supprimez des membres d'un groupe.
  - Vous ne pouvez pas diffuser une liste de membres dans ces applets de commande.
  - Vous pouvez passer une liste de groupes à ces applets de commande.
- Les applets de commande ***-ADPrincipalGroupMembership** modifient l'appartenance au groupe d'un objet, tel qu'un utilisateur. Par exemple, vous pouvez modifier un compte d'utilisateur pour l'ajouter en tant que membre d'un groupe.
  - Vous pouvez diffuser une liste de membres dans ces applets de commande.
  - Vous ne pouvez pas fournir une liste de groupes à ces applets de commande.

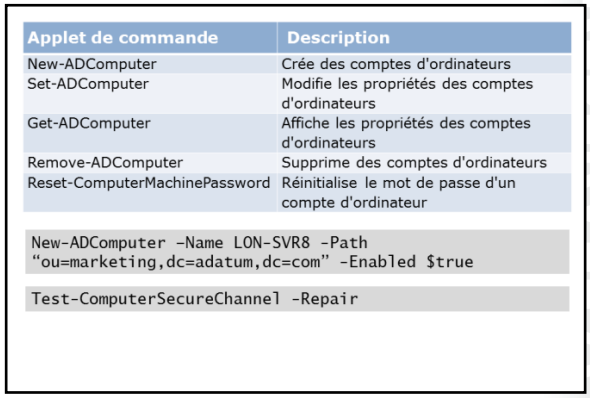
Remarque : Lorsque vous publiez une liste d'objets dans une applet de commande, vous passez une liste d'objets à une applet de commande.

Vous trouverez ci-dessous un exemple de commande à utiliser pour ajouter un membre à un groupe :

```
Add-ADGroupMember CustomerManagement -Members "Joe"
```

Utilisation des applets de commande Windows PowerShell pour gérer les comptes d'ordinateurs

Vous pouvez utiliser les applets de commande Windows PowerShell pour créer, modifier et supprimer des comptes d'ordinateurs. Ces applets de commande peuvent être utilisées pour des opérations différentes ou dans le cadre d'un script permettant d'exécuter des opérations en bloc. Certaines des applets de commande permettant de gérer les comptes d'ordinateurs se trouvent dans le tableau suivant.



Applet de commande	Description
New-ADComputer	Crée un compte d'ordinateur.
Set-ADComputer	Modifie les propriétés d'un compte d'ordinateur.
Get-ADComputer	Affiche les propriétés d'un compte d'ordinateur.
Remove-ADComputer	Supprime un compte d'ordinateur.
Test-ComputerSecureChannel	Vérifie ou répare la relation d'approbation entre un ordinateur et le domaine.
Reset-ComputerMachinePassword	Réinitialise le mot de passe d'un compte d'ordinateur.

Créer des comptes d'ordinateurs

Vous pouvez utiliser l'applet de commande **New-ADComputer** pour créer un compte d'ordinateur avant de joindre l'ordinateur au domaine. Si vous procédez ainsi, vous pouvez créer le compte d'ordinateur dans l'unité d'organisation appropriée avant de déployer l'ordinateur.

Le tableau suivant répertorie les paramètres couramment utilisés pour **New-ADComputer**.

Paramètre	Description
Nom	Définit le nom d'un compte d'ordinateur.
Chemin d'accès	Définit l'unité d'organisation ou le conteneur dans lequel le compte d'ordinateur sera créé.
Activé	Définit si le compte d'ordinateur est activé ou désactivé. Par défaut, le compte d'ordinateur est activé et un mot de passe aléatoire est généré.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Voici un exemple de script que vous pouvez utiliser pour créer un compte d'ordinateur :

```
New-ADComputer -Name LON-SVR8 -Path "ou=marketing,dc=adatum,dc=com" -Enabled $true
```

Réparer la relation d'approbation d'un compte d'ordinateur

Vous pouvez utiliser l'applet de commande **Test-ComputerSecureChannel** avec le paramètre **-Repair** pour réparer une relation d'approbation perdue entre un ordinateur et le domaine. Vous devez exécuter l'applet de commande sur l'ordinateur avec la relation d'approbation perdue.

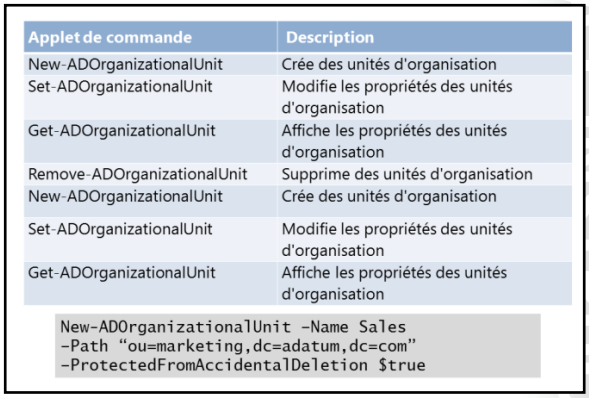
Vous pouvez utiliser la commande suivante pour réparer la relation d'approbation d'un compte d'ordinateur :

```
Test-ComputerSecureChannel -Repair
```

Utilisation des applets de commande Windows PowerShell pour gérer les unités d'organisation

Vous pouvez utiliser les applets de commande Windows PowerShell pour créer, modifier et supprimer des unités d'organisation. Ces applets de commande peuvent être utilisées pour des opérations différentes ou dans le cadre d'un script permettant d'exécuter des opérations en bloc.

Certaines des applets de commande permettant de gérer les unités d'organisation sont répertoriées dans le tableau suivant.



Applet de commande	Description
New-ADOrganizationalUnit	Crée des unités d'organisation.
Set-ADOrganizationalUnit	Modifie les propriétés des unités d'organisation.
Get-ADOrganizationalUnit	Affiche les propriétés des unités d'organisation.
Remove-ADOrganizationalUnit	Supprime des unités d'organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Créer des unités d'organisation

Vous pouvez utiliser l'applet de commande **New-ADOrganizationalUnit** permettant de créer une unité d'organisation pour représenter des services ou des emplacements physiques au sein de votre organisation.

Les paramètres couramment utilisés pour l'applet de commande **New-ADOrganizationalUnit** sont répertoriés dans le tableau suivant.

Paramètre	Description
Nom	Définit le nom d'une nouvelle unité d'organisation.
Chemin d'accès	Définit l'emplacement d'une nouvelle unité d'organisation.
ProtectedFromAccidentalDeletion	Permet d'empêcher la suppression accidentelle de l'unité d'organisation. La valeur par défaut est **$true**.

Voici un exemple de script que vous pouvez utiliser si vous voulez créer une unité d'organisation :

```
New-ADOrganizationalUnit -Name Sales -Path "ou=marketing,dc=adatum,dc=com" -
ProtectedFromAccidentalDeletion $true
```

Question : Dans l'exemple de la diapositive, le paramètre **ProtectedFromAccidentalDeletion** est-il requis ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Exécution d'opérations en bloc avec Windows PowerShell

Windows PowerShell est un environnement d'écriture de scripts puissant que vous pouvez utiliser pour exécuter des opérations en bloc, normalement fastidieuses à exécuter manuellement. Vous pouvez également exécuter quelques opérations en bloc dans les outils graphiques.

Pour exécuter des opérations en bloc à l'aide de Windows PowerShell, vous devez d'abord savoir comment créer des requêtes pour une liste d'objets AD DS et comment travailler avec des fichiers .csv. Vous pouvez alors créer des scripts qui exécutent les opérations en bloc requises.

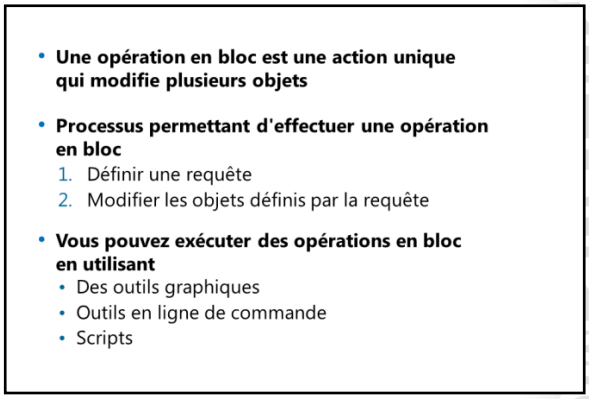
Objectifs de la leçon

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

- décrire les opérations en bloc ;
- utiliser les outils graphiques pour exécuter des opérations en bloc ;
- interroger les objets AD DS à l'aide de Windows PowerShell ;
- modifier les objets AD DS à l'aide de Windows PowerShell ;
- utiliser les fichiers .csv avec Windows PowerShell ;
- modifier et exécuter les scripts Windows PowerShell pour exécuter des opérations en bloc.

Que sont les opérations en bloc ?

Une *opération en bloc* est une action unique qui modifie plusieurs objets. L'exécution d'une opération en bloc est beaucoup plus rapide que la modification de plusieurs objets individuellement. Elle peut également être plus précise, car l'exécution de nombreuses actions individuelles augmente les risques d'erreur typographique.



Le processus général d'exécution des opérations en bloc est le suivant :

1. Définir une requête. Vous utilisez la requête pour sélectionner les objets que vous souhaitez modifier. Par exemple, vous pouvez souhaiter modifier tous les comptes d'utilisateurs dans une unité d'organisation spécifique.
2. Modifier les objets définis par la requête. À l'aide des outils graphiques, vous sélectionnez en général les objets que vous souhaitez modifier, puis vous modifiez les propriétés de ces objets. À l'aide des outils en ligne de commande, vous pouvez utiliser une liste d'objets ou de variables pour identifier les objets à modifier.

Vous pouvez exécuter des opérations en bloc avec les outils graphiques, à une invite de commandes, ou à l'aide de scripts. Chaque méthode d'exécution d'opérations en bloc possède des fonctionnalités différentes.

Par exemple :

- Les outils graphiques ont tendance à se limiter aux propriétés qu'ils peuvent modifier.
- Les outils en ligne de commande ont tendance à être plus flexibles que les outils graphiques lors de la définition des requêtes. Ils disposent de plus d'options pour modifier les propriétés d'objet.
- Les scripts peuvent combiner plusieurs actions de ligne de commande pour répondre à plus de complexité et de flexibilité.

Démonstration : Utilisation des outils graphiques pour exécuter des opérations en bloc

Vous pouvez utiliser le Centre d'administration Active Directory d'outils graphiques et le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory pour modifier les propriétés de plusieurs objets simultanément.

Remarque : Lorsque vous utilisez les outils graphiques pour modifier plusieurs comptes d'utilisateurs simultanément, vous pouvez uniquement modifier les propriétés qui s'affichent dans l'interface utilisateur.

Pour exécuter une opération en bloc à l'aide des outils graphiques, procédez comme suit :

1. Effectuez une recherche ou créez un filtre pour afficher les objets que vous souhaitez modifier.
2. Sélectionnez les objets.
3. Examinez les propriétés des objets.
4. Modifiez les propriétés souhaitées.

Dans cette démonstration, vous allez apprendre à :

- créer une requête pour tous les utilisateurs ;
- configurer l'attribut Company pour tous les utilisateurs ;
- vérifier que l'attribut Company a été modifié.

Procédure de démonstration

Créer une requête pour tous les utilisateurs

1. Démarrez **22410B-LON-DC1** et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-DC1, ouvrez le **Centre d'administration Active Directory**.
3. Accédez à la Recherche globale et ajoutez les critères **Object type is user/inetOrgPerson/computer/group/organization unit**.
4. Vérifiez que les critères que vous avez ajoutés sont de type **Utilisateur** et effectuez la recherche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configurer l'attribut Company pour tous les utilisateurs

1. Sélectionnez tous les comptes d'utilisateurs et modifiez leurs propriétés.
2. Tapez **A. Datum** comme nom de société.

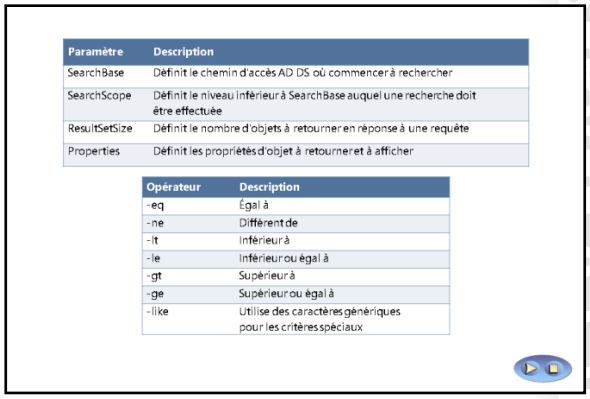
Vérifier que l'attribut Company a été modifié

- Ouvrez les propriétés d'Adam Barr et vérifiez que la société est A. Datum.

Interrogation d'objets avec Windows PowerShell

Dans Windows PowerShell, vous utilisez les applets de commande **Get-*** pour obtenir des listes d'objets, tels que des comptes d'utilisateurs. Vous pouvez également utiliser ces applets de commande pour générer des requêtes pour des objets sur lesquels vous pouvez exécuter des opérations en bloc.

Le tableau suivant répertorie les paramètres couramment utilisés avec les applets de commande **Get-AD***.



Paramètre	Description
SearchBase	Définit le chemin d'accès AD DS pour commencer à rechercher, par exemple, le domaine ou une unité d'organisation.
SearchScope	Définit le niveau inférieur à **SearchBase** auquel une recherche doit être effectuée. Vous pouvez choisir de rechercher uniquement dans la base, un niveau en dessous ou dans l'ensemble de la sous-arborescence.
ResultSetSize	Définit le nombre d'objets à retourner en réponse à une requête. Pour vérifier que tous les objets sont retournés, vous devez lui affecter la valeur **$null**.
Propriétés	Définit les propriétés d'objet à retourner et à afficher. Pour retourner toutes les propriétés, tapez un astérisque (*). Vous n'avez pas besoin d'employer ce paramètre afin d'utiliser une propriété pour le filtrage.

Créer une requête

Vous pouvez utiliser le paramètre **Filter** ou **LDAPFilter** pour créer des requêtes pour les objets avec les applets de commande **Get-AD***. Le paramètre **Filter** est utilisé pour des requêtes écrites dans Windows PowerShell. Le paramètre **LDAPFilter** est utilisé pour des requêtes écrites sous forme de chaînes de requête LDAP.

Windows PowerShell est à privilégier pour les raisons suivantes :

- Il est plus facile d'écrire des requêtes dans Windows PowerShell.
- Vous pouvez utiliser des variables dans les requêtes.
- Une conversion automatique des types de variables se produit, lorsque cela est nécessaire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le tableau suivant répertorie les opérateurs couramment utilisés que vous pouvez utiliser dans Windows PowerShell.

Opérateur	Description
-eq	Égal à
-ne	Différent de
-lt	Inférieur à
-le	Inférieur ou égal à
-gt	Supérieur à
-ge	Supérieur ou égal à
-like	Utilise des caractères génériques pour les critères spéciaux

Vous pouvez utiliser la commande suivante pour afficher toutes les propriétés d'un compte d'utilisateur :

```
Get-ADUser Administrateur -Properties *
```

Vous pouvez utiliser la commande suivante pour retourner tous les comptes d'utilisateurs dans l'unité d'organisation Marketing et toutes ses unités d'organisation enfants :

```
Get-ADUser -Filter * -SearchBase "ou=Marketing,dc=adatum,dc=com" -SearchScope subtree
```

Vous pouvez utiliser la commande suivante pour afficher tous les comptes d'utilisateurs avec une dernière date de connexion antérieure à une date spécifique :

```
Get-ADUser -Filter {lastlogondate -lt "Mars 29, 2013"}
```

Vous pouvez utiliser la commande suivante pour afficher tous les comptes d'utilisateurs du service Marketing qui ont une dernière date de connexion antérieure à une date spécifique :

```
Get-ADUser -Filter {(lastlogondate -lt "Mars 29, 2013") -and (department -eq
"Marketing")}
```

Documentation supplémentaire : Pour plus d'informations sur le filtrage avec les applets de commande **Get AD***, reportez-vous à la rubrique about_ActiveDirectory_Filter à l'adresse http://go.microsoft.com/fwlink/?LinkID=266740.

Question : Quelle est la différence entre l'utilisation de **-eq** et de **-like** lors de la comparaison de chaînes ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Modification d'objets avec Windows PowerShell

Pour exécuter une opération en bloc, vous devez passer la liste d'objets interrogés à une autre applet de commande pour modifier les objets. Dans la plupart des cas, vous utilisez les applets de commande **Set-AD*** pour modifier les objets.

Pour passer la liste des objets interrogés à une autre applet de commande en vue d'un traitement ultérieur, vous utilisez le caractère de barre verticale (|). Le caractère de barre verticale passe chaque objet de la requête à une deuxième applet de commande, qui exécute ensuite une opération spécifiée sur chaque objet.

Utilisez le caractère de barre verticale (|) pour passer une liste des objets à une applet de commande en vue d'un traitement ultérieur

```
Get-ADUser -Filter {company -notlike "*"} |
Set-ADUser -Company "A. Datum"
```

```
Get-ADUser -Filter {lastlogondate -lt "Mars 29,
2013"} | Disable-ADAccount
```

```
Get-Content C:\users.txt | Disable-ADAccount
```

Vous pouvez utiliser la commande suivante pour ces comptes dont l'attribut Company n'est pas défini. Elle génèrera une liste de comptes d'utilisateurs et donnera à l'attribut Company la valeur **A. Datum**.

```
Get-ADUser -Filter {company -notlike "*"} | Set-ADUser -Company "A. Datum"
```

Vous pouvez utiliser la commande suivante pour générer une liste de comptes d'utilisateurs qui n'ont pas ouvert de session depuis une date spécifique, puis les désactiver :

```
Get-ADUser -Filter {(lastlogondate -lt "Mars 29, 2013") -and (department -eq
"Marketing")}
```

Utiliser des objets à partir d'un fichier texte

Au lieu d'utiliser une liste d'objets à partir d'une requête pour effectuer une opération en bloc, vous pouvez utiliser une liste d'objets dans un fichier texte. Cela s'avère particulièrement utile lorsque vous devez modifier ou supprimer une liste d'objets et qu'il n'est pas possible de générer cette liste à l'aide d'une requête. Par exemple, le service des ressources humaines peut générer une liste de comptes d'utilisateurs à désactiver. Aucune requête ne peut identifier une liste d'utilisateurs qui ont quitté l'organisation.

Lorsque vous utilisez un fichier texte pour spécifier une liste d'objets, le fichier texte doit comporter le nom de chaque objet sur une seule ligne.

Vous pouvez utiliser la commande suivante pour désactiver les comptes d'utilisateurs répertoriés dans un fichier texte :

```
Get Content C:\users.txt | Disable ADAccount
```

Question : Quels attributs de compte d'utilisateur pouvez-vous utiliser lors de la création d'une requête à l'aide du paramètre **Filter** ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Utilisation des fichiers CSV

Un fichier .csv peut contenir beaucoup plus d'informations qu'une liste simple. Semblable à une feuille de calcul, un fichier .csv peut comporter plusieurs lignes et colonnes d'informations. Chaque ligne représente un objet unique et chaque colonne représente une propriété de l'objet. Cela s'avère utile pour les opérations en bloc telles que la création de comptes d'utilisateurs pour lesquelles plusieurs éléments d'information sur chaque objet sont requis.

La première ligne d'un fichier .csv définit les noms des colonnes

```
FirstName,LastName,Department
Greg,Guzik,Informatique
Robin,Young,Recherche
Qiong,Wu,Marketing
```

Une boucle Foreach traite le contenu d'un fichier .csv qui a été importé dans une variable

```
$users=Import-CSV C:\users.csv
Foreach ($i in $users) {
     Write-Host “The first name is:” $i.FirstName
     }
```

Vous pouvez utiliser l'applet de commande **Import-CSV** pour lire le contenu d'un fichier .csv dans une variable, puis utiliser les données. Après l'importation des données dans la variable, vous pouvez vous reporter à chaque ligne et à chaque colonne individuelles de données. Chaque colonne de données porte un nom qui est basé sur la ligne d'en-tête (première ligne) du fichier .csv. Vous pouvez vous reporter à chaque colonne en fonction de leur nom.

Vous trouverez ci-dessous un exemple de fichier .csv avec une ligne d'en-tête :

```
FirstName,LastName,Department
Greg,Guzik,Informatique
Robin,Young,Recherche
Qiong,Wu,Marketing
```

Utiliser Foreach pour traiter les données CSV

Dans de nombreux cas, vous créez le script qui sera réutilisé pour plusieurs fichiers .csv et vous ne connaissez pas le nombre de lignes de chaque fichier .csv. Vous pouvez utiliser une boucle **foreach** pour traiter chaque ligne d'un fichier .csv. Ce type de boucle ne requiert pas de connaître le nombre de lignes. À chaque itération de la boucle foreach, une ligne du fichier .csv est importée dans une variable qui peut être traitée.

Vous pouvez utiliser la commande suivante pour importer un fichier .csv dans une variable et utiliser une boucle **foreach** pour afficher le prénom de chaque ligne d'un fichier .csv :

```
$users=Import-CSV C:\users.csv
Foreach ($i in $users) {
 Write Host "Le premier nom est :" $i.FirstName
 }
```

Question : Dans la boucle **foreach**, comment la variable **$i** change-t-elle ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Exécution d'opérations en bloc avec Windows PowerShell

Vous pouvez utiliser un script pour combiner plusieurs commandes Windows PowerShell afin d'effectuer des tâches plus complexes. Dans un script, vous utilisez souvent des variables et des boucles pour le traitement des données. Les scripts Windows PowerShell possède une extension .ps1.

La stratégie d'exécution sur un serveur détermine si les scripts peuvent s'exécuter. La stratégie d'exécution par défaut sur Windows Server 2012 est **RemoteSigned**. Cela signifie que les scripts locaux peuvent s'exécuter sans être signés numériquement. Vous pouvez contrôler la stratégie d'exécution à l'aide de l'applet de commande **Set-ExecutionPolicy**.

Dans cette démonstration, vous allez apprendre à :

- configurer un service pour des utilisateurs ;
- créer une unité d'organisation ;
- exécuter un script de création de comptes d'utilisateurs ;
- vérifier que de nouveaux comptes d'utilisateurs ont bien été créés.

Procédure de démonstration

Configurer un service pour des utilisateurs

1. Démarrez 22410B-LON-DC1 et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-DC1, ouvrez une invite Windows PowerShell.
3. À l'invite Windows PowerShell, recherchez les comptes d'utilisateurs dans l'unité d'organisation Research à l'aide de la commande suivante :

```
Get-ADUser –Filter * -SearchBase "ou=Research,dc=adatum,dc=com"
```

4. Définissez l'attribut de service de tous les utilisateurs dans l'unité d'organisation Research à l'aide de la commande suivante :

```
Get-ADUser –Filter * -SearchBase "ou=Research,dc=adatum,dc=com" | Set-ADUser -
Department Research
```

5. Affichez une liste sous forme de tableau des utilisateurs du service Research. Affichez le nom unique et le service à l'aide de la commande suivante :

```
Get-ADUser –Filter 'department -eq "Research"' | Format-Table
DistinguishedName,Department
```

6. Utilisez le paramètre **Properties** pour permettre à la commande précédente d'afficher le service correctement. Utilisez la commande suivante :

```
Get-ADUser –Filter 'department -eq "Research"' -Properties Department | Format-Table
DistinguishedName,Department
```

Créer une unité d'organisation

- À l'invite Windows PowerShell, créez une unité d'organisation nommée **LondonBranch** à l'aide de la commande :

```
New-ADOrganizationalUnit LondonBranch -Path "dc=adatum,dc=com"
```

Exécuter un script de création de comptes d'utilisateurs

1. Ouvrez **E:\Labfiles\Mod04\DemoUsers.csv** et lisez la ligne d'en-tête.
2. Modifiez **DemoUsers.ps1** et examinez le contenu du script. Notez que le script :
   - fait référence à l'emplacement du fichier .csv ;
   - utilise une boucle **foreach** pour traiter le contenu du fichier .csv ;
   - fait référence aux colonnes définies par l'en-tête du fichier .csv.
3. À l'invite Windows PowerShell, modifiez le répertoire **E:\Labfiles\Mod04**, puis exécutez la commande suivante **:**

```
.\DemoUsers.ps1
```

Vérifier que de nouveaux comptes d'utilisateurs ont bien été créés

1. Dans le Gestionnaire de serveur, ouvrez le **Centre d'administration Active Directory**.
2. Dans le Centre d'administration Active Directory, accédez à **Adatum (local)>LondonBranch** et vérifiez que les comptes d'utilisateurs ont bien été créés. Notez que les mots de passe sont désactivés, car aucun mot de passe n'a été défini lors de la création.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Automatisation de l'administration d'AD DS à l'aide de Windows PowerShell

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

Vous avez travaillé pour A. Datum pendant plusieurs années en tant que spécialiste du support technique. À ce poste, vous avez consulté les ordinateurs de bureau pour résoudre les problèmes d'application et de réseau. Vous avez récemment accepté une promotion au sein de l'équipe d'assistance technique des serveurs. L'une de vos premières missions consiste à configurer le service d'infrastructure pour une nouvelle filiale.

Dans le cadre de la configuration d'une nouvelle filiale, vous devez créer des comptes d'utilisateurs et de groupes. La création de plusieurs utilisateurs avec les outils graphiques est inefficace, vous utiliserez donc Windows PowerShell.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- créer des comptes d'utilisateurs et de groupes à l'aide de Windows PowerShell ;
- utiliser Windows PowerShell pour créer des comptes d'utilisateurs en bloc ;
- utiliser Windows PowerShell pour modifier des comptes d'utilisateur en bloc.

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-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 **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 3 pour **22410B-LON-CL1**. Ne vous connectez pas à LON-CL1 tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Création de comptes d'utilisateurs et de groupes à l'aide de Windows PowerShell

Scénario

La société A. Datum possède un certain nombre de scripts qui ont été utilisés par le passé pour créer des comptes d'utilisateurs à l'aide des outils en ligne de commande. Tous les nouveaux scripts seront obligatoirement conçus à l'aide de Windows PowerShell. La première étape de la création de scripts consiste à identifier la syntaxe requise pour gérer les objets AD DS dans Windows PowerShell.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un compte d'utilisateur à l'aide de Windows PowerShell
2. Créer un groupe à l'aide de Windows PowerShell

▶ Tâche 1 : Créer un compte d'utilisateur à l'aide de Windows PowerShell

1. Sur LON-DC1, ouvrez une invite Windows PowerShell.
2. À l'invite Windows PowerShell, créez une unité d'organisation nommée **LondonBranch** en tapant la commande suivante :

```
New-ADOrganizationalUnit LondonBranch
```

3. Créez un compte d'utilisateur pour Ty Carlson dans l'unité d'organisation LondonBranch à l'aide de la commande suivante :

```
 New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path
"ou=LondonBranch,dc=adatum,dc=com"
```

4. Remplacez le mot de passe vide du nouveau compte par **Pa$$w0rd** à l'aide de la commande suivante :

```
Set-ADAccountPassword Ty
```

5. Activez le nouveau compte d'utilisateur à l'aide de la commande suivante :

```
Enable-ADAccount Ty
```

6. Sur LON-CL1, connectez-vous en tant que **Ty** à l'aide du mot de passe **Pa$$w0rd**.
7. Vérifiez que la connexion est réussie, puis déconnectez-vous de LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer un groupe à l'aide de Windows PowerShell

1. Sur LON-DC1, à l'invite Windows PowerShell, créez un groupe de sécurité global pour les utilisateurs de la filiale de Londres, à l'aide de la commande suivante :

```
New-ADGroup LondonBranchUsers -Path "ou=LondonBranch,dc=adatum,dc=com" -GroupScope
Global -GroupCategory Security
```

2. À l'invite Windows PowerShell, ajoutez Ty en tant que membre de LondonBranchUsers, à l'aide de la commande suivante :

```
Add-ADGroupMember LondonBranchUsers -Members Ty
```

3. À l'invite Windows PowerShell, confirmez que Ty a été ajouté en tant que membre de LondonBranchUsers, à l'aide de la commande suivante :

```
Get-ADGroupMember LondonBranchUsers
```

Résultats : À la fin de cet exercice, vous devez avoir créé des comptes d'utilisateurs et des groupes à l'aide de Windows PowerShell.

Exercice 2 : Utilisation de Windows PowerShell pour créer des comptes d'utilisateurs en bloc

Scénario

Vous disposez d'un fichier .csv qui contient un grand nombre de nouveaux utilisateurs pour la filiale. Il serait inefficace de créer ces utilisateurs individuellement avec les outils graphiques. Au lieu de cela, vous utiliserez un script Windows PowerShell pour créer les utilisateurs. Une collègue avec une bonne expérience pratique en matière de création de scripts vous a fourni un script qu'elle a créé. Vous devez modifier le script pour qu'il corresponde au format de votre fichier .csv.

Les tâches principales de cet exercice sont les suivantes :

1. Préparer le fichier .csv
2. Préparer le script
3. Exécuter le script

▶ Tâche 1 : Préparer le fichier .csv

1. Sur LON-DC1, lisez le contenu de **E:\Labfiles\Mod04\LabUsers.ps1** pour identifier les conditions requises d'en-tête du fichier .csv.
2. Modifiez le contenu de **C:\Labfiles\Mod04\LabUsers.csv** et ajoutez l'en-tête appropriée.

▶ Tâche 2 : Préparer le script

1. Sur LON-DC1, utilisez l'environnement d'écriture de scripts intégré (ISE) de Windows PowerShell pour modifier les variables de **LabUsers.ps1** :
   - $csvfile: **E:\Labfiles\Mod04\labUsers.csv**
   - $OU: **"ou=LondonBranch,dc=adatum,dc=com"**
2. Enregistrez le LabUsers.ps1 modifié.
3. Examinez le contenu du script.

▶ Tâche 3 : Exécuter le script

1. Sur LON-DC1, ouvrez une invite Windows PowerShell et exécutez **E:\Labfiles\Mod04\LabUsers.ps1**.
2. À l'invite Windows PowerShell, utilisez la commande suivante pour vérifier que les utilisateurs ont bien été créés :

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com"
```

3. Sur LON-CL1, connectez-vous en tant que **Luka** à l'aide du mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir utilisé Windows PowerShell pour créer des comptes d'utilisateurs en bloc.

Exercice 3 : Utilisation de Windows PowerShell pour modifier des comptes d'utilisateurs en bloc

Scénario

Vous avez reçu une demande de mise à jour de tous les comptes d'utilisateurs de l'unité d'organisation de la nouvelle filiale avec l'adresse exacte des nouveaux locaux. Il vous est également demandé de vérifier que tous les nouveaux comptes d'utilisateurs de la filiale sont configurés pour forcer les utilisateurs à changer leur mot de passe à la prochaine connexion.

Les tâches principales de cet exercice sont les suivantes :

1. Forcer tous les comptes d'utilisateurs de LondonBranch à changer leur mot de passe à la prochaine connexion
2. Configurer l'adresse pour les comptes d'utilisateurs de LondonBranch
3. Pour préparer le module suivant

▶ Tâche 1 : Forcer tous les comptes d'utilisateurs de LondonBranch à changer leur mot de passe à la prochaine connexion

1. Sur LON-DC1, ouvrez une invite Windows PowerShell.
2. À l'invite Windows PowerShell, créez une requête pour les comptes d'utilisateurs de l'unité d'organisation LondonBranch à l'aide de la commande suivante :

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com" | Format-Wide
DistinguishedName
```

3. À l'invite Windows PowerShell, modifiez la commande précédente pour forcer tous les comptes d'utilisateurs à changer leur mot de passe à la prochaine connexion à l'aide de la commande suivante :

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com" | Set-ADUser -
ChangePasswordAtLogon $true
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer l'adresse pour les comptes d'utilisateurs de LondonBranch

1. Sur LON-DC1, ouvrez le **Centre d'administration Active Directory**.
2. Ouvrez les propriétés de tous les comptes d'utilisateurs de **LondonBranch**.
3. Définissez l'adresse de plusieurs utilisateurs comme suit :
   - Rue : **Filiale**
   - Ville : **London**
   - Pays/région : **Royaume-Uni**

Résultats : À la fin de cet exercice, vous devez avoir modifié des comptes d'utilisateurs en bloc.

▶ Pour préparer le module suivant

Lorsque vous terminez l'atelier pratique, rétablissez tous les ordinateurs virtuels à leur état initial en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-LON-CL1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22410B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Un collègue crée un script Windows PowerShell qui crée des comptes d'utilisateurs à partir des données d'un fichier .csv. Toutefois, son script génère des erreurs lors de la tentative de définition d'un mot de passe par défaut. Pourquoi cela peut-il se passer ?

Question : Vous êtes administrateur d'une académie qui crée 20 000 comptes d'utilisateurs pour les élèves chaque année. Le système d'administration des élèves peut générer une liste de nouveaux élèves et l'exporter ensuite sous la forme de fichier .csv. Après l'exportation des données vers un fichier .csv, quelles sont les informations dont vous avez besoin pour utiliser les données dans un script ?

Question : Le service Research de votre organisation a été renommé « Recherche et développement ». Vous devez mettre à jour la propriété Department des utilisateurs du service Research pour intégrer cette modification.

Vous avez créé une requête pour des comptes d'utilisateurs avec la propriété **department** ayant pour valeur **Research**, à l'aide de l'applet de commande **Get-ADUser** et du paramètre **-Filter**. Quelle est l'étape suivante pour mettre à jour la propriété department et lui donner la valeur Research and Development ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5

Implémentation du protocole IPv4

Table des matières :

Vue d'ensemble du module **5-1**

Leçon 1 : Vue d'ensemble de TCP/IP **5-2**

Leçon 2 : Fonctionnement de l'adressage IPv4 **5-7**

Leçon 3 : Sous-réseau et super-réseau **5-12**

Leçon 4 : Configuration et résolution des problèmes liés à IPv4 **5-18**

Atelier pratique : Implémentation du protocole IPv4 **5-28**

Contrôle des acquis et éléments à retenir **5-33**

Vue d'ensemble du module

IPv4 est le protocole réseau utilisé sur Internet et les réseaux locaux. Pour pouvoir comprendre et résoudre les problèmes de communication réseau, il est essentiel que vous compreniez comment IPv4 est implémenté. Dans ce module, vous verrez comment implémenter un modèle d'adressage IPv4. Vous verrez également comment déterminer et résoudre les problèmes liés au réseau.

Objectifs

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

- décrire la suite de protocoles TCP/IP ;
- décrire l'adressage IPv4 ;
- déterminer un masque de sous-réseau nécessaire pour le sous-réseau ou le super-réseau ;
- configurer IPv4 et résoudre les problèmes de communication liés à IPv4.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble de TCP/IP

TCP/IP est une suite de protocoles normalisée qui permet la communication dans un réseau hétérogène. Ce cours fournit une vue d'ensemble d'IPv4 et de sa relation avec les autres protocoles pour permettre la communication réseau. Il couvre également le concept des sockets, dont les applications se servent pour accepter les communications réseau. De manière globale, ce cours fournit une base pour comprendre le fonctionnement de la communication réseau et résoudre les problèmes inhérents.

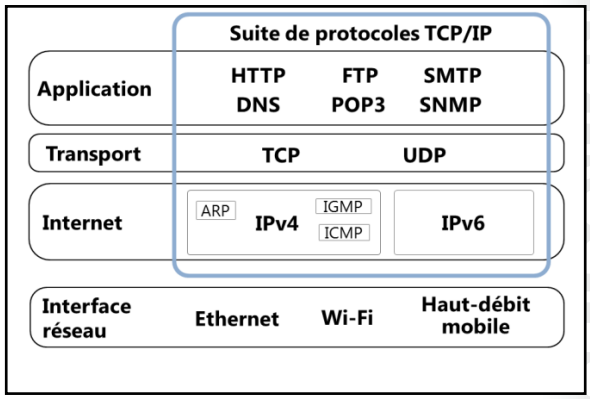
Objectifs de la leçon

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

- décrire les éléments de la suite de protocoles TCP/IP ;
- décrire les différents protocoles qui composent la suite TCP/IP ;
- décrire les protocoles TCP/IP de la couche Application ;
- décrire un socket et identifier les numéros de port des protocoles spécifiés.

Suite de protocoles TCP/IP

Les tâches effectuées par le protocole TCP/IP dans le processus de communication sont réparties entre les protocoles. Ces protocoles sont organisés en quatre couches distinctes dans la pile TCP/IP :



- Couche Application. Les applications utilisent les protocoles de la couche Application pour accéder aux ressources réseau.
- Couche transport. Les protocoles de la couche transport contrôlent la fiabilité du transfert de données sur le réseau.
- Couche Internet. Les protocoles de la couche Internet contrôlent le mouvement des paquets entre les réseaux.
- Couche interface réseau. Les protocoles de la couche interface réseau définissent la façon dont les datagrammes de la couche Internet sont transmis sur le support réseau.

Avantages liés aux couches d'architecture

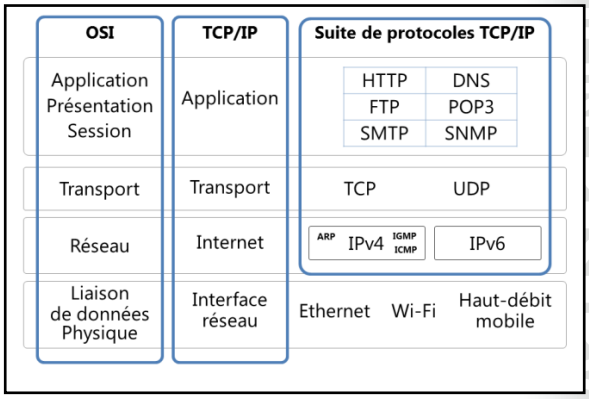
Plutôt que de créer un protocole unique, la division des fonctions réseau en une pile de protocoles distincts offre plusieurs avantages :

- Les protocoles distincts facilitent la prise en charge d'un grand nombre de plateformes informatiques.
- La création ou la modification de protocoles pour prendre en charge de nouvelles normes n'exige pas la modification de l'ensemble de la pile de protocoles.
- Le fonctionnement de plusieurs protocoles dans la même couche permet aux applications de sélectionner les protocoles qui fournissent uniquement le niveau de service requis.
- Dans la mesure où la pile est divisée en couches, le développement des protocoles peut être effectué en parallèle par du personnel spécialement qualifié pour les opérations relatives à des couches particulières.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Protocoles de la suite TCP/IP

Le modèle OSI (Open Systems Interconnection) définit des couches distinctes relatives à l'empaquetage, ainsi qu'à l'envoi et la réception de transmissions de données sur un réseau. La suite en couche des protocoles formant la pile TCP/IP effectue ces fonctions.



Couche Application

La couche Application du modèle TCP/IP correspond à la couche Application, à la couche présentation et à la couche de session du modèle OSI. Cette couche fournit des services et utilitaires qui permettent aux applications d'accéder aux ressources réseau.

Couche transport

La couche transport correspond à la couche transport du modèle OSI et est responsable de la communication de bout en bout à l'aide du protocole TCP ou UDP (User Datagram Protocol). La suite de protocoles TCP/IP offre aux programmeurs d'applications le choix entre TCP ou UDP en tant que protocole de couche transport :

- **TCP**. Fournit aux applications des communications fiables orientées connexion. Une communication orientée connexion vérifie si la destination est prête à recevoir des données avant l'envoi de ces données. Pour rendre la communication fiable, le protocole TCP s'assure que tous les paquets sont reçus. Une communication fiable est souhaitable dans la plupart des cas et est utilisée par la plupart des applications. Les serveurs Web, les clients FTP (File Transfer Protocol) et les autres applications qui transfèrent de grandes quantités de données utilisent le protocole TCP.
- **UDP**. Offre une communication non fiable, en mode non connecté. Lorsque vous utilisez le protocole UDP, la fiabilité de la remise est de la responsabilité de l'application. Les applications utilisent le protocole UDP pour communiquer plus rapidement avec une charge de traitement moins importante que le protocole TCP. Certaines applications, par exemple les applications audio et vidéo de diffusion en continu, utilisent le protocole UDP afin que l'absence d'un paquet ne retarde pas la lecture. Le protocole UDP est également utilisé par les applications qui envoient de petites quantités de données, par exemple lors des recherches de noms DNS (Domain Name System).

Le protocole de couche transport utilisé par une application est déterminé par le développeur de l'application. En outre, il est basé sur les exigences de communication de l'application.

Couche Internet

La couche Internet correspond à la couche réseau du modèle OSI et est constituée de plusieurs protocoles distincts, notamment : IP, ARP (Address Resolution Protocol), IGMP (Internet Group Management Protocol) et ICMP (Internet Control Message Protocol). Les protocoles de la couche Internet encapsulent les données de la couche transport dans des unités appelées *paquets*, qu'ils traitent, puis acheminent vers leurs destinations.

Les protocoles de la couche Internet sont les suivants :

- **IP**. Le protocole IP est responsable du routage et de l'adressage. Les systèmes d'exploitation Windows® 8 et Windows Server® 2012 implémentent une pile de protocoles IP à double couche. Par ailleurs, ils assurent la prise en charge des protocoles IPv4 et IPv6.
- **ARP**. Le protocole ARP est utilisé par le protocole IP pour déterminer l'adresse MAC (Media Access Control) des cartes réseau locales (c'est-à-dire les cartes installées sur les ordinateurs du réseau local) à partir de l'adresse IP d'un hôte local. Le protocole ARP est basé sur la diffusion, ce qui signifie que les trames ARP ne peuvent pas transiter par un routeur et qu'elles sont donc localisées. Certaines implémentations du protocole TCP/IP prennent en charge le protocole RARP (Reverse ARP) dans lequel l'adresse MAC d'une carte réseau sert à déterminer l'adresse IP correspondante.
- **IGMP**. Le protocole IGMP prend en charge les applications multitâches via les routeurs des réseaux IPv4.
- **ICMP**. Le protocole ICMP envoie des messages d'erreur dans un réseau basé sur le protocole IP.

Couche interface réseau

La couche interface réseau (parfois appelée *couche liaison* ou *couche de liaison de données*) correspond à la couche de liaison de données et à la couche physique du modèle OSI. La couche interface réseau spécifie les exigences relatives à l'envoi et la réception des paquets sur le support réseau. Bien souvent, cette couche n'est pas formellement considérée comme faisant partie de la suite de protocoles TCP/IP, car les tâches sont exécutées par le pilote de carte réseau et la carte réseau.

Applications TCP/IP

Les applications utilisent les protocoles de la couche Application pour communiquer sur le réseau. Un client et un serveur doivent utiliser le même protocole de couche Application pour communiquer. Le tableau suivant répertorie certains protocoles usuels de la couche Application.

Quelques protocoles usuels de la couche Application
- HTTP
- HTTPS
- FTP
- RDP
- SMB
- SMTP
- POP3

Protocole	Description
HTTP	Utilisé pour la communication entre les navigateurs Web et les serveurs Web.
HTTPS (HTTP/Secure)	Version du protocole HTTP qui chiffre la communication entre les navigateurs Web et les serveurs Web.
FTP	Utilisé pour transférer des fichiers entre les clients et les serveurs FTP.
RDP (Remote Desktop Protocol)	Utilisé pour contrôler à distance un ordinateur qui exécute les systèmes d'exploitation Windows sur un réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

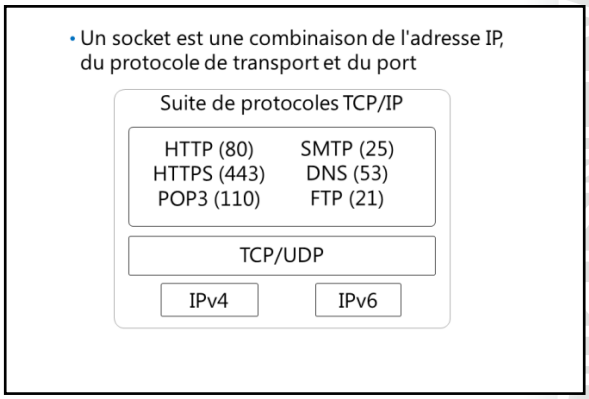
(suite)

Protocole	Description
Protocole SMB (Server Message Block)	Utilisé par les serveurs et les ordinateurs clients pour le partage de fichiers et d'imprimantes.
Protocole SMTP (Simple Mail Transfer Protocol)	Utilisé pour transférer des messages électroniques sur Internet.
POP3 (Post Office Protocol version 3)	Utilisé pour récupérer des messages à partir de certains serveurs de messagerie.
IMAP (Internet Message Application Protocol)	Utilisé pour récupérer des messages à partir de certains serveurs de messagerie.

Qu'est-ce qu'un socket ?

Lorsqu'une application souhaite établir une communication avec une autre application sur un hôte distant, elle crée un socket TCP ou UDP, selon les besoins. Un socket identifie les éléments suivants dans le cadre du processus de communication :

- protocole de transport utilisé par l'application, TCP ou UDP par exemple ;
- numéros de port TCP ou UDP que les applications utilisent ;
- adresse IPv4 ou IPv6 des hôtes de destination et source.



Cette combinaison du protocole de transport, de l'adresse IP et du port crée un socket.

Ports connus

Un numéro de port compris entre 0 et 65 535 est affecté aux applications. Les 1 024 premiers ports sont appelés *ports connus* et sont affectés à des applications spécifiques. Les applications qui sont à l'écoute des connexions utilisent des numéros de port cohérents pour permettre aux applications clientes de se connecter plus facilement. Si une application est à l'écoute sur un numéro de port non standard, vous devez spécifier le numéro de port lors de la connexion à ce dernier. Les applications clientes utilisent généralement un numéro de port source aléatoire supérieur à 1 024. Le tableau suivant identifie certains de ces ports connus.

Port	Protocole	Application
80	TCP	HTTP utilisé par un serveur Web
443	TCP	HTTPS pour un serveur Web sécurisé
110	TCP	POP3 utilisé pour la récupération du courrier électronique

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Port	Protocole	Application
143	TCP	IMAP utilisé pour la récupération du courrier électronique
25	TCP	SMTP utilisé pour l'envoi de messages électroniques
53	UDP	DNS utilisé pour la plupart des demandes de résolution de noms
53	TCP	DNS utilisé pour les transferts de zone
20, 21	TCP	FTP utilisé pour les transferts de fichiers

Vous devez connaître les numéros de port que les applications utilisent afin de pouvoir configurer les pare-feu pour autoriser la communication. La plupart des applications ont un numéro de port par défaut à cet effet, mais celui-ci peut être modifié en cas de besoin. Par exemple, certaines applications Web s'exécutent sur un autre port que le port 80 ou le port 443.

Question : Est-ce que vous pensez à d'autres ports connus ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Fonctionnement de l'adressage IPv4

La compréhension du fonctionnement de la communication réseau IPv4 est essentielle pour pouvoir implémenter, dépanner et gérer les réseaux IPv4. L'une des composantes essentielles d'IPv4 est l'adressage. La compréhension du fonctionnement de l'adressage, des masques de sous-réseau et des passerelles par défaut vous permet d'identifier la communication appropriée entre les hôtes. Pour identifier les erreurs de communication IPv4, vous devez comprendre comment le processus de communication est censé fonctionner.

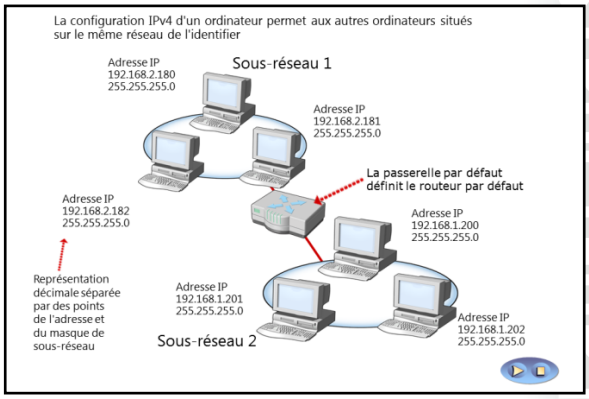
Objectifs de la leçon

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

- décrire l'adressage IPv4 ;
- identifier les adresses IPv4 publiques et privées ;
- expliquer la relation entre la notation décimale séparée par des points et les nombres binaires ;
- décrire un réseau IPv4 simple comprenant un adressage avec des classes ;
- décrire un réseau IPv4 plus complexe comprenant un adressage sans classe.

Adressage IPv4

Pour configurer la connectivité réseau, vous devez connaître les adresses IPv4 et savoir comment elles fonctionnent. La communication réseau d'un ordinateur est dirigée vers l'adresse IPv4 de cet ordinateur. Par conséquent, chaque ordinateur du réseau doit posséder une adresse IPv4 unique.



Chaque adresse IPv4 a une longueur de 32 bits. Pour rendre les adresses IP plus lisibles, celles-ci sont affichées en notation décimale séparée par des points. La notation décimale séparée par des points scinde une adresse IPv4 32 bits en quatre groupes de 8 bits, lesquels sont convertis en un nombre décimal compris entre zéro et 255. Les nombres décimaux sont séparés par un point. Chaque nombre décimal porte le nom d'*octet*.

Masque de sous-réseau

Chaque adresse IPv4 est composée d'un ID réseau et d'un ID hôte. L'*ID réseau* identifie le réseau sur lequel l'ordinateur est situé. L'*ID hôte* identifie l'ordinateur de manière unique sur ce réseau spécifique. Un *masque de sous-réseau* identifie la partie de l'adresse IPv4 qui correspond à l'ID réseau et celle qui correspond à l'ID hôte.

Dans les scénarios les plus simples, chaque octet d'un masque de sous-réseau est égal à 255 ou 0. La valeur 255 représente un octet qui fait partie de l'ID réseau, alors que la valeur 0 représente un octet qui fait partie de l'ID hôte. Par exemple, un ordinateur avec l'adresse IP 192.168.23.45 et le masque de sous-réseau 255.255.255.0 possède l'ID réseau 192.168.23.0 et l'ID hôte 0.0.0.45.

Remarque : Les termes réseau, sous-réseau et réseau local virtuel (VLAN) sont souvent utilisés de façon interchangeable. Un réseau de grande taille est souvent subdivisé en sous-réseaux. En outre, des réseaux locaux virtuels (VLAN) sont configurés sur les commutateurs pour représenter les sous-réseaux.

Passerelle par défaut

Une *passerelle par défaut* est un périphérique (généralement un routeur) d'un réseau TCP/IP qui transfère des paquets IP à d'autres réseaux. Les multiples réseaux internes d'une organisation peuvent être désignés sous le nom d'*intranet*.

Dans un intranet, tout réseau donné peut avoir plusieurs routeurs qui le connectent à d'autres réseaux, locaux et distants. Vous devez configurer l'un des routeurs comme passerelle par défaut pour les hôtes locaux. Cela permet aux hôtes locaux de communiquer avec des hôtes situés sur des réseaux distants.

Avant qu'un hôte n'envoie un paquet IPv4, il utilise son propre masque de sous-réseau pour déterminer si l'hôte de destination est sur le même réseau ou sur un réseau distant. Si l'hôte de destination est sur le même réseau, l'hôte d'envoi transmet le paquet directement à l'hôte de destination. Si l'hôte de destination est sur un réseau différent, l'hôte transmet le paquet à un routeur pour qu'il soit remis.

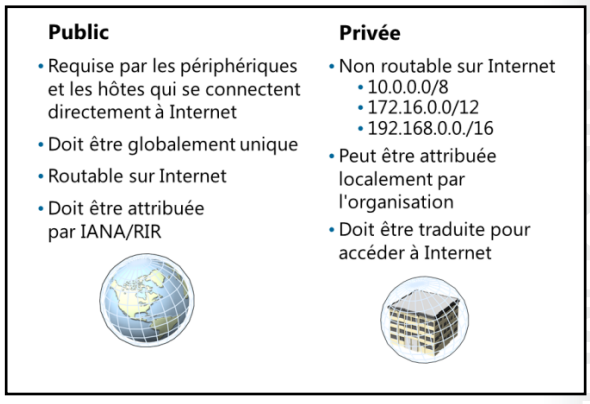
Lorsqu'un hôte transmet un paquet à un réseau distant, IPv4 consulte la table de routage interne afin de déterminer quel est le routeur approprié pour permettre au paquet d'atteindre le sous-réseau de destination. Si la table de routage ne contient pas d'informations de routage à propos du sous-réseau de destination, IPv4 transmet le paquet à la passerelle par défaut. L'hôte suppose que la passerelle par défaut contient les informations de routage requises. La passerelle par défaut est utilisée dans la plupart des cas.

Les ordinateurs clients obtiennent généralement leurs informations d'adressage IP à partir d'un serveur DHCP (Dynamic Host Configuration Protocol). Cette méthode est plus simple que l'attribution manuelle d'une passerelle par défaut sur chaque hôte. La plupart des serveurs ont une configuration IP statique qui est affectée manuellement.

> **Question :** Comment la communication réseau est-elle affectée si une passerelle par défaut est configurée de manière incorrecte ?

Adresses IPv4 publiques et privées

Les périphériques et les hôtes qui se connectent directement à Internet requièrent une adresse IPv4 publique. Les hôtes et les périphériques qui ne se connectent pas directement à Internet ne requièrent pas d'adresse IPv4 publique.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Adresses IPv4 publiques

Les adresses IPv4 publiques doivent être uniques. L'IANA (Internet Assigned Numbers Authority) affecte des adresses IPv4 publiques aux registres Internet régionaux (RIR). Les registres Internet régionaux affectent ensuite les adresses IPv4 aux fournisseurs de services Internet. En général, votre fournisseur de services Internet (ISP, Internet Service Provider) vous alloue une ou plusieurs adresses publiques à partir de son pool d'adresses. Le nombre d'adresses qui vous est alloué par votre ISP dépend du nombre de périphériques et d'hôtes que vous devez connecter à Internet.

Adresses IPv4 privées

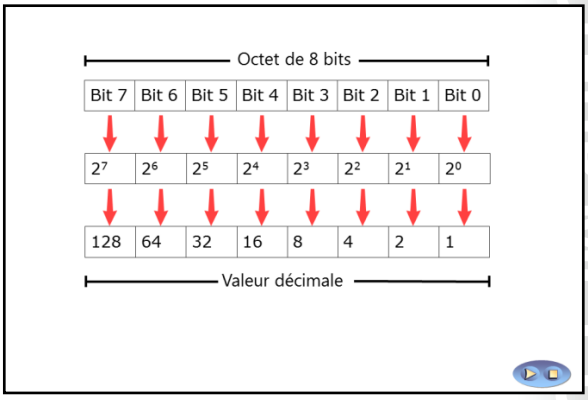
Le pool d'adresses IPv4 se restreint, c'est pourquoi les registres Internet régionaux sont peu disposés à allouer des adresses IPv4 superflues. Les technologies telles que la traduction d'adresses réseau (NAT) permettent aux administrateurs d'utiliser un nombre relativement restreint d'adresses IPv4 publiques et, en même temps, permettent aux hôtes locaux de se connecter à des hôtes distants et à des services sur Internet.

L'IANA définit les plages d'adresses du tableau suivant en tant que plages privées. Les routeurs Internet ne transfèrent pas les paquets qui proviennent de ces plages ou qui leur sont destinés.

Réseau	Plage
10.0.0.0/8	10.0.0.0-10.255.255.255
172.16.0.0/12	172.16.0.0-172.31.255.255
192.168.0.0/16	192.168.0.0-192.168.255.255

Relation entre la notation décimale séparée par des points et les nombres binaires

Lorsque vous affectez des adresses IP, vous utilisez la notation décimale séparée par des points. La notation décimale séparée par des points est basée sur le système de numération décimale. Cependant, en arrière-plan, les ordinateurs utilisent les adresses IP en binaire. Pour comprendre comment choisir un masque de sous-réseau pour des réseaux complexes, vous devez comprendre le fonctionnement des adresses IP en binaire.



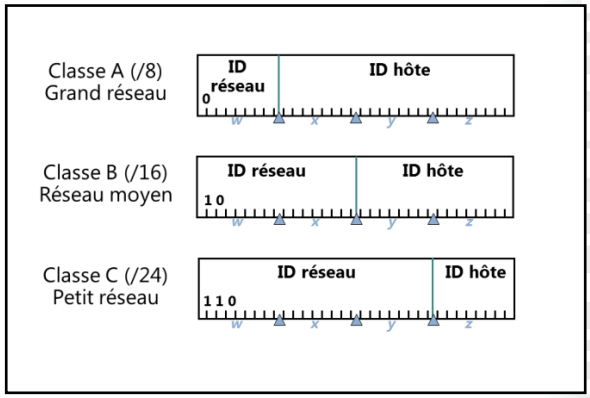
Dans un octet de 8 bits, la position de chaque bit a une valeur décimale. Un bit ayant une valeur égale à 0 a toujours la valeur zéro. Un bit ayant une valeur égale à 1 peut être converti en valeur décimale. Le *bit de poids faible* (bit le plus à droite dans l'octet) représente la valeur décimale 1. Le *bit de poids fort* (bit le plus à gauche dans l'octet) représente la valeur décimale 128. Si tous les bits d'un octet ont la valeur 1, la valeur décimale de cet octet est 255 (à savoir : 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1). Il s'agit de la valeur la plus élevée possible d'un octet.

La plupart du temps, vous pouvez utiliser une calculatrice pour convertir des nombres décimaux en système binaire et vice versa. L'application Calculatrice incluse dans les systèmes d'exploitation Windows peut effectuer des conversions du système décimal au système binaire (et inversement), comme le montre l'exemple suivant.

Binaire	Notation décimale séparée par des points
10000011 01101011 00000011 00011000	131.107.3.24

Implémentations simples d'IPv4

Classes d'adresses IPv4



L'IANA organise les adresses IPv4 en classes. Chaque classe d'adresse a un masque de sous-réseau par défaut distinct qui définit le nombre d'hôtes valides sur le réseau. Les classes d'adresses IPv4 créées par l'IANA vont de la *Classe A* à la *Classe E*.

Les classes A, B et C sont des réseaux IP que vous pouvez affecter aux adresses IP des ordinateurs hôtes. Les adresses de la classe D sont utilisées par les ordinateurs et les applications pour la multidiffusion. L'IANA réserve la classe E aux utilisations expérimentales. Le tableau suivant répertorie les caractéristiques de chaque classe d'adresse IP.

Classe	Premier octet	Masque de sous-réseau par défaut	Nombre de réseaux	Nombre d'hôtes par réseau
A	1-127	255.0.0.0	126	16,777,214
B	128-191	255.255.0.0	16,384	65,534
C	192-223	255.255.255.0	2,097,152	254

Remarque : Internet n'utilise plus le routage basé sur le masque de sous-réseau par défaut des classes d'adresses IPv4.

Réseaux IPv4 simples

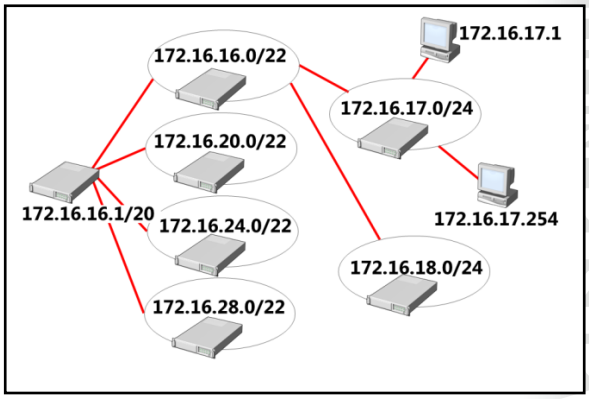
Vous pouvez utiliser des sous-réseaux pour diviser un grand réseau en plusieurs réseaux plus petits. Dans les réseaux IPv4 simples, le masque de sous-réseau définit des octets complets dans le cadre de l'ID du réseau et de l'ID de l'hôte. Un nombre 255 représente un octet qui fait partie de l'ID du réseau et un 0 représente un octet qui fait partie de l'ID de l'hôte. Par exemple, vous pouvez utiliser le réseau 10.0.0.0 avec le masque de sous-réseau 255.255.0.0 pour créer 256 réseaux plus petits.

Remarque : L'adresse IPv4 127.0.0.1 sert d'adresse de bouclage. Vous pouvez utiliser cette adresse pour tester la configuration locale de la pile de protocoles IPv4. Par conséquent, l'adresse réseau 127 n'est pas utilisable pour la configuration d'hôtes IPv4.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémentations plus complexes d'IPv4

Dans les réseaux complexes, les masques de sous-réseau ne sont pas forcément des combinaisons simples de 255 et 0. Au lieu de cela, vous pouvez subdiviser un octet en quelques bits pour l'ID réseau et d'autres pour l'ID hôte. Cela vous permet d'avoir le nombre spécifique de sous-réseaux et d'hôtes dont vous avez besoin.



L'exemple suivant montre un masque de sous-réseau qui peut être utilisé pour diviser un réseau de classe B en 16 sous-réseaux :

172.16.0.0/255.255.240.0

Dans de nombreux cas, plutôt que d'utiliser une représentation décimale séparée par des points pour le masque de sous-réseau, le nombre de bits de l'ID réseau est spécifié à la place. Cela s'appelle le routage CIDR (*Classless InterDomain Routing*). Ce qui suit est un exemple de notation CIDR :

172.16.0.0/20

Masques de sous-réseau de longueur variable

Les routeurs modernes prennent en charge l'utilisation des masques de sous-réseau de longueur variable. Les masques de sous-réseau de longueur variable vous permettent de créer des sous-réseaux de différentes tailles lorsque vous subdivisez un réseau de plus grande taille. Par exemple, vous pouvez subdiviser un petit réseau de 256 adresses en trois réseaux plus petits de 128 adresses, 64 adresses et 64 adresses. Cela vous permet d'utiliser les adresses IP d'un réseau de manière plus efficace.

Question : Est-ce que votre organisation utilise un réseau simple ou complexe ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Sous-réseau et super-réseau

Dans la plupart des organisations, vous devez créer des sous-réseaux dans le but de diviser votre réseau en sous-réseaux plus petits et d'allouer ces sous-réseaux à des fins ou des lieux spécifiques. Pour ce faire, vous devez comprendre comment sélectionner le nombre approprié de bits à inclure dans les masques de sous-réseau. Dans certains cas, vous devrez peut-être également combiner plusieurs réseaux en un seul réseau de plus grande taille via la création d'un super-réseau.

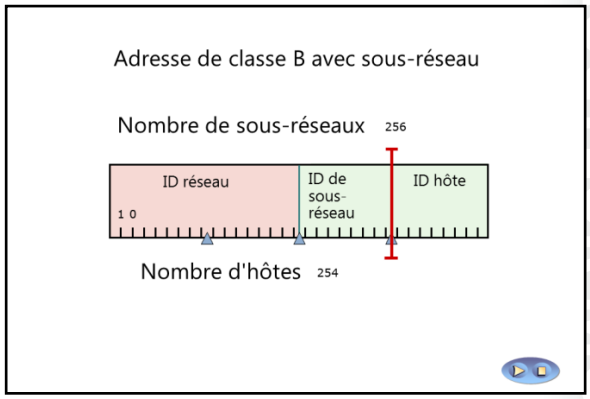
Objectifs de la leçon

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

- décrire l'utilisation des bits dans un masque de sous-réseau ou une longueur de préfixe ;
- déterminer quand utiliser des sous-réseaux ;
- calculer un masque de sous-réseau qui prend en charge un nombre spécifique d'adresses de sous-réseau ;
- calculer un masque de sous-réseau qui prend en charge un nombre spécifique d'adresses d'hôte ;
- identifier un masque de sous-réseau approprié à un scénario ;
- décrire la création d'un super-réseau.

Utilisation des bits dans un masque de sous-réseau ou une longueur de préfixe

Dans les réseaux simples, les masques de sous-réseau sont composés de quatre octets. Chaque octet a une valeur égale à 255 ou 0. Si la valeur de l'octet est 255, cet octet fait partie de l'ID réseau. Si la valeur de l'octet est 0, cet octet fait partie de l'ID hôte.



Dans les réseaux complexes, vous pouvez convertir le masque de sous-réseau en valeur binaire et évaluer chaque bit du masque de sous-réseau. Un masque de sous-réseau est composé de chiffres 1 et 0 contigus. Les chiffres 1 commencent au bit situé le plus à gauche et se répètent sans interruption jusqu'à ce que les bits deviennent des chiffres 0.

Remarque : Les applets de commande Windows PowerShell® qui permettent de configurer un réseau IPv4 utilisent une valeur de longueur de préfixe à la place d'un masque de sous-réseau pour définir le nombre de bits réseau. La longueur de préfixe correspond au nombre de bits utilisés par la notation CIDR.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez identifier l'ID réseau d'un masque de sous-réseau en fonction des chiffres 1 utilisés. Vous pouvez identifier l'ID hôte en fonction des chiffres 0 utilisés. Les bits de l'ID hôte qui sont affectés à l'ID réseau doivent être contigus par rapport à l'ID réseau d'origine.

- Chaque bit 1 fait partie de l'ID réseau.
- Chaque bit 0 fait partie de l'ID hôte.

Le processus mathématique utilisé pour comparer une adresse IP et un masque de sous-réseau est appelé *ANDing* ou conjonction logique (ET logique).

Lorsque vous utilisez plus de bits pour le masque de sous-réseau, vous pouvez avoir plus de sous-réseaux, mais moins d'hôtes sur chaque sous-réseau. Utiliser plus de bits que ce dont vous avez besoin permet la croissance du sous-réseau, mais limite celle des hôtes. En utiliser moins permet d'augmenter le nombre d'hôtes, mais limite la croissance des sous-réseaux.

Avantages de l'utilisation de sous-réseaux

Lorsque vous subdivisez un réseau en sous-réseaux, vous devez créer un ID unique pour chaque sous-réseau. Ces ID uniques sont dérivés à partir de l'ID réseau principal (vous allouez une partie des bits de l'ID hôte à l'ID réseau). Cette allocation vous permet de créer plus de réseaux.

Lorsque vous subdivisez un réseau en sous-réseaux, vous créez un ID unique pour chaque sous-réseau qui est dérivé de l'ID réseau principal

En utilisant des sous-réseaux, vous pouvez

- Utiliser une seule adresse réseau sur plusieurs emplacements physiques
- Réduire la surcharge du réseau en segmentant le trafic
- Renforcer la sécurité à l'aide de pare-feu
- Dépasser les limites des technologies actuelles

En utilisant des sous-réseaux, vous pouvez :

- utiliser un seul réseau de grande taille sur plusieurs emplacements physiques ;
- réduire les encombrements réseau en segmentant le trafic et en réduisant les diffusions sur chaque segment ;
- augmenter la sécurité en divisant le réseau et en utilisant des pare-feu pour contrôler la communication ;
- dépasser les limites des technologies actuelles, par exemple dépasser le nombre maximal d'hôtes que chaque segment peut avoir.

Calcul des adresses de sous-réseau

Avant de définir un masque de sous-réseau, évaluez la quantité de sous-réseaux et d'hôtes requise pour chaque sous-réseau. Cela vous permet d'utiliser le nombre de bits approprié pour le masque de sous-réseau.

Vous pouvez calculer le nombre de bits de sous-réseau dont vous avez besoin dans le réseau. Utilisez la formule 2^n, où *n* est le nombre de bits. Le résultat est le nombre de sous-réseaux requis par votre réseau.

Lorsque vous déterminez des adresses de sous-réseau, vous devez

- Choisir le nombre de bits de sous-réseau en fonction du nombre de sous-réseaux requis
- Utiliser 2^n pour déterminer le nombre de sous-réseaux fournis par n bits

Pour cinq emplacements, les trois bits de sous-réseau suivants sont requis

- 5 emplacements = 5 sous-réseaux requis
- 22 = 4 sous-réseaux (pas suffisant)
- 23 = 8 sous-réseaux

Le tableau suivant indique le nombre de sous-réseaux que vous pouvez créer en utilisant un nombre spécifique de bits.

Nombre de bits (n)	Nombre de sous-réseaux (2^n)
1	2
2	4
3	8
4	16
5	32
6	64

Pour déterminer rapidement les adresses de sous-réseau, vous pouvez utiliser la valeur de bit minimale dans le masque de sous-réseau. Par exemple, si vous choisissez de diviser en sous-réseaux le réseau 172.16.0.0 en utilisant 3 bits, le masque de sous-réseau est 255.255.224.0. Au format binaire, le décimal 224 est 11100000 et la valeur de bit minimale est 32. Elle constitue l'incrément entre chaque adresse de sous-réseau.

Le tableau suivant montre les adresses de sous-réseau pour cet exemple ; les 3 bits que vous avez choisi d'utiliser pour subdiviser le réseau sont indiqués en caractères gras.

Numéro de réseau binaire	Numéro de réseau décimal
172.16.**000**00000.00000000	172.16.0.0
172.16.**001**00000.00000000	172.16.32.0
172.16.**010**00000.00000000	172.16.64.0
172.16.**011**00000.00000000	172.16.96.0
172.16.**100**00000.00000000	172.16.128.0
172.16.**101**00000.00000000	172.16.160.0
172.16.**110**00000.00000000	172.16.192.0
172.16.**111**00000.00000000	172.16.224.0

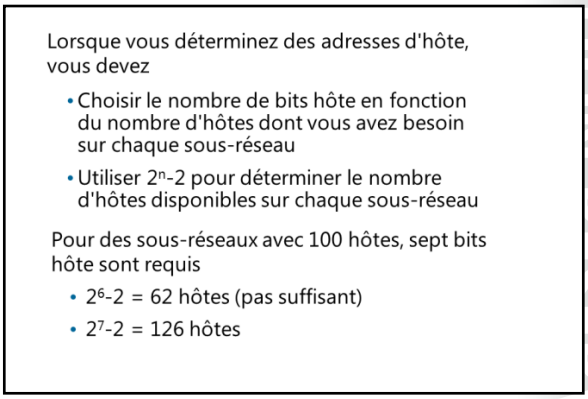
Remarque : Vous pouvez utiliser un calculateur de sous-réseaux afin de déterminer quels sont les sous-réseaux appropriés pour votre réseau, au lieu de les calculer manuellement. Les calculateurs de sous-réseaux sont largement répandus sur Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Calcul des adresses d'hôte

Pour déterminer quels sont les bits hôtes du masque, déterminez le nombre de bits requis pour la prise en charge des hôtes d'un sous-réseau. Calculez le nombre de bits hôtes requis en utilisant la formule 2^n-2, où *n* est le nombre de bits. Ce résultat doit correspondre au moins au nombre d'hôtes dont vous avez besoin pour votre réseau. C'est également le nombre maximal d'hôtes que vous pouvez configurer sur ce sous-réseau.



Sur chaque sous-réseau, deux ID hôtes sont alloués automatiquement et ne peuvent pas être utilisés par les ordinateurs. Une adresse dont l'ID hôte comprend uniquement des 0 représente le réseau. Une adresse dont l'ID hôte comprend uniquement des 1 est l'adresse de diffusion de ce réseau.

Le tableau suivant montre le nombre d'hôtes disponibles dans un réseau de classe C, selon le nombre de bits hôtes.

Nombre de bits (n)	Nombre d'hôtes (2^n-2)
1	0
2	2
3	6
4	14
5	30
6	62

Vous pouvez calculer la plage d'adresses d'hôte de chaque sous-réseau en utilisant le processus suivant :

1. Le premier hôte est supérieur d'un chiffre binaire à l'ID du sous-réseau actuel.
2. Le dernier hôte est inférieur de deux chiffres binaires à l'ID du sous-réseau suivant.

Le tableau suivant montre des exemples de calcul d'adresses d'hôte.

Réseau	Plage d'hôtes
172.16.64.0/19	172.16.64.1 – 172.16.95.254
172.16.96.0/19	172.16.96.1 – 172.16.127.254
172.16.128.0/19	172.16.128.1 – 172.16.159.254

Pour créer un modèle d'adressage approprié pour votre organisation, vous devez connaître le nombre de sous-réseaux dont vous avez besoin et le nombre d'hôtes dont vous avez besoin sur chaque sous-réseau. Une fois que vous avez ces informations, vous pouvez calculer le masque de sous-réseau approprié.

Discussion : Création d'un modèle de sous-réseau pour un nouveau bureau

Lisez le scénario suivant et répondez aux questions sur la diapositive.

- Combien de sous-réseaux sont requis ?
- Combien de bits sont requis pour créer ce nombre de sous-réseaux ?
- Combien d'hôtes sont requis sur chaque sous-réseau ?
- Combien de bits sont requis pour permettre l'utilisation de ce nombre d'hôtes ?
- Quel est le masque de sous-réseau approprié pour répondre à ces besoins ?

20 minutes

Vous identifiez une configuration réseau appropriée pour un nouveau campus. Il vous a été alloué le réseau 10.34.0.0/16, que vous pouvez diviser en sous-réseaux en fonction des besoins.

Il existe quatre bâtiments sur le nouveau campus et chacun d'eux doit avoir son propre sous-réseau pour permettre un routage entre les bâtiments. Chaque bâtiment aura un maximum de 700 utilisateurs. Chaque bâtiment aura également des imprimantes. La proportion classique d'utilisateurs par rapport aux imprimantes est de 50 pour 1.

Vous devez également allouer un sous-réseau pour le centre de données de serveurs qui peut accueillir jusqu'à 100 serveurs.

Qu'est-ce qu'un super-réseau ?

- Un super-réseau combine plusieurs petits réseaux en un réseau plus important
- Les réseaux que vous combinez doivent être contigus
- Le tableau suivant montre un exemple de super-réseau basé sur deux réseaux de classe C

Réseau	Plage
192.168.**00010000**.00000000/24	192.168.16.0 - 192.168.16.255
192.168.**00010001**.00000000/24	192.168.17.0 - 192.168.17.255
192.168.**0001000**0.00000000/23	192.168.16.0 - 192.168.17.255

Un super-réseau combine plusieurs petits réseaux en un réseau unique de grande taille. Cela peut être approprié lorsque vous avez un petit réseau qui s'est agrandi et que vous devez étendre l'espace d'adressage. Par exemple, une filiale qui utilise le réseau 192.168.16.0/24 et qui a épuisé toutes ses adresses IP peut se voir allouer le réseau supplémentaire 192.168.17.0/24. Si vous utilisez le masque de sous-réseau par défaut 255.255.255.0 pour ces réseaux, vous devez effectuer un routage entre ces derniers. Vous pouvez utiliser un super-réseau pour les combiner en un réseau unique.

Pour permettre la création de super-réseaux, les réseaux que vous combinez doivent être contigus. Par exemple, vous pouvez créer un super-réseau avec 192.168.16.0/24 et 192.168.17.0/24 mais pas avec 192.168.16.0/24 et 192.168.54.0/24.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Un super-réseau est le contraire d'un sous-réseau. Lorsque vous créez un super-réseau, vous allouez des bits de l'ID réseau à l'ID hôte. Le tableau suivant indique le nombre de réseaux que vous pouvez combiner à l'aide d'un nombre spécifique de bits.

Nombre de bits	Nombre de réseaux combinés
1	2
2	4
3	8
4	16

Le tableau suivant montre un exemple de super-réseau basé sur deux réseaux de classe C. La partie du masque de sous-réseau que vous utilisez dans le cadre de l'ID réseau est indiquée en caractères gras.

Réseau	Plage
192.168.**00010000**.00000000/24	192.168.16.0-192.168.16.255
192.168.**00010001**.00000000/24	192.168.17.0-192.168.17.255
192.168.**0001000**0.00000000/23	192.168.16.0-192.168.17.255

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Configuration et résolution des problèmes liés à IPv4

Si IPv4 est configuré de manière incorrecte, cela affecte la disponibilité des services qui s'exécutent sur un serveur. Pour garantir la disponibilité des services réseau, vous devez comprendre comment configurer IPv4 et résoudre les problèmes de ce dernier. Windows Server 2012 offre désormais la possibilité de configurer IPv4 à l'aide de Windows PowerShell, qui permet de créer des scripts.

Les outils de résolution de problèmes dans Windows Server 2012 sont similaires aux outils des versions antérieures des systèmes d'exploitation clients et serveur Windows. Toutefois, vous ne connaissez peut-être pas bien le Moniteur réseau, que vous pouvez utiliser pour effectuer une analyse détaillée de votre communication réseau.

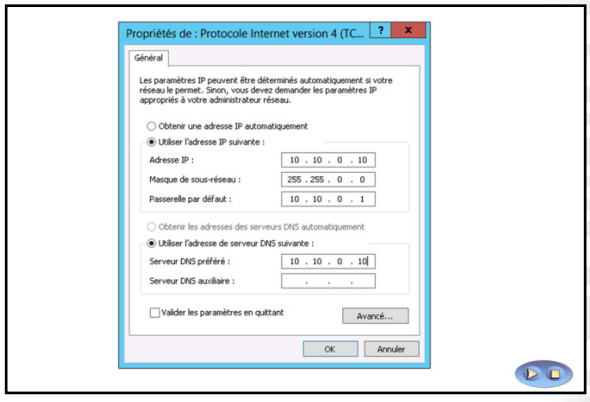
Objectifs de la leçon

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

- configurer IPv4 manuellement afin de fournir une configuration statique pour un serveur ;
- configurer un serveur afin qu'il obtienne une configuration IPv4 automatiquement ;
- expliquer l'utilisation des outils de résolution de problèmes liés à IPv4 ;
- expliquer l'utilisation des applets de commande Windows PowerShell pour résoudre les problèmes liés à IPv4 ;
- décrire le processus de dépannage qui permet de résoudre les problèmes fondamentaux liés à IPv4 ;
- décrire la fonction du Moniteur réseau ;
- utiliser le Moniteur réseau pour capturer et analyser le trafic réseau.

Configuration manuelle d'IPv4

En règle générale, vous configurez des serveurs avec une adresse IP statique. Cela vous permet de connaître et de documenter les adresses IP que vous utilisez pour les différents services de votre réseau. Par exemple, un serveur DNS est accessible à une adresse IP spécifique qui ne doit pas changer.



Une configuration IPv4 comprend les éléments suivants :

- Adresse IPv4
- Masque de sous-réseau
- Passerelle par défaut
- Serveurs DNS

Dans le cas de la configuration statique, vous devez vous rendre sur chaque ordinateur et entrer la configuration IPv4 manuellement. Cette méthode de gestion des ordinateurs est raisonnable pour les serveurs mais prend beaucoup de temps pour les ordinateurs clients. La saisie manuelle d'une configuration statique augmente également le risque d'erreurs de configuration.

Vous pouvez configurer une adresse IP statique, soit dans les propriétés de la connexion réseau, soit à l'aide de l'outil en ligne de commande netsh. Par exemple, la commande suivante permet de configurer l'interface Connexion au réseau local avec les paramètres suivants :

Adresse IP statique 10.10.0.10

Masque de sous-réseau 255.255.255.0

Passerelle par défaut 10.10.0.1

```
Netsh interface ipv4 set address name= "Connexion au réseau local" source=static
addr=10.10.0.10 mask=255.255.255.0 gateway=10.10.0.1
```

Windows Server 2012 dispose également des applets de commande Windows PowerShell, que vous pouvez utiliser pour gérer la configuration réseau. Le tableau suivant décrit quelques-unes des applets de commande Windows PowerShell qui sont disponibles pour configurer IPv4.

Applet de commande	Description des utilisations pour la configuration IPv4
New-NetIPAddress	Crée une adresse IP et la lie à une carte réseau. Vous ne pouvez pas modifier une adresse IP existante, vous devez supprimer une adresse IP existante et créer une autre adresse IP.
Set-NetIPInterface	Active ou désactive le protocole DHCP pour une interface.
New-NetRoute	Crée des entrées de table de routage, y compris la passerelle par défaut (0.0.0.0). Vous ne pouvez pas modifier le prochain tronçon d'un itinéraire existant ; vous devez plutôt supprimer un itinéraire existant et créer un autre itinéraire avec le prochain tronçon approprié.
Set-DNSClientServerAddresses	Configure le serveur DNS utilisé pour une interface.

Le code suivant est un exemple d'applets de commande Windows PowerShell que vous pouvez utiliser pour configurer l'interface Connexion au réseau local avec les paramètres suivants :

Adresse IP statique 10.10.0.10

Masque de sous-réseau 255.255.255.0

Passerelle par défaut 10.10.0.1

L'interface Connexion au réseau local est également configurée pour utiliser les serveurs DNS 10.12.0.1 et 10.12.0.2.

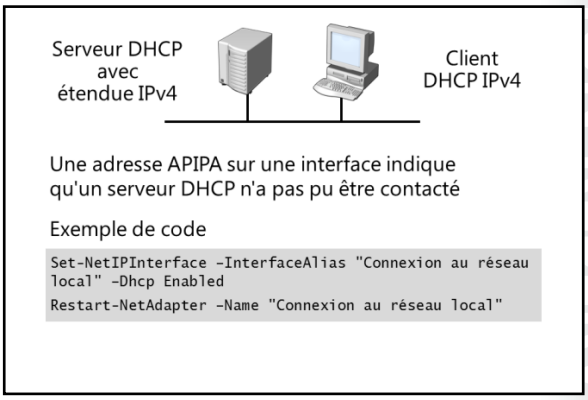
```
New-NetIPAddress –InterfaceAlias "Connexion au réseau local" –IPAddress 10.10.0.10 -
PrefixLength 24 –DefaultGateway 10.10.0.1
Set-DNSClientServerAddresses –InterfaceAlias "Connexion au réseau local" -ServerAddresses
10.12.0.1,10.12.0.2
```

Question : Est-ce que les ordinateurs ou périphériques de votre organisation ont des adresses IP statiques ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration automatique d'IPv4

Le protocole DHCP pour IPv4 vous permet d'affecter des configurations IPv4 automatiques à un grand nombre d'ordinateurs et non pas de façon individuelle. Le service DHCP reçoit des demandes de configuration IPv4 des ordinateurs que vous configurez afin d'obtenir automatiquement une adresse IPv4. Il affecte également des paramètres IPv4 supplémentaires à partir des étendues que vous définissez pour chacun des sous-réseaux de votre réseau. Le service DHCP identifie le sous-réseau d'où provient la demande et attribue la configuration IP à partir de l'étendue adéquate.



DCHP simplifie le processus de configuration IP. Toutefois, si vous utilisez DHCP pour affecter des informations IPv4 et si le service est vital pour l'entreprise, vous devez effectuer les tâches suivantes :

- concevoir le service DHCP avec une tolérance de panne de sorte que la défaillance d'un seul serveur n'empêche pas le service de fonctionner ;
- configurer avec soin les étendues sur le serveur DHCP. Si vous faites une erreur, cela peut affecter tout le réseau et empêcher la communication.

Si vous utilisez un ordinateur portable pour vous connecter à plusieurs réseaux (à votre domicile et au bureau, par exemple), une configuration IP différente peut être nécessaire pour chaque réseau. Les systèmes d'exploitation Windows prennent en charge l'utilisation de l'adressage IP privé automatique (APIPA)) ou une autre adresse IP statique pour répondre à ce type de situation.

Lorsque vous configurez des ordinateurs Windows pour obtenir une adresse IPv4 à partir de DHCP, utilisez l'onglet **Configuration alternative** pour contrôler le comportement, si un serveur DHCP n'est pas disponible. Par défaut, Windows utilise l'adressage IP privé automatique pour s'affecter automatiquement une adresse IP comprise dans la plage d'adresses allant de 169.254.0.0 à 169.254.255.255, mais sans passerelle par défaut ni serveur DNS, ce qui entraîne une limitation des fonctionnalités.

L'adressage IP privé automatique est utile pour résoudre les problèmes liés au protocole DHCP. Si l'ordinateur possède une adresse contenue dans la plage d'adressage IP privé automatique, cela signifie qu'il ne peut pas communiquer avec un serveur DHCP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows Server 2012 dispose également des applets de commande Windows PowerShell, que vous pouvez utiliser pour activer le protocole DHCP pour une interface. Le tableau suivant décrit quelques-unes des applets de commande Windows PowerShell qui sont disponibles pour configurer le protocole DHCP pour une interface.

Applet de commande	Description
Get-NetIPInterface	Obtient une liste des interfaces avec leur configuration. Cela n'inclut pas la configuration IPv4 de l'interface.
Set-NetIPInterface	Active ou désactive le protocole DHCP pour une interface.
Get-NetAdapter	Obtient une liste des cartes réseau d'un ordinateur.
Restart-NetAdapter	Désactive et réactive une carte réseau. Cela force un client DHCP à obtenir un nouveau bail DHCP.

Le code suivant illustre la façon dont vous pouvez activer le protocole DHCP pour la carte Connexion au réseau local et vérifier qu'une adresse lui est affectée :

```
Set-NetIPInterface –InterfaceAlias "Connexion au réseau local" –Dhcp Enabled
Restart-NetAdapter –Name "Connexion au réseau local"
```

Outils de résolution de problèmes IPv4

La résolution des problèmes de connectivité IPv4 s'effectue en grande partie via une ligne de commande. Windows Server 2008 propose un certain nombre d'outils en ligne de commande qui vous permettent de diagnostiquer les problèmes réseau.

Vous disposez des outils suivants pour résoudre les problèmes liés à IPv4

- Ipconfig
- Ping
- Tracert
- Pathping
- Telnet
- Netstat
- Moniteur de ressources
- Diagnostics réseau de Windows
- Observateur d'événements

Ipconfig

Ipconfig est un outil en ligne de commande qui affiche la configuration actuelle du réseau TCP/IP. En outre, vous pouvez utiliser la commande **ipconfig** pour actualiser les paramètres DHCP et DNS. Le tableau suivant décrit les options de ligne de commande pour **ipconfig**.

Commande	Description
ipconfig /all	Permet d'afficher des informations de configuration détaillées
ipconfig /release	Permet de libérer la configuration de bail pour la rendre au serveur DHCP
ipconfig /renew	Permet de renouveler la configuration de bail
ipconfig /displaydns	Permet d'afficher les entrées du cache de résolution DNS
ipconfig /flushdns	Permet de vider le cache de résolution DNS

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Ping

Ping est un outil en ligne de commande qui vérifie l'état de la connexion IP à un autre ordinateur TCP/IP. Il envoie des messages de requête d'écho ICMP et affiche la réception des messages de réponse aux requêtes d'écho correspondantes. Ping est la principale commande TCP/IP que vous utilisez pour résoudre les problèmes de connectivité. Toutefois, les pare-feu peuvent bloquer les messages ICMP.

Tracert

Tracert est un outil en ligne de commande qui identifie le chemin d'accès d'un ordinateur de destination en envoyant une série de requêtes d'écho ICMP. Tracert affiche ensuite la liste des interfaces de routeur entre une source et une destination. Cet outil identifie également les routeurs en panne, ainsi que la latence (ou vitesse). Ces résultats peuvent être incorrects si le routeur est occupé, car ce dernier affecte une priorité inférieure aux paquets ICMP.

Pathping

Pathping est un outil en ligne de commande qui trace un itinéraire via le réseau d'une manière semblable à Tracert. Toutefois, Pathping fournit des statistiques plus détaillées sur les étapes individuelles (*tronçons*) du réseau. Pathping peut fournir plus de détails, car il envoie 100 paquets pour chaque routeur, ce qui lui permet d'établir des tendances.

Route

Route est un outil en ligne de commande qui vous permet d'afficher et de modifier la table de routage locale. Vous pouvez l'utiliser pour vérifier la passerelle par défaut, qui est répertoriée sous la forme de l'itinéraire 0.0.0.0. Dans Windows Server 2012, vous pouvez également utiliser les applets de commande Windows PowerShell pour afficher et modifier la table de routage. Les applets de commande qui permettent de visualiser et modifier la table de routage locale sont **Get-NetRoute**, **New-NetRoute** et **Remove-NetRoute**.

Telnet

Vous pouvez utiliser la fonctionnalité Client Telnet pour vérifier si un port serveur est à l'écoute. Par exemple, la commande **telnet 10.10.0.10 25** tente d'ouvrir une connexion au serveur de destination, 10.10.0.10, sur le port SMTP 25. Si le port est actif et à l'écoute, il retourne un message au client Telnet.

Netstat

Netstat est un outil en ligne de commande qui vous permet d'afficher les connexions réseau et les statistiques correspondantes. Par exemple, la commande **netstat –ab** retourne tous les ports d'écoute, ainsi que l'exécutable qui est à l'écoute.

Moniteur de ressources

Le Moniteur de ressources est un outil graphique qui vous permet d'analyser l'utilisation des ressources système. Vous pouvez utiliser le Moniteur de ressources pour afficher les ports TCP et UDP qui sont en cours d'utilisation. Vous pouvez également identifier les applications qui utilisent des ports spécifiques et déterminer la quantité de données qu'elles transfèrent sur ces ports.

Diagnostics Réseau

Utilisez l'outil Diagnostics Réseau de Windows pour diagnostiquer et corriger les problèmes réseau. Au cas où un problème réseau surviendrait avec Windows Server, l'option **Diagnostiquer les problèmes de connexion** vous permet de diagnostiquer le problème et de le résoudre. L'outil Diagnostic Réseau de Windows retourne une description du problème, ainsi qu'une éventuelle solution. Toutefois, la solution peut nécessiter l'intervention manuelle de l'utilisateur.

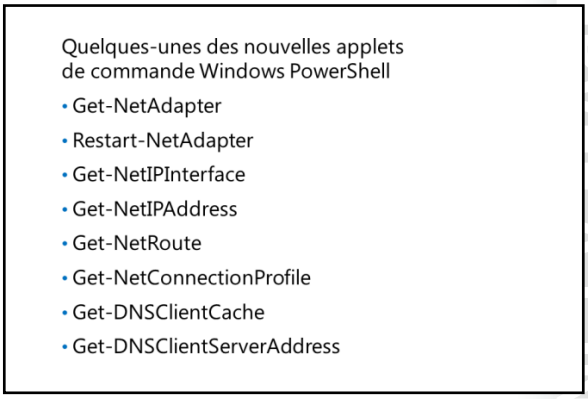
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Observateur d'événements

Les *journaux d'événements* sont des fichiers qui consignent des événements importants sur un ordinateur, tels qu'une erreur rencontrée par un processus. Lorsque ces événements se produisent, le système d'exploitation Windows enregistre l'événement dans un journal des événements approprié. Vous pouvez utiliser l'Observateur d'événements pour lire le journal des événements. Les conflits IP, qui peuvent empêcher les services de démarrer, sont listés dans le journal des événements système.

Utilisation des applets de commande Windows PowerShell pour résoudre les problèmes liés à IPv4

Windows PowerShell dans Windows Server 2012 dispose d'applets de commande de configuration réseau supplémentaires. Vous pouvez les utiliser à la place des outils en ligne de commande pour résoudre les problèmes. Même si vous pouviez utiliser Windows PowerShell dans les versions antérieures de Windows Server pour configurer le réseau et résoudre les problèmes inhérents, vous étiez obligé de recourir aux objets WMI (Windows Management Instrumentation), qui sont plus difficiles à utiliser que les applets de commande Windows PowerShell natives.

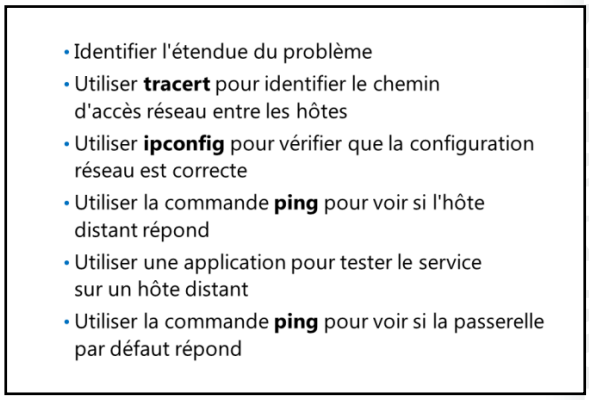


Le tableau suivant répertorie quelques-unes des nouvelles applets de commande Windows PowerShell que vous pouvez utiliser.

Applet de commande	Rôle
Get-NetAdapter	Obtient une liste des cartes réseau d'un ordinateur.
Restart-NetAdapter	Désactive et réactive une carte réseau.
Get-NetIPInterface	Obtient une liste des interfaces avec leur configuration.
Get-NetIPAddress	Obtient une liste des adresses IP configurées pour les interfaces.
Get-NetRoute	Obtient la liste des itinéraires dans la table de routage locale.
Get-NetConnectionProfile	Obtient le type de réseau (public, privé, domaine) pour lequel une carte réseau est connectée.
Get-DNSClientCache	Obtient la liste des noms DNS résolus qui sont stockés dans le cache client DNS.
Get-DNSClientServerAddress	Obtient la liste des serveurs DNS utilisés pour chaque interface.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Processus de résolution des problèmes d'IPv4



La première étape de la résolution d'un problème réseau consiste à identifier l'étendue du problème. Les causes d'un problème qui affecte un seul utilisateur sont très probablement différentes des causes d'un problème qui affecte tous les utilisateurs. Si un problème n'affecte qu'un seul utilisateur, cela signifie que ce problème est probablement lié à la configuration de l'ordinateur utilisé. Si un problème affecte tous les utilisateurs, cela signifie qu'il s'agit probablement d'un problème de configuration du serveur ou de configuration réseau. Si un problème affecte uniquement un groupe d'utilisateurs, vous devez déterminer le dénominateur commun à ce groupe d'utilisateurs.

Pour résoudre les problèmes de communication réseau, vous devez comprendre l'ensemble du processus de communication. Vous ne pouvez identifier le point de rupture du processus et de blocage de la communication que si vous comprenez comment fonctionne l'ensemble du processus de communication. Pour comprendre le fonctionnement du processus global de communication, vous devez comprendre comment fonctionne la configuration du routage et du pare-feu sur votre réseau. Pour faciliter l'identification de l'itinéraire de routage via votre réseau, vous pouvez utiliser **tracert**.

Voici certaines des étapes que vous pouvez utiliser pour identifier la cause des problèmes de communication réseau :

1. Si vous savez quelle est la configuration réseau appropriée pour l'hôte, utilisez **ipconfig** afin de vérifier s'il s'agit de la configuration appliquée. Si **ipconfig** retourne une adresse sur le réseau 169.254.0.0/16, cela indique que l'hôte n'a pas réussi à obtenir une adresse IP auprès du serveur DHCP.
2. Utilisez la commande **ping** pour voir si l'hôte distant répond. Si vous utilisez **ping** pour retourner le nom DNS de l'hôte distant, cela vous permet de vérifier la résolution de noms et la réponse de l'hôte. Gardez à l'esprit que le Pare-feu Windows sur les serveurs membres et les ordinateurs clients bloque souvent les tentatives d'exécution de la commande ping. Dans ce cas, l'absence de réponse à l'exécution de la commande ping ne signifie pas nécessairement que l'hôte distant n'est pas fonctionnel. Si l'exécution de la commande ping aboutit pour d'autres hôtes distants du même réseau, cela indique souvent que le problème se situe sur l'hôte distant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

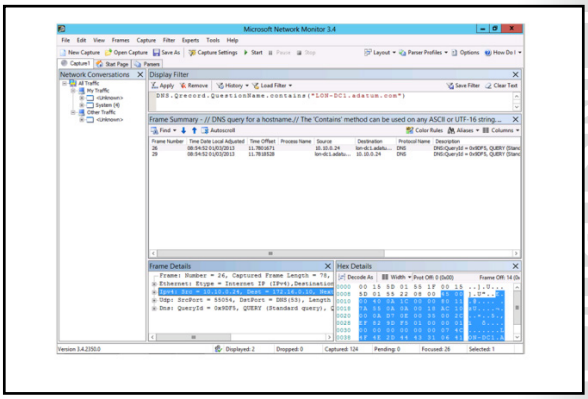
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Vous pouvez utiliser une application pour tester le service auquel vous vous connectez sur l'hôte distant. Par exemple, utilisez Windows Internet Explorer® pour tester la connectivité à un serveur Web. Vous pouvez également utiliser Telnet pour vous connecter au port de l'application distante.
4. Utilisez la commande **ping** pour voir si la passerelle par défaut répond. La plupart des routeurs répondent aux requêtes ping. Si vous n'obtenez pas de réponse lorsque vous effectuez un test ping de la passerelle par défaut, cela signifie qu'il existe probablement une erreur de configuration sur l'ordinateur client. En effet, il est possible que la passerelle par défaut soit configurée de manière incorrecte. Il est possible également que le routeur rencontre des erreurs.

Remarque : Vous pouvez forcer la commande **ping** à utiliser IPv4 au lieu d'IPv6 à l'aide de l'option **-4**.

Question : Existe-t-il d'autres étapes que vous pouvez utiliser pour résoudre les problèmes de connectivité réseau ?

Qu'est-ce que le Moniteur réseau ?



Le Moniteur réseau est un analyseur de paquets qui vous permet de capturer et d'examiner les paquets réseau du réseau auquel votre ordinateur est connecté. La capture de paquets est une technique de résolution de problèmes avancée qui vous aide à identifier les problèmes réseau inhabituels et à élaborer une solution. Par exemple, en examinant les paquets transmis sur un réseau, vous pouvez éventuellement voir des erreurs qui ne sont pas signalées par une application.

Vous pouvez installer le Moniteur réseau sur chaque système d'extrémité du processus de communication ou sur un troisième ordinateur. Si vous installez le Moniteur réseau sur un troisième ordinateur, vous devez configurer la mise en miroir des ports sur les commutateurs réseau. Veillez à configurer la mise en miroir des ports pour copier les paquets réseau destinés aux systèmes d'extrémité du processus de communication, vers le port du commutateur auquel est connecté l'ordinateur disposant du Moniteur réseau. Le Moniteur réseau peut analyser les paquets envoyés à d'autres ordinateurs, car il fonctionne en mode de proximité.

Vous pouvez télécharger le Moniteur réseau à partir du site Web de téléchargement Microsoft, puis l'installer sur un poste de travail qui exécute Windows 8 ou Windows Server 2012. Une fois installé, le Moniteur réseau se lie aux cartes réseau locales. Lorsque vous lancez le Moniteur réseau, vous pouvez voir des captures existantes ou commencer une nouvelle capture.

Utilisation du Moniteur réseau

Une fois que vous avez capturé des paquets réseau, vous devez pouvoir interpréter ce que vous voyez et savoir si le comportement est attendu ou non. Pour vous aider, le Moniteur réseau affiche les paquets sous forme de liste résumée dans le volet Résumé de la trame.

Ce volet affiche tous les paquets capturés et fournit les informations suivantes :

- Date et heure : cela vous permet de déterminer l'ordre dans lequel les paquets ont été transmis.
- Source et destination : cela indique les adresses IP source et de destination pour vous permettre de déterminer quels sont les ordinateurs impliqués dans le dialogue.
- Nom du protocole : le protocole de plus haut niveau que le Moniteur réseau peut identifier est répertorié, par exemple ARP, ICMP, TCP et SMB. Le fait de connaître le protocole de plus haut niveau vous permet d'identifier les services qui peuvent être liés aux problèmes que vous essayez de résoudre.

Lorsque vous sélectionnez une trame dans le volet Résumé de la trame, le volet Détails de la trame est mis à jour à l'aide du contenu de cette trame particulière. Vous pouvez passer en revue les détails de la trame, en examinant au fur et à mesure le contenu de chaque élément.

Chaque couche de l'architecture réseau (à partir de l'application en allant vers le bas) encapsule ses données dans le conteneur de la couche située en dessous. En d'autres termes, une requête HTTP est encapsulée dans un paquet IPv4, qui à son tour est encapsulé dans une trame Ethernet.

Lorsque vous avez recueilli une grande quantité de données, il peut s'avérer difficile de déterminer quelles sont les trames pertinentes pour votre problème spécifique. Vous pouvez utiliser le filtrage pour afficher uniquement les trames dignes d'intérêt. Par exemple, vous pouvez choisir d'afficher uniquement les paquets DNS.

Démonstration : Comment capturer et analyser le trafic réseau à l'aide du Moniteur réseau

Vous pouvez utiliser le Moniteur réseau pour capturer et afficher les paquets qui sont transmis sur le réseau. Cela vous permet d'afficher des informations détaillées qui ne sont pas visibles normalement. Ce type d'information peut être utile à la résolution des problèmes.

Dans cette démonstration, vous allez apprendre à :

- capturer le trafic réseau à l'aide du Moniteur réseau ;
- analyser le trafic réseau capturé ;
- filtrer le trafic réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Capturer le trafic réseau à l'aide du Moniteur réseau

Préparer une capture de paquets

1. Connectez-vous à LON-SVR2 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez une invite Windows PowerShell et exécutez la commande suivante :
   - **ipconfig /flushdns**
3. Ouvrez Microsoft Network Monitor 3.4, puis créez un onglet de nouvelle capture.

Capturer les paquets d'une requête ping

1. Dans le Moniteur réseau, démarrez une capture de paquets.
2. À l'invite Windows PowerShell, effectuez un test ping de **LON-DC1.adatum.com**.
3. Dans le Moniteur réseau, arrêtez la capture de paquets.

Analyser le trafic réseau capturé

1. Dans le Moniteur réseau, faites défiler l'affichage vers le bas et sélectionnez le premier paquet **ICMP**.
2. Développez la partie **Icmp** du paquet pour vérifier qu'il s'agit d'un **Echo Request Message**. Il s'agit d'une requête ping.
3. Développez la partie **Ipv4** du paquet pour afficher les adresses IP source et de destination.
4. Développez la partie **Ethernet** du paquet pour afficher les adresses MAC source et de destination.
5. Sélectionnez le deuxième paquet ICMP.
6. Dans la partie **Icmp** du paquet, vérifiez qu'il s'agit d'une **Réponse d'écho**. Il s'agit de la réponse à la requête ping.

Filtrer le trafic réseau

1. Dans le Moniteur réseau, dans le volet Filtre d'affichage, chargez le filtre DNS standard **DnsQueryName**.
2. Modifiez le filtre à appliquer aux requêtes DNS pour **LON-DC1.adatum.com**.
3. Appliquez le filtre.
4. Vérifiez que les paquets ont été filtrés afin d'afficher uniquement ceux qui correspondent au filtre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation du protocole IPv4

Scénario

La société A. Datum Corporation a un bureau et un centre de données informatiques à Londres qui prennent en charge le site de Londres ainsi que d'autres sites. Ils ont récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8. Vous avez récemment accepté une promotion au sein de l'équipe d'assistance technique des serveurs. L'une de vos premières missions consiste à configurer le service d'infrastructure pour une nouvelle filiale.

Après une évaluation de la sécurité, votre responsable vous a demandé de calculer de nouveaux sous-réseaux pour permettre à la filiale de prendre en charge la segmentation du trafic réseau. Vous devez également résoudre un problème de connectivité sur un serveur de la filiale.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- identifier les sous-réseaux appropriés pour un ensemble spécifique d'exigences ;
- résoudre les problèmes de connectivité IPv4.

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-RTR 22410B-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 **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Identification des sous-réseaux appropriés

Scénario

La nouvelle filiale est configurée avec un seul sous-réseau. Après une évaluation de la sécurité, toutes les configurations réseau des filiales sont modifiées afin que les serveurs soient placés sur un sous-réseau distinct des ordinateurs clients. Vous devez calculer le nouveau masque de sous-réseau et les passerelles par défaut des sous-réseaux dans votre filiale.

Le réseau actuel de votre filiale est 192.168.98.0/24. Ce réseau doit être subdivisé en trois sous-réseaux, comme suit :

- Un sous-réseau avec au moins 100 adresses IP pour les clients
- Un sous-réseau avec au moins 10 adresses IP pour les serveurs
- Un sous-réseau avec au moins 40 adresses IP pour une extension future

Les tâches principales de cet exercice sont les suivantes :

1. Calculer les bits requis pour prendre en charge les hôtes sur chaque sous-réseau
2. Calculer les masques de sous-réseau et les ID réseau

▶ Tâche 1 : Calculer les bits requis pour prendre en charge les hôtes sur chaque sous-réseau

1. Combien de bits sont requis pour prendre en charge 100 hôtes sur le sous-réseau client ?
2. Combien de bits sont requis pour prendre en charge 10 hôtes sur le sous-réseau serveur ?
3. Combien de bits sont requis pour prendre en charge 40 hôtes sur le sous-réseau de l'extension future ?
4. Si tous les sous-réseaux sont de la même taille, peuvent-ils être adaptés ?
5. Quelle fonctionnalité permet à un réseau unique d'être divisé en sous-réseaux de différentes tailles ?
6. Combien de bits hôtes utiliserez-vous pour chaque sous-réseau ? Utilisez l'allocation la plus simple possible, c'est-à-dire un sous-réseau de grande taille et deux sous-réseaux plus petits de même taille.

▶ Tâche 2 : Calculer les masques de sous-réseau et les ID réseau

1. Compte tenu du nombre de bits hôtes alloués, quel est le masque de sous-réseau que vous allez utiliser pour le sous-réseau client ? Calculez le masque de sous-réseau au format binaire et décimal.
    - Le sous-réseau client utilise 7 bits pour l'ID hôte. Par conséquent, vous allez utiliser 25 bits pour le masque de sous-réseau.

Binaire	Décimal

2. Compte tenu du nombre de bits hôtes alloués, quel est le masque de sous-réseau que vous allez utiliser pour le sous-réseau serveur ? Calculez le masque de sous-réseau au format binaire et décimal.
   - Le sous-réseau serveur utilise 6 bits pour l'ID hôte. Par conséquent, vous allez utiliser 26 bits pour le masque de sous-réseau.

Binaire	Décimal

3. Compte tenu du nombre de bits hôtes alloués, quel est le masque de sous-réseau que vous allez utiliser pour le sous-réseau de l'extension future ? Calculez le masque de sous-réseau au format binaire et décimal.
   - Le sous-réseau de l'extension future utilise 6 bits pour l'ID hôte. Par conséquent, vous allez utiliser 26 bits pour le masque de sous-réseau.

Binaire	Décimal

4. Pour le sous-réseau client, définissez l'ID réseau, le premier hôte disponible, le dernier hôte disponible et l'adresse de diffusion. Supposons que le sous-réseau client soit le premier sous-réseau alloué à partir du pool d'adresses disponibles. Calculez les versions binaires et décimales de chaque adresse.

Description	Binaire	Décimal
ID réseau		
Premier hôte		
Dernier hôte		
Diffusion		

5. Pour le sous-réseau serveur, définissez l'ID réseau, le premier hôte disponible, le dernier hôte disponible et l'adresse de diffusion. Supposons que le sous-réseau serveur soit le deuxième sous-réseau alloué à partir du pool d'adresses disponibles. Calculez les versions binaires et décimales de chaque adresse.

Description	Binaire	Décimal
ID réseau		
Premier hôte		
Dernier hôte		
Diffusion		

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Pour le sous-réseau à allouer ultérieurement, définissez l'ID réseau, le premier hôte disponible, le dernier hôte disponible et l'adresse de diffusion. Supposons que le sous-réseau à allouer ultérieurement soit le troisième sous-réseau alloué à partir du pool d'adresses disponibles. Calculez les versions binaires et décimales de chaque adresse.

Description	Binaire	Décimal
ID réseau		
Premier hôte		
Dernier hôte		
Diffusion		

Résultats : À la fin de cet exercice, vous aurez identifié les sous-réseaux requis pour répondre aux exigences du scénario de l'atelier pratique.

Exercice 2 : Résolution des problèmes liés à IPv4

Scénario

Un serveur de la filiale est incapable de communiquer avec le contrôleur de domaine du siège. Vous devez résoudre le problème de connectivité réseau.

Les tâches principales de cet exercice sont les suivantes :

1. Préparer la résolution des problèmes
2. Résoudre les problèmes de connectivité IPv4 entre LON-SVR2 et LON-DC1

▶ Tâche 1 : Préparer la résolution des problèmes

1. Sur LON-SVR2, ouvrez **Windows PowerShell**.
2. Dans Windows PowerShell, effectuez un test ping de **LON-DC1** et vérifiez si ce dernier est fonctionnel.
3. Exécutez le script **Break.ps1** situé dans **\\LON-DC1\E$\Labfiles\Mod05**. Ce script crée le problème que vous allez résoudre au cours de la prochaine tâche.

▶ Tâche 2 : Résoudre les problèmes de connectivité IPv4 entre LON-SVR2 et LON-DC1

1. Utilisez votre connaissance d'IPv4 pour résoudre le problème de connectivité entre LON-SVR2 et LON-DC1. Pensez à utiliser les outils suivants :
   - **Ipconfig**
   - **Ping**
   - **Tracert**
   - **Route**
   - Moniteur réseau

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

2. Une fois que vous avez résolu le problème, effectuez un test ping de LON-DC1 à partir de LON-SVR2 pour vérifier que le problème est bien résolu.

Remarque : Si vous avez encore le temps, exécutez un script supplémentaire de création de problème à partir de **\\LON-DC1\E$\Labfiles\Mod05** et résolvez le problème spécifique.

Résultats : À la fin de cet atelier pratique, vous aurez résolu un problème de connectivité IPv4.

▶ 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 **22410B-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 **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

Lors de l'implémentation du protocole IPv4, utilisez les meilleures pratiques suivantes :

- Tenez compte des besoins de croissance lors de la planification des sous-réseaux IPv4. Vous aurez ainsi la garantie de ne pas avoir à modifier votre modèle de configuration IPv4.
- Définissez des objectifs pour les plages d'adresses et les sous-réseaux spécifiques. Cela vous permet d'identifier facilement les hôtes en fonction de leur adresse IP et d'utiliser des pare-feu pour augmenter la sécurité.
- Utilisez des adresses IPv4 dynamiques pour les clients. Il est beaucoup plus facile de gérer la configuration IPv4 des ordinateurs clients avec le protocole DHCP plutôt qu'une configuration manuelle.
- Utilisez des adresses IPv4 statiques pour les serveurs. Lorsque les serveurs ont une adresse IPv4 statique, il est plus facile d'identifier l'emplacement des services sur le réseau.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Conflits d'adresses IP	
Plusieurs passerelles par défaut définies	
Configuration IPv4 incorrecte	

Questions de contrôle des acquis

Question : Vous occupez depuis peu un poste d'administrateur de serveur dans une petite organisation implantée à un seul emplacement. L'organisation utilise la plage d'adresses 131.107.88.0/24 pour le réseau interne. Est-ce un problème ?

Question : Vous travaillez pour une organisation qui fournit des services d'hébergement Web à d'autres organisations. Vous disposez d'un seul réseau /24 via votre fournisseur de services Internet pour les hôtes Web. Vous êtes presque à court d'adresses IPv4 et avez demandé à votre fournisseur de services Internet une plage d'adresses supplémentaires. Dans l'idéal, vous souhaitez créer un super-réseau en associant le réseau existant au nouveau réseau. Existe-t-il des exigences particulières pour la création d'un super-réseau ?

Question : Vous avez installé une nouvelle application Web qui s'exécute sur un numéro de port non standard. Un collègue teste l'accès à la nouvelle application Web et indique qu'il ne peut pas s'y connecter. Quelles sont les causes les plus probables de son problème ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Outils

Outil	Utilisation	Emplacement
Moniteur réseau	Capturer et analyser le trafic réseau	Téléchargement depuis le site Web Microsoft
Ipconfig	Afficher la configuration réseau	Invite de commandes
Ping	Vérifier la connectivité réseau	Invite de commandes
Tracert	Vérifier le chemin d'accès réseau entre les hôtes	Invite de commandes
Pathping	Vérifier le chemin d'accès réseau et la fiabilité entre les hôtes	Invite de commandes
Route	Afficher et configurer la table de routage locale	Invite de commandes
Telnet	Tester la connectivité d'un port spécifique	Invite de commandes
Netstat	Afficher les informations de connectivité réseau	Invite de commandes
Moniteur de ressources	Afficher les informations de connectivité réseau	Outils du Gestionnaire de serveur
Diagnostics réseau de Windows	Diagnostiquer un problème de connexion réseau	Propriétés de la connexion réseau
Observateur d'événements	Afficher les événements système liés au réseau	Outils du Gestionnaire de serveur

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6

Implémentation du protocole DHCP (Dynamic Host Configuration Protocol)

Table des matières :

Vue d'ensemble du module **6-1**

Leçon 1 : Installation d'un rôle Serveur DHCP **6-2**

Leçon 2 : Configuration des étendues DHCP **6-8**

Leçon 3 : Gestion d'une base de données DHCP **6-13**

Leçon 4 : Sécurisation et surveillance DHCP **6-17**

Atelier pratique : Implémentation de DHCP **6-23**

Contrôle des acquis et éléments à retenir **6-28**

Vue d'ensemble du module

Le protocole DHCP (Dynamic Host Configuration Protocol) joue un rôle important dans l'infrastructure de 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® (WDS) et la protection d'accès réseau (NAP). Pour prendre en charge une infrastructure réseau basée sur Windows Server et résoudre les éventuels problèmes, il est important que vous sachiez déployer et configurer le rôle Serveur DHCP et résoudre les problèmes associés.

Objectifs

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

- installer le rôle Serveur DHCP ;
- configurer les étendues DHCP ;
- gérer une base de données DHCP ;
- sécuriser et surveiller le rôle Serveur DHCP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Installation d'un rôle Serveur DHCP

L'utilisation du protocole DHCP peut contribuer à simplifier la configuration d'un ordinateur client. Cette leçon décrit les avantages de DHCP, présente le fonctionnement de ce protocole et explique comment contrôler DHCP sur un réseau Windows Server 2012 avec les services de domaine Active Directory® (AD DS).

Objectifs de la leçon

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

- décrire les avantages de l'utilisation de DHCP ;
- expliquer comment DHCP alloue des adresses IP aux clients réseau ;
- décrire le fonctionnement du processus de création d'un bail DHCP ;
- décrire le fonctionnement du processus de renouvellement d'un bail DHCP ;
- décrire le rôle d'un agent de relais DHCP ;
- expliquer comment un rôle Serveur DHCP est autorisé ;
- expliquer comment ajouter et autoriser le rôle Serveur DHCP.

Avantages liés à l'utilisation du protocole DHCP

Le protocole DHCP simplifie la configuration des clients IP dans un environnement réseau. Si vous n'utilisez pas DHCP, à chaque fois que vous ajoutez un client à un réseau, vous devez le configurer en reprenant les informations du réseau sur lequel il était installé, notamment l'adresse IP, le masque de sous-réseau du réseau et la passerelle par défaut permettant l'accès à d'autres réseaux.

Le protocole DHCP simplifie et réduit le travail administratif grâce à l'usage de la configuration automatique du protocole IP

Configuration automatique du protocole IP	Configuration manuelle du protocole IP
Les adresses IP sont fournies automatiquement	Les adresses IP sont entrées manuellement
L'exactitude des informations de configuration est garantie	Risque de saisie incorrecte d'une adresse IP
La configuration des clients est mise à jour automatiquement	Des problèmes de communications et de réseau peuvent en découler
Une source courante de problèmes réseau est éliminée	Le déplacement fréquent d'ordinateurs décuple les tâches d'administration

Gérer les nombreux ordinateurs qui constituent un réseau devient une tâche très fastidieuse lorsqu'elle est effectuée manuellement. Il n'est pas rare que des sociétés aient des milliers de périphériques informatiques à gérer : périphériques portables, ordinateurs de bureau, ordinateurs portables, etc. Il n'est pas possible de gérer manuellement les configurations IP de réseau pour les entreprises de cette taille.

Avec le rôle Serveur DHCP, vous faites en sorte que tous les clients disposent d'informations de configuration appropriées, ce qui contribue à éliminer les erreurs humaines pendant la configuration. Lorsque d'importantes informations de configuration changent dans le réseau, il est possible de les mettre à jour à l'aide du rôle Serveur DHCP sans qu'il soit nécessaire d'intervenir directement sur chaque ordinateur.

De même, DHCP est un service clé pour les utilisateurs itinérants qui changent souvent de réseau. DHCP permet aux administrateurs réseau de fournir des informations de configuration réseau complexes aux utilisateurs non techniciens, sans que ceux-ci n'aient à se préoccuper des détails de configuration de leur réseau.

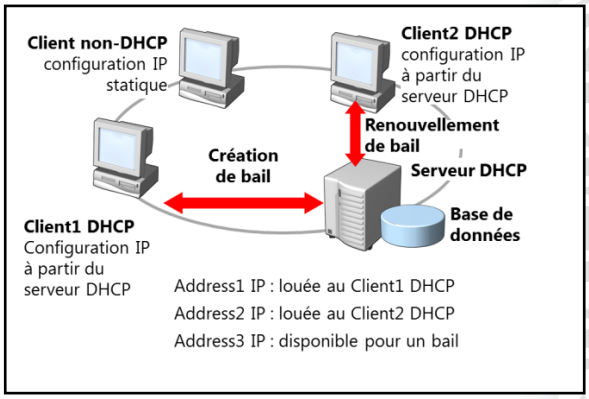
La configuration avec état et sans état de DHCP version 6 (v6) est prise en charge pour la configuration de clients dans un environnement IPv6. La configuration avec état intervient lorsque le serveur DHCPv6 attribue l'adresse IPv6 au client, en même temps que d'autres données DHCP. La configuration 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 d'IPv6.

La protection d'accès réseau (NAP) fait partie d'un nouvel ensemble d'outils qui peuvent empêcher l'accès total à l'intranet aux ordinateurs qui ne sont pas conformes aux exigences d'intégrité du système. La protection d'accès réseau (NAP) couplée à DHCP contribue à isoler du réseau d'entreprise les ordinateurs susceptibles d'être infectés par un programme malveillant. La protection d'accès réseau par DHCP permet aux administrateurs de s'assurer que les clients DHCP sont en conformité avec les stratégies de sécurité internes. Par exemple, tous les clients réseau doivent être à jour et disposer d'un programme antivirus valide et à jour avant qu'une configuration IP permettant un accès total à l'intranet ne leur soit attribuée.

Vous pouvez installer DHCP en tant que rôle sur une installation minimale (Server Core) de Windows Server 2012. Server Core vous permet de créer un serveur avec une exposition aux attaques réduite. Pour gérer DHCP à partir de Server Core, vous devez installer et configurer le rôle à partir de l'interface de ligne de commande. Vous pouvez également gérer le rôle DHCP s'exécutant sur l'installation Server Core de Windows Server 2012 à partir d'une console basée sur une interface graphique utilisateur dans laquelle le rôle DHCP est déjà installé.

Comment le protocole DHCP alloue des adresses IP

DHCP alloue les adresses IP en suivant un processus dynamique également appelé *bail*. Bien que vous puissiez définir la durée du bail sur Illimité, vous définissez en général cette durée sur quelques heures ou jours. La durée du bail par défaut pour les clients câblés est de huit jours, et de trois jours pour les clients sans fil.



DHCP utilise des messages IP pour établir des communications. Par conséquent, les serveurs DHCP sont limités aux communications à l'intérieur de leur sous-réseau IP. Cela signifie que dans bon nombre de réseaux, il existe un serveur DHCP pour chaque sous-réseau IP.

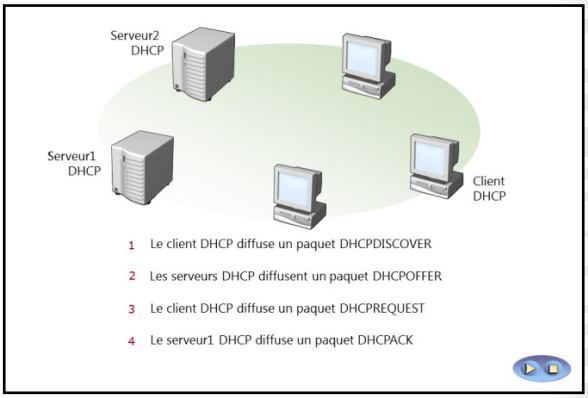
Pour qu'un ordinateur soit considéré comme un client DHCP, il doit être configuré pour obtenir une adresse IP automatiquement. Par défaut, tout ordinateur est configuré pour obtenir une adresse IP automatiquement. Dans un réseau sur lequel un serveur DHCP est installé, un client DHCP répondra à un message DHCP.

Si un ordinateur est configuré avec une adresse IP par un administrateur, il dispose d'une adresse IP statique, est considéré comme un client non-DHCP et ne communiquera pas avec un serveur DHCP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

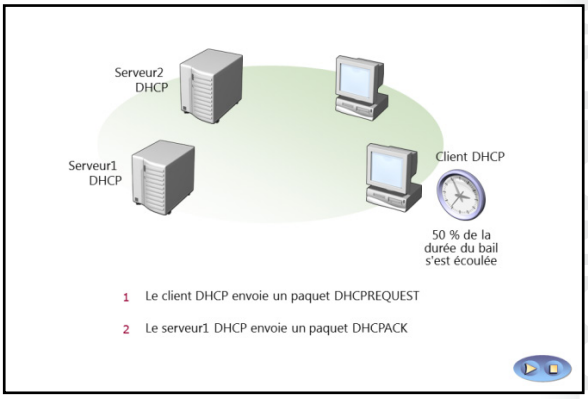
Comment fonctionne le processus de création d'un bail DHCP ?



Vous utilisez le processus de génération de bail DHCP en quatre étapes pour attribuer une adresse IP aux clients. Le fait de comprendre le fonctionnement de chaque étape vous aide à résoudre les problèmes survenant lorsque les clients ne parviennent pas à obtenir une adresse IP. Les quatre étapes sont les suivantes :

1. Le client DHCP diffuse un paquet DHCPDISCOVER à chaque ordinateur du sous-réseau. Seul un ordinateur qui a le rôle Serveur DHCP ou un ordinateur ou routeur qui exécute un agent de relais DHCP répond. Dans ce dernier cas, l'agent de relais DHCP transfère le message au serveur DHCP avec lequel il est configuré.
2. Un serveur DHCP répond avec un paquet DHCPOFFER. Ce paquet contient une adresse potentielle pour le client.
3. Le client reçoit le paquet DHCPOFFER. Il peut recevoir des paquets de plusieurs serveurs, auquel cas il sélectionne généralement le serveur qui a répondu le plus rapidement à son paquet DHCPDISCOVER. Il s'agit habituellement du serveur DHCP le plus proche du client. Le client diffuse alors un paquet DHCPREQUEST qui contient un identificateur de serveur. Ce dernier indique aux serveurs DHCP qui reçoivent le paquet DHCPOFFER quel serveur le client a choisi d'accepter.
4. Les serveurs DHCP reçoivent le paquet DHCPREQUEST. Les serveurs non acceptés par le client utilisent le message comme notification indiquant que le client refuse l'offre du serveur. Le serveur choisi stocke l'adresse IP du client dans la base de données DHCP et répond par un message DHCPACK. Si, pour une raison ou une autre, le serveur DHCP ne peut pas fournir l'adresse contenue dans le paquet DHCPOFFER initial, le serveur DHCP envoie un message DHCPNAK.

Comment fonctionne le processus de renouvellement d'un bail DHCP ?



Lorsque le bail DHCP 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 utiliser l'adresse IP attribuée par le serveur DHCP sur une longue période s'ils fonctionnent de façon continue sur un réseau sans être arrêtés.

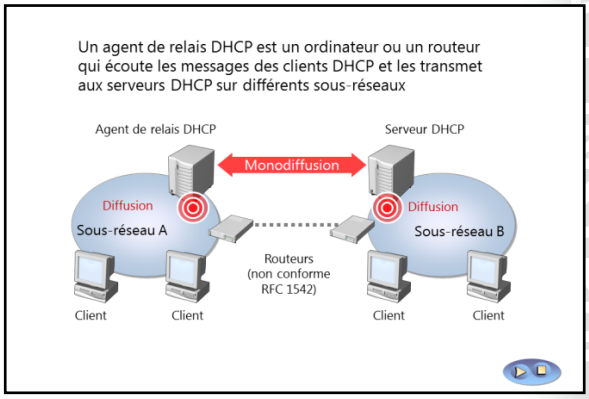
Pour renouveler le bail de l'adresse IP, le client diffuse un message DHCPREQUEST. Le serveur qui a initialement loué l'adresse IP renvoie au client un message DHCPACK qui contient tous les nouveaux paramètres qui n'existaient pas lors de la création du bail.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si le client DHCP ne peut pas contacter le serveur DHCP, alors le client attend que 87,5 pour cent de la durée du bail soient écoulés. Si le renouvellement échoue, ce qui signifie que 100 pour cent de la durée du bail sont écoulés, l'ordinateur client tente d'entrer en contact avec la passerelle par défaut configurée. Si la passerelle ne répond pas, le client suppose qu'elle est sur un nouveau sous-réseau et passe à la phase de détection. Il tente alors d'obtenir une configuration IP de n'importe quel serveur DHCP.

Les ordinateurs clients tentent également de renouveler le bail pendant le processus de démarrage ou lorsque l'ordinateur détecte une modification du réseau. Ceci est dû au fait que les ordinateurs clients peuvent avoir été déplacés alors qu'ils étaient hors connexion ; par exemple, un ordinateur portable peut avoir été branché à un nouveau sous-réseau. Si le renouvellement réussit, la période de bail est réinitialisée. Dans Windows Server 2012, le rôle DHCP prend en charge une nouvelle fonctionnalité appelée protocole de basculement de serveur DHCP. Ce protocole active la synchronisation des informations de bail entre les serveurs DHCP et augmente la disponibilité du service DHCP. Si un serveur DHCP n'est pas disponible, les autres serveurs DHCP continuent de desservir les clients sur le même sous-réseau.

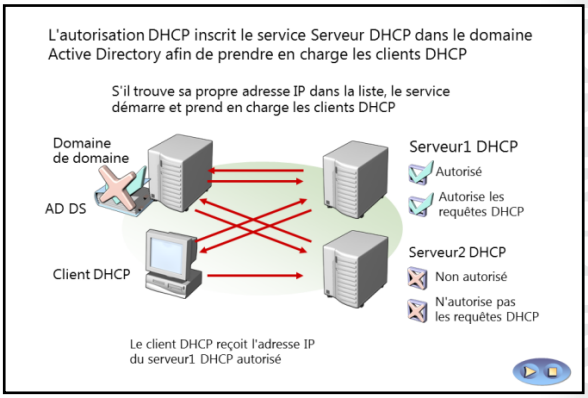
Définition d'un agent de relais DHCP



DHCP utilise des messages IP pour établir des communications. Par conséquent, les serveurs DHCP sont limités aux communications à l'intérieur de leur sous-réseau IP. Cela signifie que dans bon nombre de réseaux, il existe un serveur DHCP pour chaque sous-réseau IP. Or, si les sous-réseaux sont nombreux, le déploiement de serveurs pour chaque sous-réseau peut s'avérer onéreux. Un même serveur DHCP peut desservir des groupes de sous-réseaux plus petits. Pour pouvoir répondre à une requête d'un client DHCP, le serveur DHCP doit être en mesure de recevoir les requêtes DHCP. Pour cela, vous devez configurer un agent de relais DHCP sur chaque sous-réseau. Un *agent de relais DHCP* est un ordinateur ou un routeur qui écoute les messages des clients DHCP et les transmet aux serveurs DHCP sur différents sous-réseaux.

Avec l'agent de relais DHCP, les paquets de diffusion DHCP peuvent être relayés dans un autre sous-réseau IP via un routeur. Ensuite, vous pouvez configurer l'agent de relais DHCP dans le sous-réseau qui a besoin d'adresses IP. En outre, vous pouvez configurer l'agent avec l'adresse IP du serveur DHCP. L'agent pourra ainsi capturer les messages du client et les transférer au serveur DHCP d'un autre sous-réseau. Vous pouvez également relayer des paquets DHCP dans d'autres sous-réseaux à l'aide d'un routeur compatible avec la norme RFC 1542.

Autorisation du serveur DHCP



Le protocole DHCP permet à un ordinateur client d'acquérir des informations de configuration sur le réseau dans lequel il démarre. La communication DHCP intervient généralement avant toute authentification de l'utilisateur ou de l'ordinateur. Par ailleurs, comme le protocole DHCP est basé sur des diffusions IP, un serveur DHCP mal configuré au sein d'un réseau peut fournir des informations incorrectes aux clients. Pour éviter cela, le serveur doit être autorisé. L'*autorisation DHCP* est le processus qui consiste à inscrire le service Serveur DHCP dans le domaine Active Directory afin de prendre en charge les clients DHCP.

Configuration requise pour Active Directory

Vous devez autoriser le rôle serveur DHCP de Windows Server 2012 dans AD DS avant de pouvoir commencer à louer des adresses IP. Il est possible d'affecter un seul serveur DHCP à la distribution d'adresses IP pour les sous-réseaux qui contiennent plusieurs domaines AD DS. Par conséquent, le serveur DHCP doit être autorisé par un compte d'administrateur d'entreprise.

Remarques concernant les serveurs DHCP autonomes

Un serveur DHCP autonome est un ordinateur qui exécute Windows Server 2012, qui ne fait pas partie d'un domaine AD DS et sur lequel le rôle Serveur DHCP a été installé et configuré. Si le serveur DHCP autonome détecte un serveur DHCP autorisé dans le domaine, il ne loue pas d'adresses IP et s'arrête automatiquement.

Serveurs DHCP non autorisés

De nombreux périphériques réseau intègrent un logiciel serveur DHCP, ce qui explique que bon nombre de routeurs peuvent faire office de serveur DHCP. Or, il est fréquent que ces serveurs ne reconnaissent pas les serveurs autorisés par DHCP, si bien qu'ils sont à même de louer des adresses IP aux clients. Dans ce cas, vous devez mener l'enquête afin de détecter les serveurs DHCP non autorisés, qu'ils soient installés sur des périphériques ou des serveurs non-Microsoft. Une fois que vous les avez détectés, vous devez désactiver le service DHCP sur ces serveurs. Vous pouvez rechercher l'adresse IP du serveur DHCP en exécutant la commande **ipconfig /all** sur l'ordinateur client DHCP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Ajout du rôle Serveur DHCP

Dans cette démonstration, vous allez apprendre à installer et autoriser le rôle Serveur DHCP.

Procédure de démonstration

Installer le rôle Serveur DHCP

1. Connectez-vous à LON-SVR1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd.**
2. Ouvrez le **Gestionnaire de serveur** et installez le rôle **Serveur DHCP**.
3. Dans l'Assistant Ajout de rôles, acceptez tous les paramètres par défaut.
4. Fermez le Gestionnaire de serveur.

Autoriser le serveur DHCP

1. Basculez vers LON-SVR1.
2. Ouvrez la console DHCP.
3. Autorisez le serveur **lon-svr1.adatum.com** dans AD DS.

Remarque : Laissez tous les ordinateurs virtuels dans leur état actuel pour la démonstration suivante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration des étendues DHCP

Une fois le rôle DHCP installé sur un serveur, vous devez configurer les étendues DHCP. L'étendue DHCP est la méthode privilégiée pour configurer les options d'un groupe d'adresses IP. Elle est basée sur un sous-réseau IP et certains de ses paramètres peuvent être spécifiques au matériel ou à des groupes de clients personnalisés. Cette leçon présente les étendues DHCP et explique comment les gérer.

Objectifs de la leçon

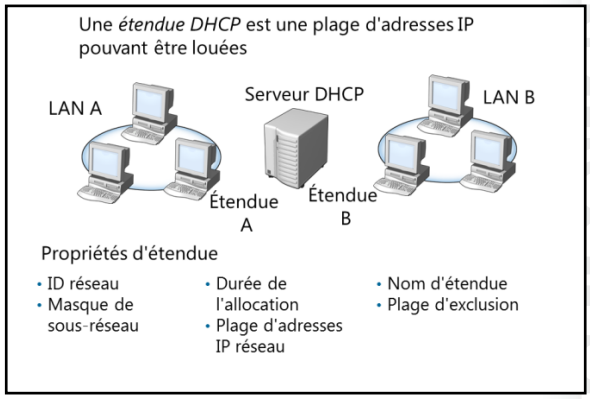
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le rôle d'une étendue DHCP ;
- décrire une réservation DHCP ;
- décrire les options DHCP ;
- expliquer comment appliquer les options DHCP ;
- créer et configurer une étendue DHCP.

Que sont les étendues DHCP ?

Une *étendue DHCP* est une plage d'adresses IP disponibles pour le bail et gérées par un serveur DHCP. En règle générale, une étendue DHCP se limite aux adresses IP d'un sous-réseau donné.

Par exemple, une étendue DHCP du réseau 192.168.1.0/24 (masque de sous-réseau 255.255.255.0) prend en charge une plage comprise entre 192.168.1.1 et 192.168.1.254. Lorsqu'un ordinateur ou périphérique du sous-réseau 192.168.1.0/24 demande une adresse IP, l'étendue qui a défini la plage de cet exemple alloue une adresse comprise entre 192.168.1.1 et 192.168.1.254.



Remarque : Souvenez-vous que le serveur DHCP, lorsqu'il est déployé sur le même sous-réseau, consomme une adresse IPv4. Cette adresse doit être exclue de la plage d'adresses IPv4.

Pour configurer une étendue, vous devez définir les propriétés suivantes :

- **Nom et description**. Cette propriété identifie l'étendue.
- **Plage d'adresses IP**. Cette propriété répertorie la plage d'adresses pouvant être proposées pour le bail et comprend habituellement la plage complète des adresses d'un sous-réseau donné.
- **Masque de sous-réseau**. Cette propriété est utilisée par les ordinateurs clients pour déterminer leur emplacement dans l'infrastructure réseau de l'entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- **Exclusions**. Cette propriété répertorie les adresses uniques ou les blocs d'adresses qui font partie de la plage d'adresses IP, mais qui ne sont pas proposés pour le bail.
- **Délai**. Cette propriété correspond à la durée d'attente avant l'exécution de DHCPOFFER.
- **Durée du bail**. *Cette propriété indique la durée du bail. U*tilisez des durées plus courtes pour les étendues disposant d'un nombre limité d'adresses IP et des durées plus longues pour les réseaux plus statiques.
- **Options**. Vous pouvez configurer de nombreux propriétés facultatives sur une étendue, mais les plus courantes sont les suivantes :
  - option 003 – Routeur (passerelle par défaut du sous-réseau)
  - option 006 – Serveurs DNS (Domain Name System)
  - option 015 – Suffixe DNS

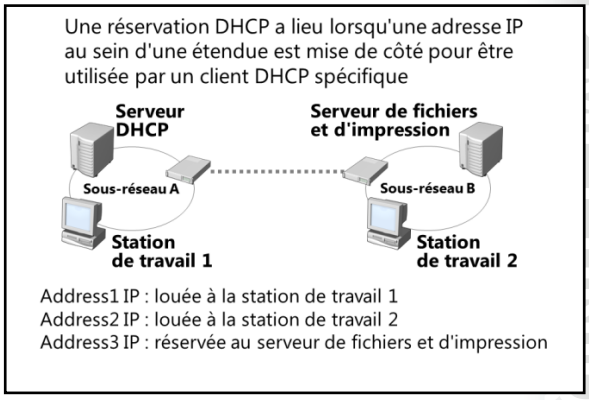
Étendues IPv6

Vous pouvez configurer les options d'une étendue IPv6 en tant qu'étendue distincte dans le nœud IPv6 de la console DHCP. Le nœud IPv6 contient différentes options que vous pouvez modifier, ainsi qu'un mécanisme de bail amélioré.

Lorsque vous configurez une étendue DHCPv6, vous devez définir les propriétés suivantes :

- **Nom et description**. Cette propriété identifie l'étendue.
- **Préfixe**. Le préfixe d'adresse IPv6 est similaire à la plage d'adresses IPv4 ; il définit essentiellement l'adresse réseau.
- **Exclusions**. Cette propriété répertorie les adresses uniques ou les blocs d'adresses qui font partie du préfixe IPv6, mais qui ne sont pas proposés pour le bail.
- **Durée de vie préférée**. Cette propriété définit la durée de validité des adresses louées.
- **Options**. Comme pour IPv4, vous pouvez configurer de nombreuses options.

Qu'est-ce qu'une réservation DHCP ?



La pratique recommandée consiste à fournir une adresse IP prédéterminée aux périphériques réseau tels que les imprimantes réseau. Avec une réservation DHCP, vous êtes assuré que les adresses IP que vous excluez d'une étendue configurée ne sont pas attribuées à un autre périphérique. Une *réservation DHCP* est une adresse IP spécifique au sein d'une étendue qui est réservée de manière permanente pour le bail d'un client DHCP spécifique. De plus, une réservation DHCP garantit que les périphériques ayant fait l'objet de réservations disposeront à coup sûr d'une adresse IP même si une étendue se trouve à court d'adresses. Le fait de configurer des réservations vous permet de centraliser la gestion des adresses IP fixes.

Configuration de réservations DHCP

Pour configurer une réservation, vous devez connaître l'adresse MAC (Media Access Control) ou l'adresse physique de l'interface réseau du périphérique. Cette adresse indique au serveur DHCP que le périphérique doit avoir une réservation. Vous pouvez acquérir l'adresse MAC d'une interface réseau en utilisant la commande **ipconfig/all**. Généralement, l'adresse MAC des imprimantes réseau et des autres périphériques réseau est apposée sur le périphérique proprement dit. Sur la plupart des ordinateurs portables, cette information figure également à la base du châssis.

Que sont les options DHCP ?

Les serveurs DHCP peuvent configurer autre chose que des adresses IP ; ils fournissent également des informations sur les ressources réseau, telles que les serveurs DNS et la passerelle par défaut. Les *options DHCP* sont des valeurs de données de configuration courantes qui s'appliquent au serveur, aux étendues, aux réservations et aux options de classe. Vous pouvez appliquer les options DHCP aux niveaux du serveur, de l'étendue, de l'utilisateur et du fournisseur. Les options DHCP sont identifiées par un code d'option. La plupart de ces codes d'option sont tirés de la documentation RFC que vous pouvez consulter sur le site Web de l'IETF (Internet Engineering Task Force).

Les options DHCP sont des valeurs de données de configuration courantes qui s'appliquent au serveur, aux étendues, aux réservations et aux options de classe

Les options d'étendue courantes sont les suivantes
- Routeur (Passerelle par défaut)
- Nom DNS
- Serveurs DNS
- Serveurs WINS

Options DHCP courantes

Le tableau suivant présente les codes d'option courants demandés par les clients DHCP Windows.

Code d'option	Nom
1	Masque de sous-réseau
3	Routeur
6	Serveurs DNS
15	Nom de domaine DNS
44	Serveurs WINS/NBNS (Windows Internet Naming Service/NetBIOS Name Service)
46	Type de nœud WINS/NetBT (WINS/NetBIOS sur TCP/IP)
47	Identificateur d'étendue NetBIOS
51	Durée du bail
58	Durée de renouvellement (T1)
59	Durée de reliaison (T2)

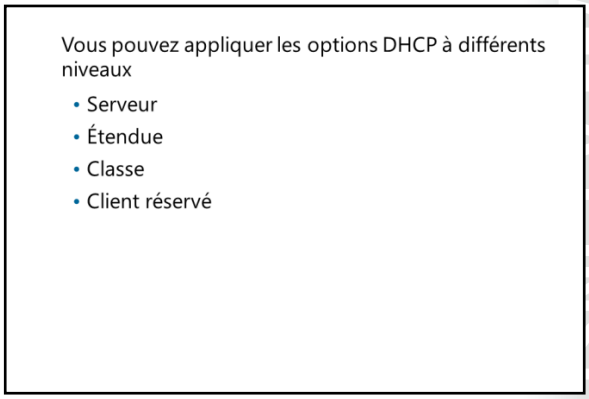
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Code d'option	Nom
31	Détection des routeurs
33	Itinéraire statique
43	Informations spécifiques au fournisseur
249	Itinéraires statiques sans classe

Comment les options DHCP sont-elles appliquées ?

Le service DHCP applique les options aux ordinateurs clients dans l'ordre suivant :



1. **Au niveau du serveur**. Une option au niveau du serveur est attribuée à tous les clients DHCP du serveur DHCP.
2. **Au niveau de l'étendue**. Une option au niveau de l'étendue est attribuée à tous les clients d'une étendue.
3. **Au niveau de la classe**. Une option au niveau de la classe est attribuée à tous les clients qui s'identifient comme membres d'une classe.
4. **Au niveau du client réservé**. Une option au niveau de la réservation est attribuée à un seul client DHCP.

Vous devez comprendre ces options lorsque vous configurez DHCP pour savoir quels sont les paramètres de niveau prioritaires lorsque vous configurez plusieurs paramètres à différents niveaux.

Si des paramètres d'option DHCP conflictuels sont appliqués à chaque niveau, l'option appliquée en dernier remplace le paramètre précédemment appliqué. Par exemple, si la passerelle par défaut est configurée au niveau de l'étendue et qu'une passerelle par défaut différente est appliquée pour un client réservé, le paramètre client réservé devient le paramètre effectif.

Vous pouvez également configurer des **stratégies d'affectation d'adresses** au niveau du serveur ou de l'étendue. Une stratégie d'affectation d'adresses contient un ensemble de conditions que vous définissez afin de louer différents adresses et paramètres IP DHCP à différents types de clients DHCP, tels que des ordinateurs, des ordinateurs portables, des imprimantes réseau ou des téléphones IP. Les conditions définies dans ces stratégies différencient les divers types de clients et comprennent plusieurs critères, tels que l'adresse MAC ou les informations de fournisseur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Création et configuration d'une étendue DHCP

Vous pouvez créer des étendues à l'aide de la console MMC (Microsoft Management Console) pour le rôle Serveur DHCP ou de l'outil en ligne de commande de configuration réseau Netsh. Ce dernier vous permet de gérer les étendues à distance si le serveur DHCP s'exécute sur une installation minimale (Server Core) de Windows Server 2012. Il est également utile pour les scripts et l'automatisation de la mise en service de serveurs.

Dans cette démonstration, vous allez apprendre à configurer une étendue et ses options dans DHCP.

Procédure de démonstration

Configurer une étendue et les options d'étendue dans DHCP

1. Dans le volet de navigation de DHCP, développez **lon-svr1.adatum.com**, développez et cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**.
2. Créez une étendue avec les propriétés suivantes :
   - Nom : **Filiale**
   - Plage d'adresses IP : **172.16.0.100-172.16.0.200**
   - Longueur : **16**
   - Masque de sous-réseau : **255.255.0.0**
   - Exclusions : **172.16.0.190-172.16.0.200**
   - Autres paramètres : utilisez les valeurs par défaut
   - Configurez les options **Routeur 172.16.0.1**
3. Utilisez les paramètres par défaut pour toutes les autres pages, puis activez l'étendue.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Gestion d'une base de données DHCP

La base de données DHCP stocke des informations sur les baux d'adresses IP. En cas de problème, il est important de savoir comment sauvegarder la base de données et comment résoudre les problèmes de base de données éventuels. Cette leçon explique comment gérer la base de données et les données qu'elle contient.

Objectifs de la leçon

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

- décrire la base de données DHCP ;
- expliquer la procédure de sauvegarde et de restauration d'une base de données DHCP ;
- expliquer la procédure de rapprochement d'une base de données DHCP ;
- expliquer la procédure de déplacement d'une base de données DHCP.

Qu'est-ce qu'une base de données DHCP ?

Une *base de données DHCP* est une base de données dynamique contenant les données en relation avec les étendues, les baux d'adresse et les réservations. La base de données contient également le fichier de données où sont stockées les informations de configuration DHCP et les données de bail pour les clients qui ont loué une adresse IP du serveur DHCP. Par défaut, les fichiers de base de données DHCP sont stockés dans le dossier %systemroot%\System32\Dhcp.

La *base de données DHCP* est une base de données dynamique qui contient des informations de configuration, telles que

- Étendues
- Réservations
- Baux d'adresses

Windows Server 2012 stocke la base de données DHCP dans le dossier %Systemroot%\System32\Dhcp

La base de données DHCP comporte les fichiers suivants

- Dhcp.mdb
- Dhcp.tmp
- J50.log et J50*.log
- Res*.log
- J50.chk

Fichiers de base de données du service DHCP

Le tableau suivant décrit quelques fichiers de base de données du service DHCP.

Fichier	Description
Dhcp.mdb	Dhcp.mdb est le fichier de base de données du serveur DHCP.
Dhcp.tmp	Dhcp.tmp est un fichier temporaire que la base de données DHCP utilise comme fichier d'échange lors des opérations de maintenance d'index de la base de données. Après une défaillance du système, Dhcp.tmp reste parfois dans le répertoire *Systemroot*\System32\Dhcp.
J50.log et J50#####.log	J50.log et J50#####.log sont les journaux de toutes les transactions de base de données. La base de données DHCP utilise ces fichiers pour récupérer les données, si nécessaire.
J50.chk	Il s'agit du fichier de point de contrôle.

Remarque : Vous ne devez pas supprimer ou modifier les fichiers de base de données de service DHCP.

La base de données de serveur DHCP est dynamique. Elle est mise à jour lorsque des clients DHCP sont attribués ou qu'ils libèrent leurs paramètres de configuration TCP/IP. La base de données DHCP n'étant pas une base de données distribuée comme la base de données du serveur WINS (Windows Internet Name Service), la maintenance de la base de données du serveur DHCP est moins complexe.

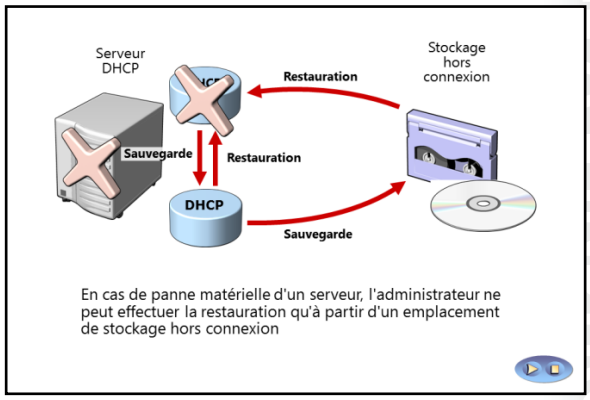
Par défaut, la base de données DHCP et les entrées associées du Registre sont sauvegardées automatiquement à intervalles de 60 minutes. Vous pouvez modifier cet intervalle par défaut en modifiant la valeur **BackupInterval** dans la clé de Registre suivante :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters
```

Vous pouvez aussi sauvegarder une base de données DHCP manuellement à tout moment.

Sauvegarde et restauration d'une base de données DHCP

Vous pouvez sauvegarder une base de données DHCP manuellement ou la configurer de sorte qu'elle soit sauvegardée automatiquement. Une sauvegarde automatique est appelée *sauvegarde synchrone*. Une sauvegarde manuelle est appelée *sauvegarde asynchrone*.



Sauvegarde automatique (synchrone)

Le chemin d'accès de sauvegarde par défaut pour la sauvegarde de DHCP est systemroot\System32\Dhcp\Backup. Pour vous conformer aux meilleures pratiques, vous pouvez modifier ce chemin dans les propriétés du serveur de façon à le faire pointer vers un autre volume.

Sauvegarde manuelle (asynchrone)

Si vous devez créer une sauvegarde immédiatement, vous pouvez exécuter l'option de sauvegarde manuelle dans la console DHCP. Cette opération nécessite soit des autorisations de niveau administrateur, soit que le compte utilisateur soit membre du groupe Administrateurs DHCP.

Éléments sauvegardés

Lors d'une sauvegarde synchrone ou asynchrone, c'est la base de données DHCP entière qui est enregistrée, à savoir :

- toutes les étendues ;
- les réservations ;
- les baux ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- l'ensemble des options, y compris les options de serveur, les options d'étendue, les options de réservation et les options de classe ;
- toutes les clés de Registre et les autres paramètres de configuration (par exemple, les paramètres de journal d'audit et les paramètres d'emplacement des dossiers) définis dans les propriétés du serveur DHCP. Ces paramètres sont stockés dans la clé de Registre suivante :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters

  Pour sauvegarder cette clé, ouvrez l'Éditeur du Registre et enregistrez la clé spécifiée dans un fichier texte.

Remarque : Les informations d'identification pour les mises à jour dynamiques DNS (nom d'utilisateur, domaine et mot de passe) qu'utilise le serveur DHCP lors de l'inscription des ordinateurs clients DHCP auprès du service DNS ne sont pas sauvegardées, quelle que soit la méthode de sauvegarde employée.

Restauration d'une base de données

Si vous devez restaurer la base de données, utilisez la fonction Restore de la console du serveur DHCP. Vous serez invité à spécifier l'emplacement de la sauvegarde. Une fois que vous aurez sélectionné l'emplacement, le service DHCP s'arrête et la base de données est restaurée. Pour restaurer la base de données, le compte d'utilisateur doit disposer d'autorisations de niveau administrateur ou être membre du groupe Administrateurs DHCP.

Sécurité des sauvegardes

Une fois le fichier de base de données DHCP sauvegardé, il doit être stocké dans un emplacement protégé auquel seuls les administrateurs DHCP peuvent accéder. Ceci est un gage de protection durable des informations de réseau contenues dans les fichiers de sauvegarde.

Utilisation de Netsh

Vous pouvez également utiliser des commandes dans le contexte de serveur DHCP de Netsh pour sauvegarder la base de données ; cela est utile pour sauvegarder la base de données à un emplacement distant à l'aide d'un fichier script.

La commande suivante est un script que vous pouvez utiliser dans l'invite Serveur DHCP de Netsh pour sauvegarder les données DHCP de toutes les étendues :

```
export "c:\My Folder\Dhcp Configuration" all
```

Pour restaurer la base de données DHCP, utilisez la commande suivante :

```
import "c:\My Folder\Dhcp Configuration" all
```

Remarque : Le contexte Serveur DHCP de Netsh n'existe pas sur les ordinateurs serveurs sur lesquels le rôle Serveur DHCP n'est pas installé.

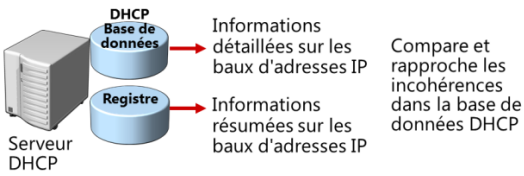
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Rapprochement d'une base de données DHCP

Le rapprochement des étendues peut résoudre les incohérences qui affectent les ordinateurs clients.

Le service Serveur DHCP stocke les informations de bail d'adresses IP d'étendue sous les deux formes suivantes :

- informations détaillées sur les baux d'adresses IP, stockées dans la base de données DHCP ;
- informations résumées sur les baux d'adresses IP, stockées dans le Registre du serveur.



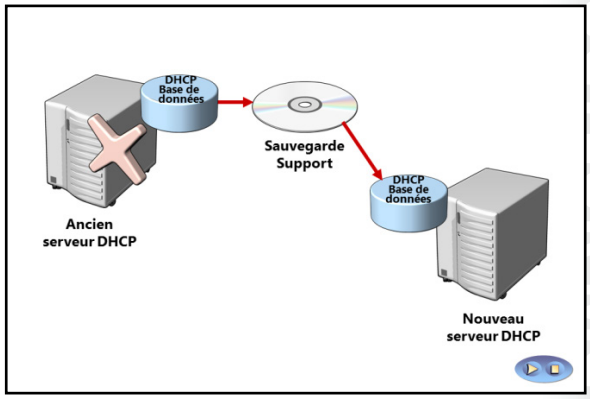
Exemple		
Registre	**Base de données DHCP**	**Après rapprochement**
Un client a l'adresse IP 192.168.1.34	L'adresse IP 192.168.1.34 est disponible	L'entrée de bail est créée dans la base de données DHCP

Lorsque vous rapprochez des étendues, les entrées détaillées et résumées sont comparées pour déceler les incohérences.

Pour corriger et réparer ces incohérences, vous devez rapprocher toutes les incohérences d'étendues. Après avoir sélectionné et rapproché les incohérences d'étendues, le service DHCP restitue ces adresses IP au propriétaire d'origine ou crée une réservation temporaire pour ces adresses. Ces réservations sont valides pendant la durée du bail assignée à l'étendue. Lorsque le bail arrive à expiration, les adresses sont récupérées pour une utilisation ultérieure.

Déplacement d'une base de données DHCP

Si vous êtes amené à déplacer le rôle Serveur DHCP vers un autre serveur, la pratique recommandée consiste à déplacer la base de données DHCP sur ce même serveur. Vous serez ainsi assuré que les baux clients seront conservés et vous réduirez les risques de rencontrer des problèmes de configuration au niveau des clients.



Dans un premier temps, vous devez déplacer la base de données en la sauvegardant sur l'ancien serveur DHCP. Vous arrêtez ensuite le service DHCP sur l'ancien serveur DHCP. Enfin, vous copiez la base de données DHCP sur le nouveau serveur, où vous pourrez la restaurer en suivant la procédure normale de restauration de base de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Sécurisation et surveillance DHCP

Le protocole DHCP n'intègre aucune méthode d'authentification des utilisateurs. Cela signifie que si vous ne prenez pas de précautions, les baux IP risquent d'être octroyés à des périphériques et à des utilisateurs non autorisés.

DHCP est un service essentiel dans les environnements réseau de nombreuses entreprises. Si le service DHCP ne fonctionne pas correctement ou si un problème de serveur DHCP se produit du fait d'une situation particulière, il est important que vous puissiez identifier le problème et déterminer ses causes potentielles afin de le résoudre.

Cette leçon explique comment empêcher les utilisateurs non autorisés d'obtenir un bail, comment gérer les serveurs DHCP non autorisés et comment configurer les serveurs DHCP pour permettre à un groupe spécifique de les gérer.

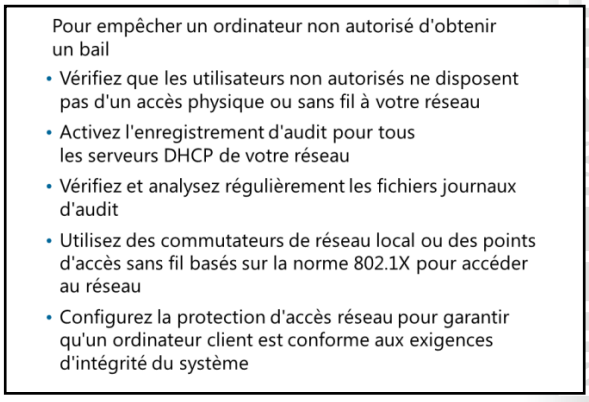
Objectifs de la leçon

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

- expliquer comment empêcher un ordinateur non autorisé d'obtenir un bail ;
- expliquer comment empêcher les serveurs DHCP non autorisés et non-Microsoft de louer des adresses IP ;
- expliquer comment déléguer l'administration du rôle Serveur DHCP ;
- décrire les statistiques DHCP ;
- décrire le journal d'audit DHCP ;
- identifier les problèmes courants pouvant survenir avec DHCP.

Procédure pour empêcher un ordinateur non autorisé d'obtenir un bail

Par nature, DHCP peut être difficile à sécuriser. En effet, le protocole a été conçu pour fonctionner avant que les informations nécessaires à l'authentification d'un ordinateur client via un contrôleur de domaine ne soient disponibles. C'est pourquoi vous devez prendre des précautions pour empêcher les ordinateurs non autorisés d'obtenir un bail avec DHCP.



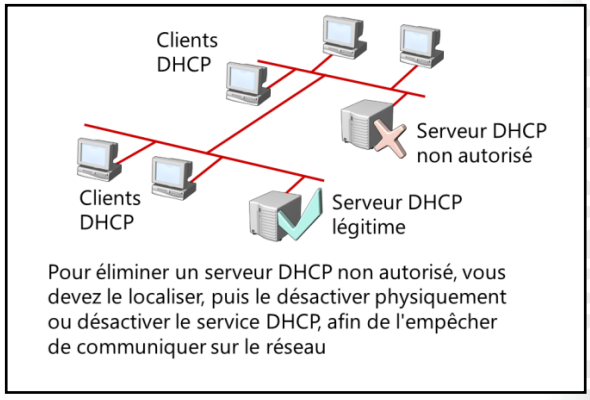
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les précautions à prendre pour limiter l'accès non autorisé sont les suivantes :

- Veillez à limiter l'accès physique : si des utilisateurs peuvent accéder à une connexion réseau active sur votre réseau, leurs ordinateurs sont probablement en mesure d'obtenir une adresse IP. Si un port réseau n'est pas utilisé, vous devez le déconnecter physiquement de l'infrastructure de commutation.
- Activez l'enregistrement d'audit sur tous les serveurs DHCP : vous obtiendrez un historique de l'activité et pourrez en outre déterminer à quel moment un utilisateur non autorisé a obtenu une adresse IP sur le réseau. Veillez à prévoir du temps pour examiner à intervalles réguliers les journaux d'audit.
- Exigez des connexions authentifiées de couche 2 au réseau : la plupart des commutateurs matériels d'entreprise prennent désormais en charge l'authentification IEEE (Institute of Electrical and Electronics Engineers, Inc.) 802.1X qui permet une authentification utilisateur au niveau du port. Les normes sans fil sécurisées, telles que Wi-Fi Protected Access (WPA) Enterprise et WPA2 Enterprise, utilisent également l'authentification 802.1X.
- Implémentez un système NAP : la protection d'accès réseau (NAP) permet aux administrateurs de garantir qu'un ordinateur client est conforme aux exigences d'intégrité du système, notamment l'exécution de toutes les dernières mises à jour du système d'exploitation Windows ou l'exécution d'un client antivirus à jour. Si des utilisateurs qui ne respectent pas les exigences de sécurité tentent d'accéder au réseau, ils reçoivent une configuration d'adresse IP qui leur permet d'accéder à un réseau de mise à jour où ils peuvent se procurer les mises à jour nécessaires. L'administrateur peut également limiter l'accès au réseau en autorisant uniquement les ordinateurs intègres à accéder au réseau local (LAN) interne.

Procédure pour empêcher des serveurs DHCP non autorisés et non-Microsoft de louer des adresses IP

Nombreux sont les périphériques et les systèmes d'exploitation réseau qui intègrent plusieurs implémentations de serveur DHCP. Sachant que par nature, les réseaux ne sont pratiquement jamais homogènes, il est possible qu'à un moment donné, un serveur DHCP qui ne vérifie pas les serveurs authentifiés par Active Directory soit activé sur le réseau. Dans ce cas, les clients risquent d'obtenir des données de configuration incorrectes.



Pour éliminer un serveur DHCP non autorisé, vous devez le localiser, puis le désactiver physiquement ou désactiver le service DHCP, afin de l'empêcher de communiquer sur le réseau

Pour supprimer un serveur DHCP non autorisé, vous devez d'abord le localiser. Vous devez ensuite l'empêcher de communiquer sur le réseau en le désactivant physiquement ou en désactivant le service DHCP.

Si les utilisateurs se plaignent de ne pas disposer de connexion au réseau, vérifiez l'adresse IP de leur serveur DHCP. Utilisez la commande **ipconfig/all** pour vérifier le champ d'adresse IP du serveur DHCP. Si l'adresse IP n'est pas celle d'un serveur DHCP autorisé, le réseau compte probablement en son sein un serveur non autorisé.

Vous pouvez employer l'utilitaire DHCP Server Locator (Dhcploc.exe) pour localiser les serveurs DHCP actifs sur un sous-réseau. Vous trouverez l'utilitaire DHCP Server Locator dans les Outils du Kit de ressources Windows Server 2003, les Outils de support Windows XP ou la Galerie TechNet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Délégation de l'administration DHCP

Assurez-vous que seules les personnes autorisées peuvent administrer le rôle Serveur DHCP. Pour cela, effectuez l'une des tâches suivantes :

- limitez les membres du groupe Administrateurs DHCP ;
- affectez les utilisateurs qui ont besoin de l'accès en lecture seule au groupe Utilisateurs DHCP.

- Pour déléguer les personnes qui sont habilitées à administrer le service DHCP
- Limitez les membres du groupe Administrateurs DHCP
- Ajoutez des utilisateurs au groupe Utilisateurs DHCP s'ils ont besoin d'un accès en lecture seule à la console DHCP

Compte	Autorisations
Groupe Administrateurs DHCP	Peut afficher et modifier toutes les données relatives au serveur DHCP
Groupe Utilisateurs DHCP	Bénéficie d'un accès en lecture seule au serveur à travers la console DHCP

Le groupe local Administrateurs DHCP est utilisé pour limiter et octroyer l'accès aux fonctions d'administration des serveurs DHCP. Par conséquent, le groupe Administrateurs DHCP est créé dans AD DS lorsque le rôle Serveur DHCP est installé sur un contrôleur de domaine, ou sur l'ordinateur local lorsque le rôle Serveur DHCP est installé sur des membres de domaine ou des serveurs autonomes.

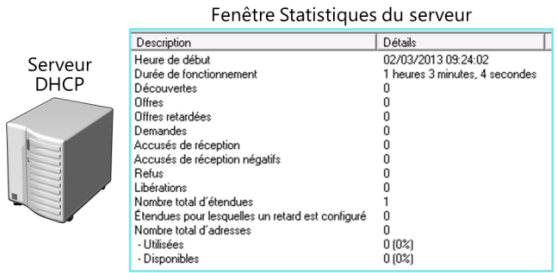
Autorisations requises pour autoriser et administrer le service DHCP

Seuls les administrateurs d'entreprise peuvent autoriser un service DHCP. Si un administrateur dont les informations d'identification sont inférieures à celles d'un administrateur d'entreprise doit autoriser le domaine, il doit utiliser la délégation Active Directory. Tout utilisateur du groupe Administrateurs DHCP peut gérer le service DHCP du serveur. Tout utilisateur du groupe Utilisateurs DHCP peut bénéficier d'un accès en lecture seule à la console DHCP.

En quoi consistent les statistiques DHCP ?

Les statistiques DHCP fournissent des informations sur l'activité et l'utilisation du service DHCP. Vous pouvez utiliser cette console pour déterminer rapidement s'il existe un problème au niveau du service DHCP ou des clients DHCP du réseau. Les statistiques peuvent s'avérer utiles si vous détectez un nombre excessif de paquets d'accusé de réception négatif (NAK), ce qui peut indiquer que le serveur ne fournit pas les données correctes aux clients.

Les statistiques DHCP sont collectées au niveau du serveur ou au niveau de l'étendue



Vous pouvez configurer la fréquence d'actualisation des statistiques sous l'onglet **Général** de la boîte de dialogue **Propriétés** du serveur.

Statistiques sur le serveur DHCP

Les statistiques sur le serveur DHCP offrent un aperçu de l'utilisation du serveur DHCP. Ces données peuvent vous être utiles pour connaître rapidement l'état du serveur DHCP. Certaines informations, telles que le nombre d'offres, le nombre de demandes, le nombre total d'adresses utilisées/disponibles, peuvent vous aider à vous faire une idée de l'état du serveur. Les statistiques sur le serveur sont gérés séparément pour IPv4 et IPv6.

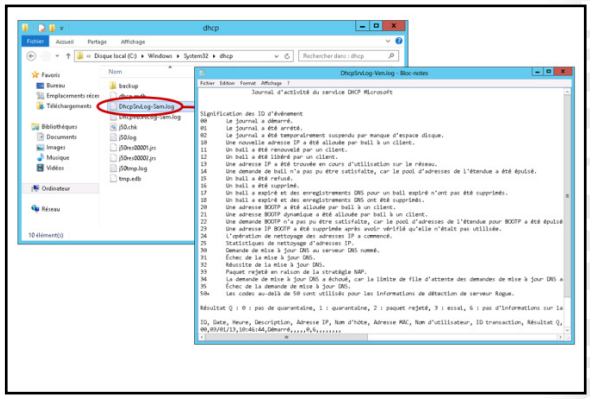
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Statistiques sur les étendues DHCP

Bien que nettement moins détaillées, les statistiques sur les étendues DHCP fournissent des informations sur le nombre total d'adresses contenues dans une étendue donnée, le nombre d'adresses utilisées et le nombre d'adresses disponibles. Si vous remarquez dans les statistiques du serveur que le nombre d'adresses disponibles est peu élevé, il est simplement possible qu'une étendue soit proche de son point d'épuisement. Les statistiques d'étendue permettent à un administrateur de déterminer rapidement l'état d'une étendue donnée eu égard aux adresses disponibles.

Qu'est-ce que le journal d'audit DHCP ?

Le *journal d'audit DHCP* est un journal qui consigne l'activité d'un serveur DHCP. Vous pouvez utiliser ce journal pour suivre les demandes, les octrois et les refus de bail. Ces informations vous permettent de résoudre les problèmes de performances des serveurs DHCP. Par défaut, les fichiers journaux sont stockés dans le dossier %*systemroot*%\system32\dhcp. Vous pouvez configurer les paramètres du fichier journal dans la boîte de dialogue **Propriétés** du serveur.



Les fichiers journaux d'audit DHCP sont nommés en fonction du jour de la semaine où ils ont été créés. Par exemple, si le journal d'audit est activé un lundi, le fichier s'intitule DhcpSrvLog-Mon.log.

Champs du fichier journal d'audit DHCP

Le tableau suivant décrit les champs contenus dans un journal d'audit DHCP.

Champ	Description
ID	Code d'identification d'événement du serveur DHCP
Date	Date à laquelle l'entrée a été écrite dans le journal du serveur DHCP
Heure	Heure à laquelle l'entrée a été écrite dans le journal du serveur DHCP
Description	Description de l'événement du serveur DHCP
Adresse IP	Adresse IP du client DHCP
Nom d'hôte	Nom d'hôte du client DHCP
Adresse MAC	Adresse MAC utilisée par la carte réseau du client

Codes d'identification des événements courants

Les codes d'identification des événement courants se présentent comme suit :

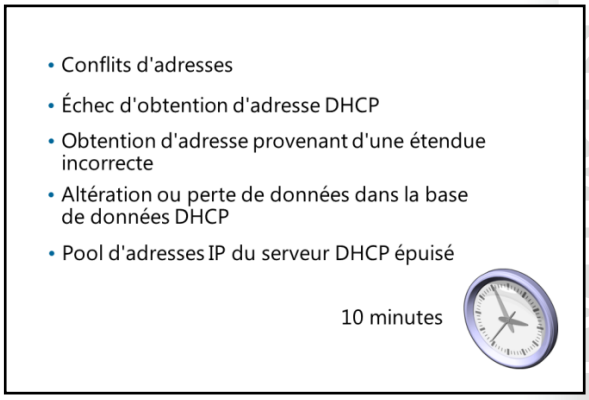
- ID,Date,Heure,Description,Adresse IP,Nom d'hôte,Adresse MAC

Les codes d'identification d'événements courants sont les suivants :

- 00,06/22/99,22:35:10,Démarré,,,,
- 56,06/22/99,22:35:10,Échec de l'autorisation, arrêt du service,,domaine1.local,,
- 55,06/22/99,22:45:38,Autorisé (en service),,domaine1.local

Discussion : Problèmes DHCP courants

Le tableau suivant décrit quelques problèmes DHCP courants. Écrivez les solutions possibles dans la colonne Solution, puis discutez de vos réponses avec la classe.



Problème	Description	Exemple	Solution
Conflits d'adresses	La même adresse IP est offerte à deux clients différents.	Un administrateur supprime un bail. Toutefois, le client qui bénéficiait du bail fonctionne toujours comme si le bail était valide. Si le serveur DHCP ne vérifie pas l'adresse IP, il risque de la louer à un autre ordinateur, ce qui va entraîner un conflit d'adresse. Cela peut également se produire si deux serveurs DHCP ont des étendues qui se chevauchent.	
Échec d'obtention d'adresse DHCP	Au lieu de recevoir une adresse DHCP, le client reçoit une adresse APIPA (Automatic Private IP Addressing) auto-assignée.	Si le pilote de la carte réseau d'un client est mal configurée, cela peut entraîner un échec d'obtention d'adresse DHCP. En outre, le serveur DHCP ou l'agent de relais sur le sous-réseau du client peut être hors ligne. Une autre raison pourrait être que l'étendue du serveur DHCP est épuisée. Dans ce cas, il est nécessaire d'étendre ou de modifier l'étendue.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Problème	Description	Exemple	Solution
Obtention d'adresse provenant d'une étendue incorrecte	Le client obtient une adresse IP provenant d'une étendue incorrecte, ce qui lui vaut des problèmes de communication.	Si le client est connecté à un réseau incorrect ou si l'agent de relais DHCP n'est pas correctement configuré, cette erreur peut se produire.	
Altération ou perte de données dans la base de données DHCP	La base de données DHCP devient illisible ou est perdue en raison d'une défaillance matérielle.	Une défaillance matérielle peut entraîner l'altération de la base de données.	
Épuisement du pool d'adresses du serveur DHCP	Les étendues IP du serveur DHCP sont épuisées. Tout nouveau client qui demandera une demande IP essuiera un refus.	Si toutes les adresses IP qui sont attribuées à une étendue sont louées, cette erreur se produit.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation de DHCP

Scénario

La société A. Datum Corporation a un bureau et un centre de données informatiques à Londres qui prennent en charge le site de Londres ainsi que d'autres sites. A. Datum a récemment déployé une infrastructure Windows 2012 Server avec des clients Windows 8.

Vous avez récemment accepté une promotion au sein de l'équipe d'assistance technique des serveurs. L'une de vos premières missions consiste à configurer le service d'infrastructure pour une nouvelle filiale. Dans le cadre de cette mission, vous devez configurer un serveur DHCP qui fournira des adresses IP et la configuration requise aux ordinateurs clients. Les serveurs sont configurés avec des adresses IP statiques et n'utilisent pas DHCP.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- implémenter DHCP ;
- implémenter un agent de relais DHCP (facultatif).

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-SVR1 22410B-LON-RTR 22410B-LON-CL1 22410B-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 débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Microsoft Hyper-V®, cliquez sur **22410B-LON-DC1**, puis, dans le volet Actions, cliquez sur **Démarrer**.
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 : **Administrateur**
    - Mot de passe : **Pa$$w0rd**.
    - Domaine : **ADATUM**
5. Répétez les étapes 2 à 4 pour **22410B-LON-SVR1** et **22410B-LON-CL1**.
6. Pour l'exercice 2 facultatif, vous devez répéter les étapes 2 à 4 pour **22410B-LON-RTR** et **22410B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Implémentation de DHCP

Scénario

Dans le cadre de la configuration de l'infrastructure de la nouvelle filiale, vous devez configurer un serveur DHCP qui fournira des adresses IP et la configuration requise aux ordinateurs clients. Les serveurs sont configurés avec des adresses IP statiques et n'utilisent généralement pas DHCP pour obtenir des adresses IP.

Un des ordinateurs clients de la filiale doit accéder à une application de comptabilité installée au siège social. L'équipe réseau utilise des pare-feu basés sur les adresses IP pour limiter l'accès à cette application. L'équipe réseau vous a demandé d'attribuer une adresse IP statique à cet ordinateur client. Plutôt que de configurer manuellement une adresse IP statique sur l'ordinateur client, vous décidez de créer une réservation dans DHCP pour l'ordinateur client.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le rôle Serveur DHCP (Dynamic Host Configuration Protocol)
2. Configurer les étendues et les options DHCP
3. Configurer le client pour utiliser DHCP, puis tester la configuration
4. Configurer un bail en tant que réservation

▶ Tâche 1 : Installer le rôle Serveur DHCP (Dynamic Host Configuration Protocol)

1. Basculez vers LON-SVR1.
2. Ouvrez le **Gestionnaire de serveur** et installez le rôle **Serveur DHCP**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, acceptez toutes les valeurs par défaut.

▶ Tâche 2 : Configurer les étendues et les options DHCP

1. Dans le Gestionnaire de serveur, ouvrez la console **DHCP**.
2. Autorisez le serveur **lon-svr1.adatum.com** dans AD DS.
3. Dans le volet de navigation de DHCP, accédez à **IPv4**, cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**.
4. Créez une étendue avec les propriétés suivantes :
   - Nom : **Filiale**
   - Plage d'adresses IP : **172.16.0.100-172.16.0.200**
   - Longueur : **16**
   - Masque de sous-réseau : **255.255.0.0**
   - Exclusions : **172.16.0.190-172.16.0.200**
   - Configurez les options **Routeur 172.16.0.1**
   - Utilisez les valeurs par défaut pour tous les autres paramètres
5. Activez l'étendue.

▶ Tâche 3 : Configurer le client pour utiliser DHCP, puis tester la configuration

1. Basculez vers LON-CL1.
2. Reconfigurez la connexion au réseau local à l'aide des informations suivantes :
   - **Configurez Protocole Internet version 4 (TCP/IPv4)**
   - **Obtenir une adresse IP automatiquement**
   - **Obtenir les adresses des serveurs DNS automatiquement**
3. Ouvrez la fenêtre d'invite de commandes et lancez le processus DHCP à l'aide de la commande **ipconfig /renew**.
4. Pour tester la configuration, vérifiez que LON-CL1 a reçu une adresse IP de l'étendue DHCP en saisissant **ipconfig /all** dans la fenêtre d'invite de commandes.

   Cette commande renverra les informations telles que l'adresse IP, le masque de sous-réseau et l'état d'activation de DHCP, qui devrait être **Oui**.

▶ Tâche 4 : Configurer un bail en tant que réservation

1. Dans la fenêtre d'invite de commandes, tapez **ipconfig/all** pour afficher l'adresse physique de la carte réseau.
2. Basculez vers **LON-SVR1**.
3. Ouvrez la console **DHCP**.
4. Dans la console DHCP, dans le volet de navigation, accédez à **Étendue [172.16.0.0] Filiale**, cliquez avec le bouton droit sur **Réservations**, puis cliquez sur **Nouvelle réservation**.
5. Créez une nouvelle réservation pour **LON-CL1** utilisant l'adresse physique de la carte réseau **LON-CL1** et l'adresse IP **172.16.0.155**.
6. Sur LON-CL1, utilisez la commande **ipconfig** pour renouveler et vérifier l'adresse IP.

Résultats : À la fin de cet exercice, vous aurez implémenté DHCP, configuré les étendues et options DHCP, et configuré une réservation DHCP.

▶ Pour préparer l'exercice facultatif

Si vous voulez effectuer l'atelier pratique facultatif, rétablissez l'ordinateur virtuel suivant : 22410B-LON-CL1. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V-Manager**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-LON-CL1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Implémenter un agent de relais DHCP (exercice facultatif)

Scénario

Pour éviter de configurer un serveur DHCP supplémentaire sur le sous-réseau, votre gestionnaire vous a demandé de configurer un agent de relais DHCP pour un autre sous-réseau de votre filiale.

Les tâches principales de cet exercice sont les suivantes :

1. Installer un agent de relais DHCP
2. Configurer un agent de relais DHCP
3. Tester l'agent de relais DHCP avec un client
4. Pour préparer le module suivant

▶ Tâche 1 : Installer un agent de relais DHCP

1. Basculez vers **LON-RTR**.
2. Dans le **Gestionnaire de serveur**, ouvrez Routage et accès distant.
3. Procédez comme suit pour ajouter l'agent de relais DHCP au routeur :
   - Dans le volet de navigation, développez **IPv4**, cliquez avec le bouton droit sur **Général**, puis cliquez sur **Nouveau protocole de routage**.
   - Dans la liste **Protocoles de routage**, cliquez sur **Agent de relais DHCP**, puis sur **OK**.

▶ Tâche 2 : Configurer un agent de relais DHCP

1. Ouvrez **Routage et accès distant**.
2. Procédez comme suit pour configurer l'agent de relais DHCP :
   - Dans le volet de navigation, cliquez avec le bouton droit sur **Agent de relais DHCP**, puis cliquez sur **Nouvelle interface**.
   - Dans la boîte de dialogue **Nouvelle interface pour Agent de relais DHCP**, cliquez sur **Connexion au réseau local 2**, puis sur **OK**.
   - Dans la boîte de dialogue **Propriétés de : Propriétés de relais DHCP – Con…**, cliquez sur **OK**.
   - Cliquez avec le bouton droit sur **Agent de relais DHCP**, puis cliquez sur **Propriétés**.
   - Dans la boîte de dialogue **Propriétés de : Agent de relais DHCP**, dans la zone **Adresse du serveur**, tapez **172.16.0.21**, puis cliquez sur **Ajouter** et **OK**.
3. Fermez la boîte de dialogue Routage et accès distant.

▶ Tâche 3 : Tester l'agent de relais DHCP avec un client

Remarque : Pour tester la manière dont un client reçoit une adresse IP de l'agent de relais DHCP sur un autre sous-réseau, vous devez créer une autre étendue DHCP.

1. Basculez vers **LON-SVR1**.
2. Ouvrez la console **DHCP**.
3. Dans le volet de navigation de DHCP, développez **lon-svr1.adatum.com**, développez **IPv4**, cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Créez une étendue avec les propriétés suivantes :
   - Nom : **Filiale 2**
   - Plage d'adresses IP : **10.10.0.100-10.10.0.200**
   - Longueur : **16**
   - Masque de sous-réseau : **255.255.0.0**
   - Exclusions : **10.10.0.190-10.10.0.200**
   - Les autres paramètres utilisent les valeurs par défaut
   - Configurez les options **Routeur 10.10.0.1**. Les autres paramètres utilisent les valeurs par défaut
5. Activez l'étendue.
6. Pour tester le client, basculez vers **LON-CL2**.
7. Ouvrez la fenêtre Centre Réseau et partage et configurez les propriétés **Connexion au réseau local, Protocole Internet version 4 (TCP/IPv4)** avec les paramètres suivants :
   - **Obtenir une adresse IP automatiquement**
   - **Obtenir les adresses des serveurs DNS automatiquement**
8. Ouvrez la fenêtre d'invite de commandes.
9. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez la commande suivante :

   ipconfig /renew
10. Vérifiez que les paramètres de l'adresse IP et du serveur DNS sur **LON-CL2** sont obtenus à partir d'étendue de serveur DHCP installée sur **LON-SVR1**.

Remarque : L'adresse IP doit être comprise dans la plage suivante : **10.10.0.100/16** à **10.10.0.200/16**.

Résultats : À la fin de cet exercice, vous aurez implémenté un agent de relais DHCP.

▶ 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 **22410B-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 **22410B-LON-SVR1**, **22410B-LON-RTR** et **22410B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Consacrez du temps à la conception de votre modèle d'adressage IP afin qu''il réponde aux besoins actuels et futurs de votre infrastructure informatique.
- Déterminez les périphériques qui ont besoin de réservations DHCP, tels que les imprimantes réseau, les scanneurs réseau ou les caméras IP.
- Isolez votre réseau des serveurs DHCP non autorisés.
- Configurez la base de données DHCP sur les configurations de lecteurs hautement disponibles, tels que les disques RAID-5 (Redundant Array of Independent Disks) ou RAID-1, pour assurer la disponibilité du service DHCP en cas de défaillance d'un seul disque.
- Sauvegardez la base de données DHCP régulièrement et testez la procédure de restauration dans un environnement isolé non utilisé pour la production.
- Surveillez l'utilisation des serveurs DHCP par le système et mettez à niveau le matériel des serveurs DHCP si nécessaire pour améliorer les performances du service.

Questions de contrôle des acquis

Question : Vous avez deux sous-réseaux dans votre entreprise et souhaitez utiliser DHCP pour allouer des adresses aux ordinateurs client sur les deux sous-réseaux. Vous ne souhaitez pas déployer deux serveurs DHCP. De quels facteurs devez-vous tenir compte ?

Question : Votre entreprise s'est développée et votre étendue IPv4 est presque à court d'adresses. Que devez-vous faire ?

Question : De quelles informations avez-vous besoin pour configurer une réservation DHCP ?

Question : Pouvez-vous configurer l'option 003 - Routeur comme option d'étendue DHCP au niveau du serveur ?

Outils

Outil	Utilisation	Emplacement
DHCP	Interface graphique de gestion du serveur DHCP	Gestionnaire de serveur
PowerShell	Interface de ligne de commande permettant de gérer le serveur DHCP	Barre des tâches Windows sur le Bureau
Ipconfig.exe	Gestion et résolution des problèmes en relation avec les paramètres IP du client	Ligne de commande
Netsh.exe	Configuration des paramètres IP côté client et côté serveur, y compris ceux du rôle Serveur DHCP	Ligne de commande
Regedit.exe	Modification et affinage des paramètres, y compris ceux du rôle Serveur DHCP	Interface Windows ou ligne de commande

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7

Implémentation du système DNS (Domain Name System)

Table des matières :

Vue d'ensemble du module **7-1**

Leçon 1 : Résolution de noms pour les clients et les serveurs Windows **7-2**

Leçon 2 : Installation et gestion d'un serveur DNS **7-12**

Leçon 3 : Gestion des zones DNS **7-19**

Atelier pratique : Implémentation de la réplication DNS **7-23**

Contrôle des acquis et éléments à retenir **7-28**

Vue d'ensemble du module

La résolution de noms est le processus de traduction logicielle des noms, que les utilisateurs peuvent lire et comprendre, et des adresses IP numériques, qui sont nécessaires aux communications TCP/IP. Pour cette raison, la résolution de noms est l'un des concepts les plus importants de toute infrastructure du réseau. Vous pouvez comparer DNS (Domain Name System) à un annuaire des ordinateurs sur Internet. Les ordinateurs clients utilisent le processus de résolution de noms lors de la localisation d'hôtes sur Internet et lors de la localisation d'autres hôtes et services dans un réseau interne. DNS (Domain Name System) est l'une des technologies les plus répandues pour la résolution de noms. Les services de domaine Active Directory® (AD DS) dépendent fortement de DNS, de même que le trafic Internet. Ce module présente certains concepts de base relatifs à la résolution de noms, ainsi qu'à l'installation et la configuration d'un service Serveur DNS et de ses composants.

Objectifs

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

- décrire la résolution de noms pour les clients utilisant le système d'exploitation Windows® et les serveurs Windows Server® ;
- installer et gérer le service Serveur DNS ;
- gérer les zones DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Résolution de noms pour les clients et les serveurs Windows

Vous pouvez configurer un ordinateur pour communiquer sur un réseau en utilisant un nom au lieu d'une adresse IP. L'ordinateur utilise ensuite la résolution de noms pour trouver une adresse IP qui correspond à un nom, par exemple un nom d'hôte. Ce cours porte sur les différents types de nom d'ordinateur, les méthodes utilisées pour les résoudre, ainsi que la résolution des problèmes liés à la résolution de noms.

Objectifs de la leçon

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

- décrire les noms d'ordinateurs ;
- décrire DNS ;
- décrire les zones et les enregistrements DNS ;
- décrire la résolution des noms DNS Internet ;
- décrire la résolution LLMNR (Link Local Multicast Name Resolution) ;
- décrire la façon dont un client résout un nom ;
- résoudre les problèmes liés à la résolution de noms.

Que sont les noms d'ordinateurs ?

L'ensemble de protocoles TCP/IP identifie les ordinateurs source et de destination en fonction de leur adresse IP. Toutefois, les utilisateurs d'ordinateurs sont plus enclins à utiliser et à se souvenir de noms que de chiffres. Pour cette raison, les administrateurs affectent généralement des noms aux ordinateurs. Les administrateurs lient ensuite ces noms aux adresses IP des ordinateurs via un système de résolution de noms tel que DNS. Ces noms sont soit au format de *nom d'hôte*, par exemple dc1.contoso.com (qui est reconnu par DNS), soit au format de *nom NetBIOS*, par exemple DC1, (qui est reconnu par le service WINS (Windows Internet Name Service)).

Name	Description
Nom d'hôte	• Jusqu'à 255 caractères • Peut contenir des caractères alphabétiques et numériques, des points et des tirets • Partie du nom de domaine complet
Nom NetBIOS	• Représente un ordinateur unique ou un groupe d'ordinateurs • 15 caractères sont utilisés pour le nom • Le 16ème caractère identifie le service • Espace de noms plat

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Type de nom

Le type de nom (nom d'hôte ou nom NetBIOS) qu'une application utilise est déterminé par le développeur d'applications. Si le développeur d'applications conçoit une application pour demander des services réseau via des sockets Windows, les noms d'hôtes sont utilisés. En revanche, si le développeur d'applications conçoit une application pour demander des services via NetBIOS, un nom NetBIOS est utilisé. La plupart des applications actuelles, notamment les applications Internet, utilisent des sockets Windows (et, par conséquent, des noms d'hôtes) pour accéder aux services réseau. NetBIOS est utilisé par de nombreuses applications des versions antérieures du système d'exploitation Windows.

Les versions antérieures des systèmes d'exploitation Windows, par exemple Microsoft® Windows 98 et Windows Millennium Edition, requièrent NetBIOS pour prendre en charge les fonctionnalités réseau telles que le partage de fichiers. Toutefois, depuis Microsoft Windows 2000, tous les systèmes d'exploitation prennent en charge NetBIOS (sans pour autant nécessiter NetBIOS) à des fins de compatibilité descendante avec les versions antérieures de Windows.

Remarque : Vous pouvez utiliser des applications de sockets Windows pour spécifier l'hôte de destination, soit par l'adresse IP, soit par le nom d'hôte. Les applications NetBIOS requièrent l'utilisation d'un nom NetBIOS.

Noms d'hôtes

Un nom d'hôte est un nom convivial associé à l'adresse IP d'un ordinateur afin de l'identifier en tant qu'hôte TCP/IP. Le nom d'hôte peut comprendre jusqu'à 255 caractères (caractères alphabétiques et numériques, points et traits d'union).

Vous pouvez utiliser les noms d'hôtes sous diverses formes. Les deux formes les plus répandues sont l'alias et le nom de domaine complet (FQDN). Un alias est un nom unique associé à une adresse IP, tel que *payroll*. Vous pouvez combiner un alias avec un nom de domaine pour créer un nom de domaine complet. Un nom de domaine complet est structuré pour être utilisé sur Internet et inclut des points comme séparateurs. Exemple d'un nom de domaine complet : payroll.contoso.com.

Noms NetBIOS

Un nom NetBIOS, qui compte 16 caractères, identifie une ressource NetBIOS sur le réseau. Un nom NetBIOS peut représenter un ordinateur unique ou un groupe d'ordinateurs. Les 15 premiers caractères sont utilisés pour le nom, le dernier caractère identifie la ressource ou le service de l'ordinateur auquel il est fait référence. Le nom de 15 caractères peut inclure le nom de l'ordinateur, le nom du domaine et le nom de l'utilisateur connecté. Le seizième caractère est un identificateur hexadécimal d'un octet.

L'espace de noms NetBIOS est plat, ce qui signifie que les noms ne peuvent être utilisés qu'une seule fois au sein d'un réseau. Vous ne pouvez pas organiser les noms NetBIOS en une structure hiérarchique, comme c'est le cas avec les noms de domaine complets.

Documentation supplémentaire : Pour plus d'informations sur la résolution de noms NetBIOS, consultez la page Résolution de noms NetBIOS à l'adresse http://go.microsoft.com/fwlink/?LinkId=269710.

Qu'est-ce que DNS ?

DNS est un service qui résout les noms de domaine complets et autres noms d'hôtes en adresses IP. Tous les systèmes d'exploitation Windows Server incluent un service Serveur DNS.

DNS peut être utilisé pour effectuer les tâches suivantes

- Résoudre des noms d'hôtes en adresses IP
- Rechercher des contrôleurs de domaine et des serveurs de catalogue global
- Résoudre des adresses IP en noms d'hôtes
- Rechercher des serveurs de messagerie pendant la remise du courrier électronique

Lorsque vous utilisez DNS, les utilisateurs de votre réseau peuvent localiser les ressources réseau en tapant des noms conviviaux (par exemple www.microsoft.com), que l'ordinateur résout ensuite en adresses IP. L'avantage réside dans le fait que les adresses IPv4 peuvent être difficiles à mémoriser (par exemple 131.107.0.32), alors qu'il est généralement plus facile de se souvenir d'un nom de domaine. En outre, vous pouvez utiliser des noms d'hôtes qui ne changent pas, alors que les adresses IP sous-jacentes peuvent être modifiées en fonction des besoins de votre organisation.

DNS utilise une base de données (stockée dans un fichier ou dans les services AD DS) de noms et d'adresses IP pour fournir ce service. Les logiciels clients DNS effectuent des requêtes dans la base de données DNS et la mettent à jour. Par exemple, dans une organisation, un utilisateur qui tente de localiser un serveur d'impression peut utiliser le nom DNS printserver.contoso.com. Le logiciel client DNS va résoudre le nom en adresse IP de l'imprimante, par exemple 172.16.23.55. Même si l'adresse IP de l'imprimante change, le nom convivial peut rester le même.

À l'origine, un seul fichier sur Internet contenait la liste de tous les noms de domaine et leurs adresses IP correspondantes. Cette liste est rapidement devenue trop longue à gérer et distribuer. DNS a été développé pour résoudre les problèmes liés à l'utilisation d'un fichier unique sur Internet. Avec l'adoption de la norme IPv6, le rôle de DNS est de plus en plus important, car les adresses IPv6 sont encore plus complexes que les adresses IPv4 (par exemple, 2001:db8:4136:e38c:384f:3764:b59c:3d97).

DNS regroupe les informations sur les ressources réseau en une structure hiérarchique de domaines. Cette structure hiérarchique de domaines est une arborescence inversée qui possède un domaine racine à son sommet et qui progresse vers le bas en branches distinctes avec des niveaux communs de domaines parents. Cette progression se poursuit toujours plus bas vers les domaines enfants individuels. La représentation de l'ensemble de la structure hiérarchique de domaines s'appelle un *espace de noms DNS*.

Internet utilise un espace de noms DNS unique avec plusieurs serveurs racine. Pour faire partie de l'espace de noms DNS Internet, un nom de domaine doit être inscrit auprès d'un bureau d'enregistrement DNS. Cela garantit qu'il n'existe pas deux organisations qui tentent d'utiliser le même nom de domaine.

Si les hôtes qui sont situés sur Internet n'ont pas besoin de résoudre les noms de votre domaine, vous pouvez héberger un domaine en interne, sans l'inscrire. Toutefois, vous devez toujours veiller à ce que le nom de domaine soit unique par rapport aux noms de domaine Internet. Sinon, la connectivité aux ressources Internet risque de s'en trouver affectée. Il est fréquent de garantir cette unicité en créant un domaine interne dans le domaine .local. Le domaine .local est réservé à un usage interne, à l'instar des adresses IP privées qui sont réservées à un usage interne.

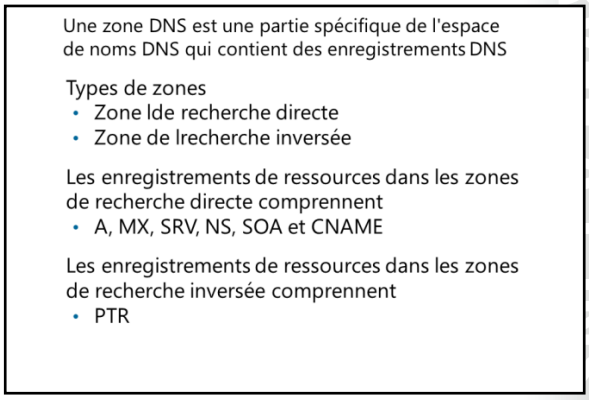
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Outre la résolution des noms d'hôtes en adresses IP, DNS peut être utilisé pour effectuer les tâches suivantes :

- Rechercher des contrôleurs de domaine et des serveurs de catalogue global. Cela a lieu lors de la connexion aux services AD DS.
- Résoudre des adresses IP en noms d'hôtes. Cela est utile lorsqu'un fichier journal contient uniquement l'adresse IP d'un hôte.
- Rechercher un serveur de messagerie pour la remise du courrier électronique. Cela a lieu lors de la remise de l'ensemble du courrier électronique Internet.

Zones et enregistrements DNS

Une *zone DNS* est une partie spécifique de l'espace de noms DNS qui contient des enregistrements DNS. Une zone DNS est hébergée sur un serveur DNS chargé de répondre aux requêtes portant sur les enregistrements d'un domaine spécifique. Par exemple, le serveur DNS chargé de résoudre www.contoso.com en adresse IP doit contenir la zone contoso.com.



La zone de contenu peut être stockée dans un fichier ou dans la base de données AD DS. Lorsque le serveur DNS stocke la zone dans un fichier, ce dernier se trouve dans un dossier local sur le serveur. Lorsque la zone n'est pas stockée dans les services AD DS, seule une copie de la zone peut être accessible en écriture, alors que toutes les autres copies sont en lecture seule.

Les types de zone DNS les plus couramment utilisés dans le DNS Windows Server sont les zones de recherche directe et les zones de recherche inversée.

Zones de recherche directe

Les zones de recherche directe résolvent les noms d'hôtes en adresses IP et hébergent les enregistrements de ressources courants, notamment les enregistrements de ressources d'hôte (A), d'alias (CNAME), de service (SRV), de serveur de messagerie (MX), de source de noms (SOA) et de serveur de noms (NS). Le type d'enregistrement de ressource le plus courant est l'enregistrement de ressource d'hôte (A).

Zones de recherche inversée

La zone de recherche inversée résout les adresses IP en noms de domaine. Une zone inversée fonctionne de la même manière qu'une zone directe, mais l'adresse IP fait partie de la requête et le nom d'hôte représente l'information retournée. Les zones de recherche inversée hébergent les enregistrements de ressources SOA, NS et de pointeur (PTR). Les zones inversées ne sont pas toujours configurées, mais vous devez les configurer pour réduire le nombre de messages d'avertissement et d'erreur.

De nombreux protocoles Internet standard se fient aux données de recherche des zones inversées pour valider les informations des zones directes. Par exemple, si la recherche directe indique que training.contoso.com est résolu en 192.168.2.45, vous pouvez utiliser une recherche inversée pour confirmer que 192.168.2.45 est associé à training.contoso.com.

Remarque : Dans Windows Server 2008 R2 et Windows Server 2012, vous pouvez également utiliser la technologie DNSSec pour effectuer un type de vérification similaire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

De nombreux serveurs de messagerie utilisent une recherche inversée pour réduire le volume de courrier indésirable. En effectuant une recherche inversée, les serveurs de messagerie tentent de détecter les serveurs SMTP (Simple Mail Transfer Protocol () ouverts (relais ouverts).

Il est important de disposer d'une zone de recherche inversée si vous avez des applications qui s'appuient sur la recherche d'hôtes en fonction de leurs adresses IP. De nombreuses applications enregistrent ces informations dans des journaux de sécurité ou des événements. Si vous observez une activité suspecte pour une adresse IP particulière, vous pouvez rechercher le nom d'hôte à l'aide des informations de la zone inversée.

Enregistrements de ressources

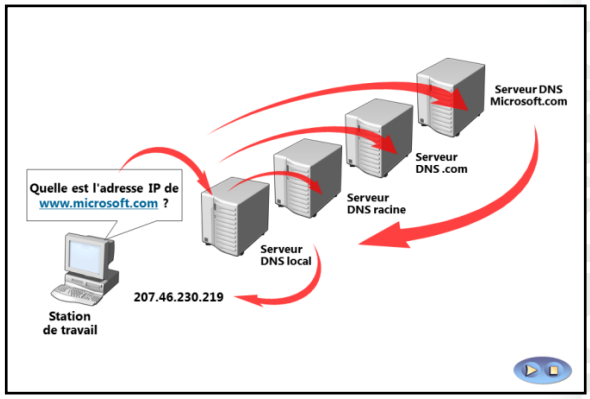
Le fichier de zone DNS stocke les enregistrements de ressources. Les enregistrements de ressources spécifient un type de ressource et l'adresse IP permettant de localiser la ressource. L'enregistrement de ressource le plus courant est un enregistrement de ressource d'hôte (A). Il s'agit d'un enregistrement simple qui résout un nom d'hôte en une adresse IP. L'hôte peut être une station de travail, un serveur ou un autre périphérique réseau, tel qu'un routeur.

Les enregistrements de ressources facilitent également la recherche de ressources pour un domaine particulier. Par exemple, lorsqu'un serveur Microsoft Exchange Server a besoin de trouver le serveur responsable de la remise du courrier d'un autre domaine, il demande l'enregistrement de ressource du serveur de messagerie (MX) de ce domaine. Cet enregistrement pointe vers l'enregistrement de ressource d'hôte (A) de l'hôte qui exécute le service de messagerie SMTP (Simple Mail Transfer Protocol).

Les enregistrements de ressources peuvent également contenir des attributs personnalisés. Les enregistrements MX, par exemple, comportent un attribut de préférence, qui s'avère utile si une organisation possède plusieurs serveurs de messagerie. L'enregistrement MX indique au serveur d'envoi quel serveur de messagerie l'organisation réceptrice préfère. Les enregistrements SRV contiennent également des informations sur le port que le service écoute et sur le protocole que vous devez utiliser pour communiquer avec le service.

Résolution des noms DNS Internet

Lors de la résolution de noms DNS sur Internet, tout un système d'ordinateurs est utilisé au lieu d'un seul serveur. Il existe des centaines de serveurs sur Internet, appelés *serveurs racine*, qui gèrent l'ensemble du processus de résolution DNS. Ces serveurs sont représentés par 13 noms de domaine complets. Une liste de ces 13 serveurs est préchargée sur chaque serveur DNS. Lorsque vous inscrivez un nom de domaine sur Internet, vous payez pour faire partie de ce système.



Pour voir comment ces serveurs fonctionnent conjointement afin de résoudre un nom DNS, examinez le processus de résolution de noms suivant pour le nom www.microsoft.com :

1. Un poste de travail interroge le serveur DNS local pour obtenir l'adresse IP de www.microsoft.com.
2. Si le serveur DNS local ne dispose pas de l'information, il interroge un serveur DNS racine pour connaître l'emplacement des serveurs DNS .com.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

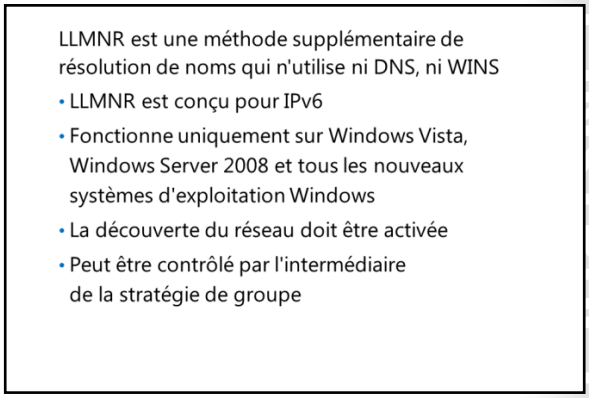
3. Le serveur DNS local interroge un serveur DNS .com pour connaître l'emplacement des serveurs DNS microsoft.com.
4. Le serveur DNS local interroge le serveur DNS microsoft.com pour connaître l'adresse IP de www.microsoft.com.
5. L'adresse IP de www.microsoft.com est retournée au poste de travail.

Le processus de résolution de noms peut être modifié par mise en cache ou par redirection :

- Mise en cache. Une fois qu'un serveur DNS local a résolu un nom DNS, il met en cache les résultats pendant environ 24 heures. Les requêtes de résolution ultérieures du nom DNS obtiennent les informations mises en cache.
- Redirection. Au lieu d'interroger les serveurs racine, vous pouvez configurer un serveur DNS pour rediriger les requêtes DNS vers un autre serveur DNS. Par exemple, les requêtes portant sur tous les noms Internet peuvent être redirigées vers un serveur DNS chez un fournisseur de services Internet.

Qu'est-ce que la résolution LLMNR (Link-Local Multicast Name Resolution) ?

Dans Windows Server 2012, la résolution LLMNR (Link-local Multicast Name Resolution) est une nouvelle méthode de résolution des noms en adresses IP. En raison de diverses limitations (qui ne sont pas traitées dans ce cours), la résolution LLMNR est généralement utilisée sur les réseaux localisés uniquement. Bien que la résolution LLMNR puisse résoudre les adresses IPv4, elle a été conçue spécifiquement pour le protocole IPv6. Par conséquent, si vous voulez l'utiliser, IPv6 doit être pris en charge et activé sur vos hôtes.



La résolution LLMNR est couramment utilisée dans les réseaux où :

- il n'y a aucun service DNS ou NetBIOS pour la résolution de noms ;
- l'implémentation de ces services n'est pas pratique pour une raison quelconque ;
- ces services ne sont pas disponibles.

Par exemple, vous voulez mettre en place un réseau temporaire à des fins de test, sans une infrastructure serveur.

La résolution LLMNR est prise en charge sur Windows Vista®, Windows Server 2008 et tous les nouveaux systèmes d'exploitation Windows. Elle utilise un système simple de messages de requête et de réponse pour résoudre les noms d'ordinateurs en adresses IPv6 ou IPv4. Pour qu'un nœud réponde à une requête de résolution LLMNR, la découverte réseau doit être activée. Toutefois, cette méthode n'est pas seulement nécessaire pour effectuer une requête de résolution de noms.

Pour utiliser la résolution LLMNR, vous devez activer la fonctionnalité de découverte du réseau pour tous les nœuds du sous-réseau local. Cette fonctionnalité est disponible dans le Centre Réseau et partage. Gardez à l'esprit que la découverte du réseau est généralement désactivée pour les réseaux que vous désignez comme publics.

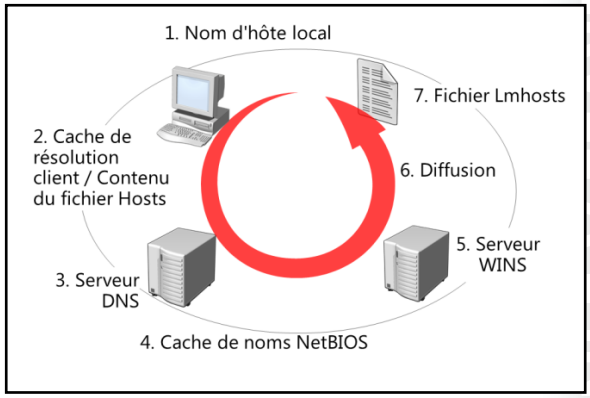
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous voulez contrôler l'utilisation de la résolution LLMNR sur votre réseau, vous pouvez la configurer via une stratégie de groupe. Pour désactiver la résolution LLMNR via une stratégie de groupe, définissez la valeur de stratégie de groupe suivante :

> Stratégie de groupe = Configuration de l'ordinateur\Modèles d'administration\Réseau\Client DNS\Désactiver la résolution de noms multidiffusion.
>
> Définissez cette valeur sur Activé si vous ne voulez pas utiliser la résolution LLMNR, ou sur Désactivé si vous voulez utiliser la résolution LLMNR.

Comment un client résout un nom

Les systèmes d'exploitation Windows prennent en charge plusieurs méthodes distinctes pour résoudre les noms d'ordinateurs, par exemple DNS, WINS et le processus de résolution de noms d'hôtes.



DNS

Comme indiqué précédemment, DNS est la norme Microsoft de résolution de noms d'hôtes en adresses IP. Pour plus d'informations sur DNS, consultez la deuxième rubrique de ce cours *Qu'est-ce que DNS*.

WINS

WINS fournit une base de données centralisée qui permet d'inscrire les mappages dynamiques des noms NetBIOS d'un réseau. Les systèmes d'exploitation Windows conservent la prise en charge de WINS pour assurer une compatibilité descendante.

Vous pouvez résoudre les noms NetBIOS en utilisant les options suivantes :

- Messages de diffusion. Les messages de diffusion, toutefois, ne fonctionnent pas bien sur les réseaux de grande envergure, car les routeurs ne transmettent pas de diffusion.
- Fichier Lmhosts sur tous les ordinateurs. L'utilisation d'un fichier Lmhosts pour la résolution de noms NetBIOS est une solution qui requiert une maintenance élevée, car vous devez maintenir le fichier manuellement sur tous les ordinateurs.
- Fichier Hosts sur tous les ordinateurs. À l'image d'un fichier Lmhosts, vous pouvez également utiliser un fichier Hosts pour la résolution de noms NetBIOS. Ce fichier est également stocké localement sur chaque ordinateur. Il est utilisé pour les mappages fixes de noms aux adresses IP sur le segment réseau local.

Remarque : Le rôle serveur DNS dans Windows Server 2008 R2 et Windows Server 2012 fournit également un nouveau type de zone, la zone GlobalNames. Vous pouvez utiliser la zone GlobalNames pour résoudre les noms en une partie qui sont uniques 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.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Processus de résolution de noms d'hôtes

Lorsqu'une application spécifie un nom d'hôte et utilise des sockets Windows, le protocole TCP/IP utilise le cache de résolution DNS et DNS lors de la tentative de résolution de noms d'hôtes. Le fichier d'hôtes est chargé dans le cache de résolution DNS. Si NetBIOS sur TCP/IP est activé, TCP/IP utilise également des méthodes de résolution de noms NetBIOS lors de la résolution de noms d'hôtes.

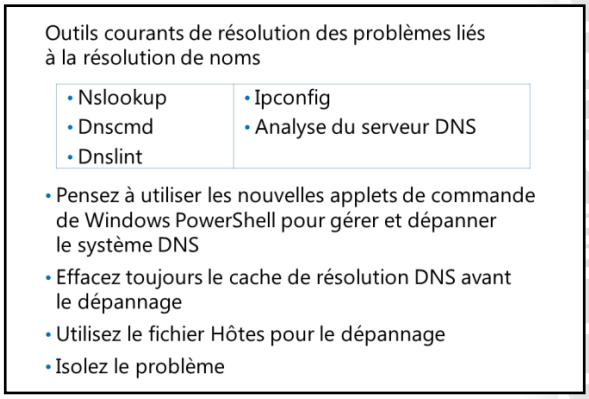
Les systèmes d'exploitation Windows résolvent les noms d'hôtes en effectuant les tâches suivantes dans cet ordre précis :

1. Vérification de la similarité du nom d'hôte et du nom d'hôte local.
2. Recherche du cache de résolution DNS ; Dans le cache de résolution du client DNS, les entrées du fichier Hosts sont préchargées.
3. Envoi d'une demande DNS à ses serveurs DNS configurés.
4. Conversion du nom d'hôte en un nom NetBIOS et vérification du cache de noms NetBIOS local.
5. Contact des serveurs WINS configurés de l'hôte.
6. Diffusion de trois messages maximum de demande de requête de nom NetBIOS sur le sous-réseau connecté directement.
7. Recherche du fichier Lmhosts.

Remarque : Vous pouvez contrôler l'ordre utilisé pour résoudre les noms. Par exemple, si vous désactivez NetBIOS sur TCP/IP, aucune des méthodes de résolution de noms NetBIOS n'est tentée. Vous pouvez aussi modifier le type de nœud NetBIOS, ce qui change l'ordre dans lequel les méthodes de résolution de noms NetBIOS sont tentées.

Résolution des problèmes liés à la résolution de noms

Comme pour la plupart des autres technologies, la résolution de noms requiert parfois une résolution des problèmes correspondants. Des problèmes peuvent se produire lorsque le serveur DNS, ses zones et ses enregistrements de ressources ne sont pas configurés correctement. Lorsque des enregistrements de ressources provoquent des problèmes, il peut s'avérer parfois plus difficile d'identifier le vrai problème parce que les problèmes de configuration ne sont pas toujours évidents.



Outils et commandes

Les outils en ligne de commande et les commandes que vous utilisez pour résoudre les problèmes de configuration sont les suivants :

- **Nslookup** : utilisez cet outil pour interroger des informations DNS. Il s'agit d'un outil flexible, capable de fournir des informations précieuses à propos de l'état du serveur DNS. Vous pouvez également l'utiliser pour rechercher des enregistrements de ressources et valider leur configuration. Vous pouvez, en outre, tester des transferts de zone, des options de sécurité et la résolution des enregistrements MX.
- **DNSCmd** : utilisez cet outil en ligne de commande pour gérer le rôle serveur DNS. Cet outil permet de créer des scripts dans des fichiers de commandes dans le but d'automatiser des tâches de gestion DNS de routine ou de procéder à un simple travail d'installation et de configuration sans assistance de nouveaux serveurs DNS sur votre réseau.
- **Dnslint** : utilisez cet outil pour diagnostiquer les problèmes DNS courants. Cet outil diagnostique rapidement les problèmes de configuration de DNS et peut générer un rapport au format HTML sur l'état du domaine que vous testez.
- **Ipconfig** : utilisez cette commande pour afficher et modifier les détails de la configuration IP que l'ordinateur utilise. Cet outil inclut des options de ligne de commande supplémentaires que vous pouvez utiliser pour dépanner et prendre en charge des clients DNS. Vous pouvez consulter le cache DNS local du client à l'aide de la commande **ipconfig/displaydns**. En outre, vous pouvez effacer le cache local à l'aide de **ipconfig/flushdns**. Si vous voulez réinscrire un hôte dans DNS, vous pouvez utiliser **ipconfig /registerdns**.
- **Analyse du serveur DNS**: pour tester si le serveur peut communiquer avec des serveurs en amont, vous pouvez effectuer de simples requêtes locales et récursives à partir de l'onglet **Analyse** du serveur DNS. Vous pouvez également planifier ces tests pour qu'ils s'exécutent de manière régulière. L'onglet **Analyse** du serveur DNS est disponible uniquement dans Windows Server 2008 et Windows Server 2012, dans la boîte de dialogue **Propriétés de : *nom du serveur DNS***. L'applet de commande **Test-DNSServer** peut également servir à vérifier les fonctionnalités du serveur DNS.

Dans Windows Server 2012, il existe un nouvel ensemble d'applets de commande Windows PowerShell® que vous pouvez utiliser pour la gestion des clients et serveurs DNS. Voici certaines des applets de commande les plus fréquemment utilisées :

- **Clear-DNSClientCache**. Cette applet de commande efface le cache client, à l'instar de **ipconfig /flushdns**.
- **Get-DNSClient**. Cette applet de commande affiche les détails des interfaces réseau.
- **Get-DNSClientCache**. Cette applet de commande affiche le contenu du cache client DNS local.
- **Register-DNSClient**. Cette applet de commande inscrit toutes les adresses IP de l'ordinateur sur le serveur DNS configuré.
- **Resolve-DNSName**. Cette applet de commande effectue une résolution de noms DNS pour un nom spécifique, à l'instar de **Nslookup**.
- **Set-DNSClient**. Cette applet de commande définit les configurations de client DNS spécifiques à l'interface sur l'ordinateur.

Ces applets de commande vous permettent également d'utiliser plusieurs commutateurs et options, ce qui vous donne accès à des options et des fonctionnalités supplémentaires.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Processus de résolution des problèmes

Lorsque vous résolvez des problèmes liés à la résolution de noms, vous devez identifier les méthodes de résolution de noms utilisées par l'ordinateur, ainsi que l'ordre dans lequel l'ordinateur les utilise. Veillez à effacer le cache de résolution DNS entre les tentatives de résolution. Si vous ne pouvez pas vous connecter à un hôte distant et si vous pensez qu'il existe un problème de résolution de noms, vous pouvez résoudre le problème lié à la résolution de noms en procédant comme suit :

1. Ouvrez une invite de commandes avec élévation de privilèges, puis désactivez le cache de résolution DNS en tapant **ipconfig /flushdns**. Vous pouvez aussi ouvrir Windows PowerShell et utiliser l'applet de commande **Clear-DNSClientCache** équivalente.
2. Tentez d'effectuer un test ping de l'hôte distant à l'aide de son adresse IP. Cela permet de déterminer si le problème est lié à la résolution de noms. Si le test ping réussit avec l'adresse IP mais qu'il échoue avec le nom d'hôte correspondant, cela signifie que le problème est lié à la résolution de noms.
3. Tentez d'effectuer un test ping de l'hôte distant à l'aide de son nom d'hôte. Pour plus de précision, utilisez le nom de domaine complet avec un point final. Par exemple, si vous travaillez chez Contoso, Ltd, entrez la commande suivante à l'invite de commandes : **Ping LON-dc1.contoso.com**.
4. Si le test ping réussit, cela signifie que le problème n'est probablement pas lié à la résolution de noms. Si le test ping échoue, modifiez le fichier texte C:\windows\system32\drivers\etc\hosts, puis ajoutez l'entrée appropriée à la fin du fichier. Dans l'exemple précédent de Contoso, Ltd, vous devez ajouter la ligne ci-après et enregistrer le fichier :

   10.10.0.10 LON-dc1.contoso.com
5. Recommencez le test ping à l'aide du nom d'hôte. La résolution de noms doit maintenant s'effectuer correctement. Assurez-vous que le nom a été résolu correctement en examinant le cache de résolution DNS. Pour afficher le cache de résolution DNS, à l'invite de commandes, tapez **IPConfig /displaydns**, ou utilisez l'applet de commande Windows PowerShell équivalente.
6. Supprimez l'entrée que vous avez ajoutée au fichier Hosts, puis effacez à nouveau le cache de résolution.
7. À l'invite de commandes, tapez la commande suivante, puis examinez le contenu du fichier filename.txt afin d'identifier l'étape qui a échoué lors de la résolution de noms :

```
Nslookup.exe -d2 LON-dc1.contoso.com. > filename.txt
```

Remarque : Vous devez également savoir comment interpréter la sortie du cache de résolution DNS afin de pouvoir déterminer si le problème de résolution de noms se situe au niveau de la configuration de l'ordinateur client, du serveur de noms ou de la configuration des enregistrements dans la base de données de zone du serveur de noms. L'interprétation de la sortie du cache de résolution DNS n'est pas traitée dans ce cours.

Leçon 2
Installation et gestion d'un serveur DNS

Pour utiliser un service Serveur DNS, vous devez d'abord l'installer. L'installation du service Serveur DNS sur un serveur DNS est une procédure simple. Pour gérer votre service Serveur DNS, il est important que vous compreniez le fonctionnement des composants du serveur DNS et leur finalité. Dans ce cours, vous découvrirez les composants DNS. Vous apprendrez également comment installer et gérer le rôle serveur DNS.

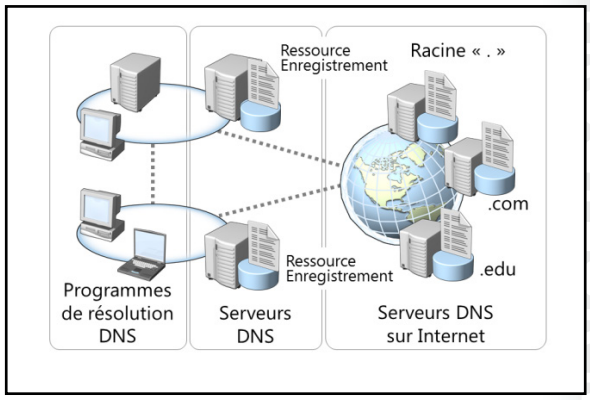
Objectifs de la leçon

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

- décrire les composants d'une solution DNS ;
- décrire les indications de racine ;
- décrire les requêtes DNS ;
- décrire la redirection ;
- expliquer le fonctionnement de la mise en cache du serveur DNS ;
- expliquer comment installer le rôle serveur DNS.

Quels sont les composants d'une solution DNS ?

Les composants d'une solution DNS incluent les serveurs DNS, les serveurs DNS sur Internet et les résolutions DNS (ou *clients DNS*).



Serveur DNS

Un serveur DNS répond aux requêtes DNS récursives et itératives. Les serveurs DNS peuvent également héberger une ou plusieurs zones d'un domaine particulier. Les zones contiennent différents enregistrements de ressources. Les serveurs DNS peuvent également mettre en cache des recherches afin de gagner du temps pour les requêtes communes.

Serveurs DNS sur Internet

Les serveurs DNS sur Internet sont accessibles au public. Ces serveurs hébergent des informations sur les domaines publics, tels que les domaines de premier niveau (par exemple .com, .net et .edu).

Résolution DNS

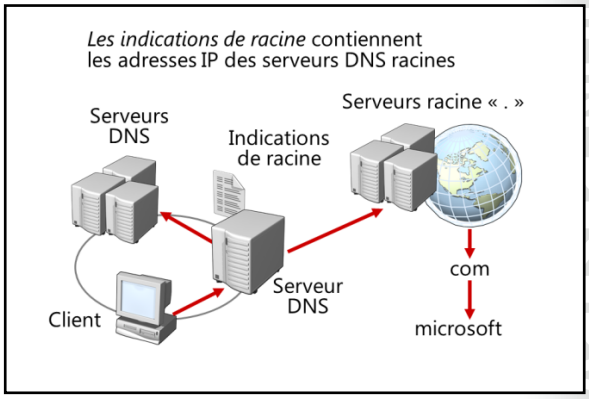
La résolution DNS génère et envoie des requêtes itératives ou récursives au serveur DNS. Une résolution DNS peut être un ordinateur qui exécute une recherche DNS nécessitant une interaction avec le serveur DNS. Les serveurs DNS peuvent également publier des demandes DNS sur d'autres serveurs DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les indications de racine ?

Les indications de racine correspondent à une liste de 13 noms de domaine complets sur Internet que votre serveur DNS utilise s'il ne parvient pas à résoudre une requête DNS en utilisant ses propres données de zone, un redirecteur DNS ou son propre cache. Les indications de racine répertorient les serveurs les plus élevés dans la hiérarchie DNS et peuvent fournir les informations nécessaires à un serveur DNS pour qu'il exécute une requête itérative sur la couche inférieure suivante de l'espace de noms DNS.



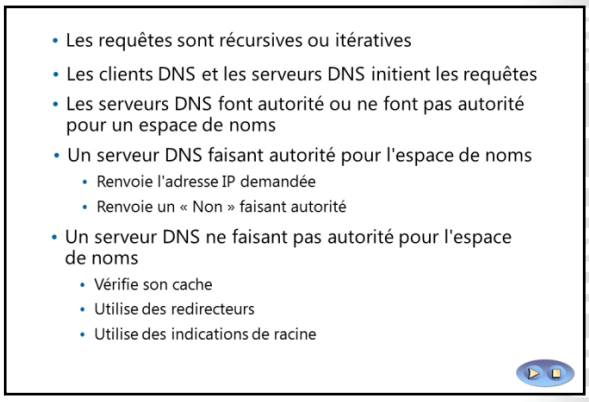
Les serveurs racine sont automatiquement installés lorsque vous installez le rôle DNS. Ils sont copiés à partir du fichier cache.dns inclus dans les fichiers d'installation du rôle DNS. Vous pouvez également ajouter des indications de racine à un serveur DNS pour prendre en charge des recherches de domaines non contigus dans une forêt.

Lorsqu'un serveur DNS communique avec un serveur d'indications de racine, il utilise uniquement une requête itérative. Si vous sélectionnez l'option **Ne pas utiliser la récursivité pour ce domaine** (dans la boîte de dialogue **Propriétés du serveur DNS**), le serveur ne sera pas en mesure d'exécuter des requêtes sur les indications de racine. Si vous configurez le serveur à l'aide d'un redirecteur, il va tenter d'envoyer une requête récursive à son serveur de redirection. Si le serveur de redirection ne répond pas à cette requête, le premier serveur répond que l'hôte est introuvable.

Il est important de comprendre que la récursivité sur un serveur DNS et les requêtes récursives ne sont pas la même chose. La récursivité sur un serveur DNS signifie que le serveur utilise ses indications de racine pour tenter de résoudre une requête DNS, alors qu'une requête récursive est une requête adressée à un serveur DNS, où le demandeur demande au serveur de se charger de fournir une réponse complète à la requête. Les rubriques suivantes décrivent les requêtes récursives de manière plus approfondie.

Que sont les requêtes DNS ?

Une *requête DNS* est une requête de résolution de noms envoyée à un serveur DNS. Le serveur DNS fournit ensuite une réponse faisant autorité ou ne faisant pas autorité à la requête du client.



Remarque : Il est important de noter que les serveurs DNS peuvent également servir de programmes de résolution DNS et envoyer des requêtes DNS à d'autres serveurs DNS.

Réponses faisant autorité ou ne faisant pas autorité

Les deux types de réponse sont les suivants :

- Faisant autorité. Une réponse faisant autorité est une réponse que le serveur retourne et qu'il sait correcte, car la requête est adressée au serveur faisant autorité qui gère le domaine. Un serveur DNS fait autorité lorsqu'il héberge une copie principale ou secondaire d'une zone DNS.
- Ne faisant pas autorité. Une réponse ne faisant pas autorité est une réponse où le serveur DNS qui contient le domaine demandé dans son cache répond à une requête en utilisant des redirecteurs ou des indications de racine. Dans la mesure où la réponse fournie risque de ne pas être exacte (car seul le serveur DNS faisant autorité pour le domaine donné peut émettre cette information), il s'agit d'une réponse ne faisant pas autorité.

Si le serveur DNS fait autorité pour l'espace de noms de la requête, il vérifie la zone, puis réagit de l'une des manières suivantes :

- Il renvoie l'adresse demandée.
- Il renvoie une réponse de type « Non, ce nom n'existe pas » faisant autorité.

Remarque : Une réponse faisant autorité peut être donnée uniquement par le serveur faisant autorité directe pour le nom demandé.

S'il ne fait pas autorité pour l'espace de noms de la requête, le serveur DNS local réagit de l'une des manières suivantes :

- Il vérifie son cache et renvoie une réponse mise en cache.
- Il transmet la requête qu'il ne sait pas résoudre à un serveur spécifique appelé *redirecteur*.
- Il utilise les adresses connues de plusieurs serveurs racine pour rechercher un serveur DNS faisant autorité afin de résoudre la requête. Ce processus utilise des indications de racine.

Requêtes récursives

Dans une requête récursive, le demandeur demande au serveur DNS une adresse IP entièrement résolue de la ressource demandée, avant de retourner la réponse au demandeur. Le serveur DNS peut être amené à effectuer plusieurs requêtes destinées à d'autres serveurs DNS avant de trouver la réponse recherchée. Les requêtes récursives sont généralement effectuées par un client DNS vers un serveur DNS, ou par un serveur DNS configuré pour transmettre les requêtes non résolues vers un autre serveur DNS, dans le cas d'un serveur DNS configuré pour utiliser un redirecteur.

Une requête récursive a deux résultats possibles :

- Le serveur DNS renvoie l'adresse IP de l'hôte demandé.
- Le serveur DNS ne peut pas résoudre une adresse IP.

Pour des raisons de sécurité, il est parfois nécessaire de désactiver les requêtes récursives sur un serveur DNS. Ainsi, le serveur DNS en question n'essaiera pas de transférer ses demandes DNS à un autre serveur. Cette désactivation peut s'avérer utile lorsque vous ne souhaitez pas qu'un serveur DNS particulier communique à l'extérieur de son réseau local.

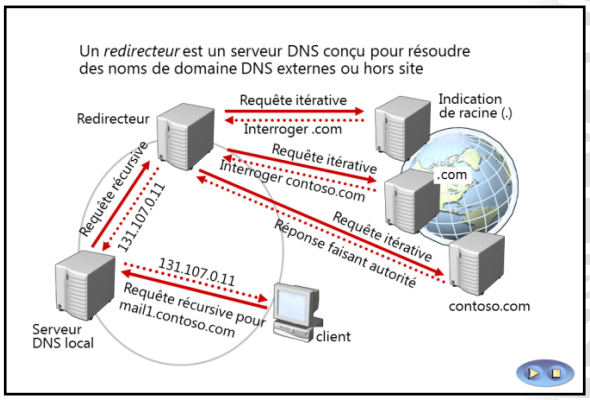
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Requêtes itératives

Les requêtes itératives ont accès aux informations de noms de domaine qui se trouvent sur le système DNS. À l'aide des requêtes itératives, vous pouvez résoudre rapidement et efficacement des noms sur de nombreux serveurs. Lorsqu'un serveur DNS reçoit une demande à laquelle il ne peut pas répondre en utilisant ses informations locales ou ses recherches mises en cache, il fait la même demande à un autre serveur DNS en utilisant une requête itérative. Lorsqu'un serveur DNS reçoit une requête itérative, il peut répondre soit en indiquant l'adresse IP du nom de domaine (s'il la connaît), soit en adressant la demande aux serveurs DNS responsables du domaine sur lequel porte la requête. Le serveur DNS poursuit ce processus jusqu'à ce qu'il trouve un serveur DNS qui fait autorité pour le nom demandé, jusqu'à ce qu'une erreur se produise ou jusqu'à l'expiration du délai.

Qu'est-ce que le transfert ?

Un *redirecteur* est un serveur DNS réseau qui transfère des requêtes DNS de noms DNS externes aux serveurs DNS situés à l'extérieur de son réseau. Vous pouvez également utiliser des redirecteurs conditionnels pour transférer des requêtes en fonction de noms de domaine spécifiques.



Une fois que vous avez désigné un serveur DNS réseau en tant que redirecteur, d'autres serveurs DNS de ce réseau transfèrent les requêtes qu'ils ne savent pas résoudre localement à ce serveur. À l'aide d'un redirecteur, vous pouvez gérer la résolution de noms pour les noms externes à votre réseau, par exemple les noms situés sur Internet. Cela améliore l'efficacité de la résolution de noms pour les ordinateurs de votre réseau.

Le redirecteur doit être en mesure de communiquer avec le serveur DNS situé sur Internet. Cela signifie que soit vous le configurez afin de transférer les demandes à un autre serveur DNS, soit vous le configurez afin d'utiliser des indications de racine pour communiquer.

Méthode conseillée : Utilisez un serveur DNS de redirection central pour la résolution de noms Internet. Cela peut améliorer la sécurité, car vous pouvez isoler le serveur DNS de redirection dans un réseau de périmètre, lequel garantit qu'aucun serveur au sein du réseau ne communique directement avec Internet.

Redirecteur conditionnel

Un *redirecteur conditionnel* est un serveur DNS sur un réseau qui transfère des requêtes DNS en fonction du nom de domaine DNS de la requête. 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.contoso.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.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

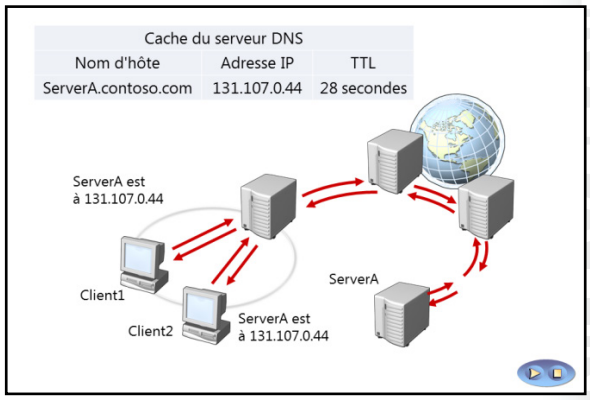
Redirection conditionnelle dans Windows Server 2008 R2 et Windows Server 2012

Dans Windows Server 2008 R2 et Windows Server 2012, la configuration des redirecteurs conditionnels a été déplacée vers un nœud dans la console de configuration DNS. Vous pouvez répliquer ces informations sur d'autres serveurs DNS via l'intégration du service DNS à Active Directory.

Méthode conseillée : Utilisez des redirecteurs conditionnels si vous avez plusieurs espaces de noms internes. Ainsi, la résolution de noms est plus rapide.

Fonctionnement de la mise en cache du serveur DNS

La mise en cache DNS augmente les performances du système DNS de l'organisation en accélérant les recherches DNS.



Lorsqu'un serveur DNS résout correctement un nom DNS, il ajoute ce nom à son cache. Au fur et à mesure, il génère un cache des noms de domaine et de leurs adresses IP associées pour la plupart des domaines que l'organisation utilise ou auxquels elle accède. La durée par défaut de conservation d'un nom dans le cache est d'une heure. Le propriétaire d'une zone peut changer ce paramètre en modifiant l'enregistrement SOA pour la zone DNS appropriée.

Un serveur cache uniquement est le type idéal de serveur DNS à utiliser en tant que redirecteur. Il n'héberge aucune donnée de zone DNS. Il répond uniquement aux requêtes de recherche des clients DNS.

Dans Windows Server 2012, vous pouvez accéder au contenu du cache du serveur DNS en sélectionnant l'affichage Avancé dans la console du Gestionnaire DNS. Lorsque vous activez cet affichage, le contenu mis en cache s'affiche sous la forme d'un nœud dans le Gestionnaire DNS. Vous pouvez également supprimer des entrées spécifiques (ou la totalité) du cache du serveur DNS. Vous pouvez également utiliser l'applet de commande Windows PowerShell **Get-DNSServerCache** pour afficher le contenu du cache.

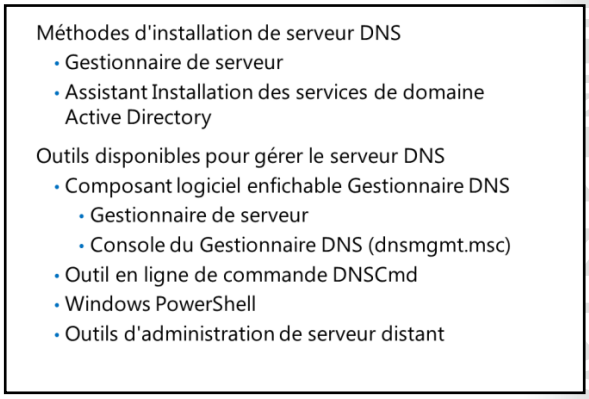
Le cache client DNS est stocké sur l'ordinateur local par le service client DNS. Pour voir la mise en cache côté client, à une invite de commandes, exécutez la commande **ipconfig /displaydns**. Cela permet d'afficher le cache client DNS local. Si vous avez besoin d'effacer le cache local, vous pouvez utiliser **ipconfig /flushdns**. Pour ce faire, vous pouvez également utiliser les applets de commande Windows PowerShell **Get-DNSClientCache** et **Clear-DNSClientCache**.

Pour empêcher les caches clients DNS d'être remplacés, utilisez la fonctionnalité de verrouillage de cache DNS, disponible dans Windows Server 2008 R2 et Windows Server 2012. Lorsque cette fonctionnalité est activée, les enregistrements mis en cache ne sont pas remplacés pendant la valeur de la durée de vie (TTL, Time to Live). Le verrouillage du cache fournit une sécurité améliorée contre les attaques par empoisonnement du cache.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment installer le rôle serveur DNS

Par défaut, le rôle serveur DNS n'est pas installé sur Windows Server 2012. En fait, vous devez l'ajouter comme un rôle lorsque vous configurez le serveur pour effectuer ce rôle. Vous installez le rôle serveur DNS à l'aide de l'Assistant Ajout de rôles et de fonctionnalités dans le Gestionnaire de serveur.



Vous pouvez également ajouter le rôle serveur DNS lorsque vous effectuez la promotion de votre serveur en contrôleur de domaine. Pour ce faire, utilisez la page **Options** du contrôleur de domaine de l'Assistant Installation des services de domaine Active Directory.

Une fois que vous avez installé le rôle serveur DNS, le composant logiciel enfichable Gestionnaire DNS peut être ajouté à vos consoles d'administration. Le composant logiciel enfichable est automatiquement ajouté à la console du Gestionnaire de serveur et à la console du Gestionnaire DNS. Vous pouvez exécuter le Gestionnaire DNS à partir de la zone Accueil en tapant **dnsmgmt.msc**.

Lorsque vous installez le rôle serveur DNS, l'outil en ligne de commande dnscmd.exe est également ajouté. Vous pouvez utiliser l'outil DNSCmd pour créer un script de la configuration DNS et automatiser cette dernière. Pour obtenir de l'aide sur cet outil, à l'invite de commandes, tapez : **dnscmd.exe /?**.

Dans Windows Server 2012, vous pouvez également utiliser Windows PowerShell pour gérer un serveur DNS. Il est recommandé d'utiliser les applets de commande Windows PowerShell pour gérer le serveur DNS à l'aide de lignes de commande. En outre, vous pouvez utiliser les outils en ligne de commande Nslookup, DNSCmd, Dnslint et Ipconfig dans l'environnement Windows PowerShell.

Pour administrer un serveur DNS distant, ajoutez les Outils d'administration de serveur distant sur votre poste de travail d'administration, lequel doit exécuter Windows Vista Service Pack 1 (SP1) ou une version plus récente du système d'exploitation Windows.

Démonstration : Installation du rôle de serveur DNS

De nombreuses organisations possèdent déjà ou veulent plusieurs serveurs DNS sur leur réseau. Vous pouvez installer des serveurs DNS à l'aide de la console du Gestionnaire de serveur. Pour permettre à votre serveur DNS de résoudre les noms Internet, vous devrez probablement activer la redirection.

Dans cette démonstration, vous allez apprendre à :

- installer un second serveur DNS ;
- configurer le transfert.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Installer un second serveur DNS

1. Connectez-vous à LON-DC1 et LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-SVR1, ouvrez le **Gestionnaire de serveur**.
3. Démarrez l'**Assistant Ajout de rôles et de fonctionnalités**.
4. Ajoutez le rôle serveur DNS.

Configurer le transfert

- Configurez le serveur DNS avec un redirecteur sur l'adresse IP **172.16.0.10**.

Remarque : Laissez tous les ordinateurs virtuels dans leur état actuel pour la démonstration suivante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Gestion des zones DNS

Le serveur DNS héberge les données de zone dans une base de données Active Directory ou dans le fichier de zone. En outre, le serveur DNS peut héberger plusieurs types de zone. Dans ce cours, vous découvrirez les types de zone DNS et les zones DNS intégrées à Active Directory.

Objectifs de la leçon

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

- décrire les types de zones DNS ;
- décrire les mises à jour dynamiques ;
- décrire les zones intégrées à Active Directory ;
- expliquer comment créer une zone intégrée à Active Directory.

Quels sont les types de zone DNS ?

Il existe quatre types de zone DNS :

- Principale
- Secondary
- Stub
- Intégrée à Active Directory

Zones	Description
Principale	Copie en lecture/écriture d'une base de données DNS
Secondary	Copie en lecture seule d'une base de données DNS
Stub	Copie d'une zone contenant uniquement des enregistrements utilisés pour localiser des serveurs de noms
Intégrée à–Active Directory	Données de zone stockées dans AD DS plutôt que dans des fichiers de zone

Zone principale

Une zone principale est une zone pour laquelle le serveur DNS est à la fois l'hôte et la source principale des informations relatives à cette zone. En outre, le serveur DNS stocke la copie principale des données de zone dans un fichier local ou dans les services AD DS. Lorsque le serveur DNS stocke la zone dans un fichier, le fichier de la zone principale est nommé par défaut *nom_zone*.dns et se trouve sur le serveur dans le dossier %windir%\System32\Dns. Lorsque la zone n'est pas stockée dans les services AD DS, il s'agit du seul serveur DNS qui dispose d'une copie accessible en écriture de la base de données.

Zone secondaire

Une zone secondaire est une zone pour laquelle le serveur DNS sert d'hôte mais où il représente la source secondaire des informations de zone. Les informations relatives à la zone au niveau de ce serveur doivent être obtenues à partir d'un autre serveur DNS distant qui héberge également la zone. Ce serveur DNS doit avoir un accès réseau au serveur DNS distant pour recevoir les informations mises à jour de la zone. Étant donné qu'une zone secondaire est une copie d'une zone principale qu'un autre serveur héberge, la zone secondaire ne peut pas être stockée dans les services AD DS. Les zones secondaires peuvent s'avérer utiles si vous répliquez des données provenant de zones DNS non Windows.

Zone de stub

Une zone de stub est une copie répliquée 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 les noms entre des espaces de noms DNS distincts, lesquels peuvent s'avérer nécessaires lorsqu'une fusion d'entreprises a besoin que les serveurs DNS de deux espaces de noms DNS distincts résolvent les noms des clients dans les deux espaces de noms.

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.

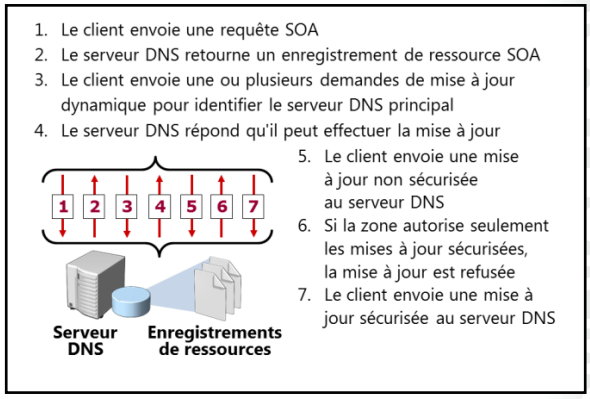
Les serveurs maîtres d'une zone de stub sont représentés par un ou plusieurs serveurs DNS qui font autorité pour la zone enfant. En règle générale, c'est le serveur DNS qui héberge la zone principale pour le nom de domaine délégué.

Zone intégrée à Active Directory

Si les services AD DS stockent les données de zone, le serveur DNS peut utiliser le modèle de réplication multimaître pour répliquer les données de la zone principale. Cela vous permet de modifier des données de zone sur plusieurs serveurs DNS simultanément.

Que sont les mises à jour dynamiques ?

Une mise à jour dynamique est une mise à jour de DNS en temps réel. Les mises à jour dynamiques sont importantes pour les clients DNS qui changent d'emplacement, car elles peuvent inscrire et mettre à jour dynamiquement leurs enregistrements de ressources sans intervention manuelle.



Le service client DHCP (Dynamic Host Configuration Protocol) effectue l'inscription, indépendamment du fait que l'adresse IP du client soit obtenue à partir d'un serveur DHCP ou qu'elle soit fixe. L'inscription a lieu lors des événements suivants :

- le client démarre et le service client DHCP a démarré ;
- une adresse IP est configurée, ajoutée ou modifiée sur n'importe quelle connexion réseau ;
- un administrateur exécute la commande **ipconfig /registerdns** à l'invite de commandes, ou exécute l'applet de commande Windows PowerShell **Register-DNSClient**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le processus relatif aux mises à jour dynamiques est le suivant :

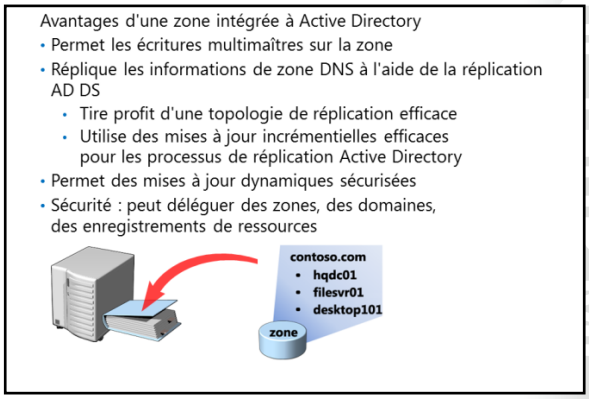
1. Le client identifie un serveur de noms et envoie une mise à jour. Si le serveur de noms héberge uniquement une zone secondaire, le serveur de noms refuse la mise à jour du client. Si la zone n'est pas une zone intégrée à Active Directory, le client peut être amené à effectuer cette opération plusieurs fois.
2. Si la zone prend en charge les mises à jour dynamiques, le client finit par joindre un serveur DNS qui peut écrire dans la zone. Ce serveur DNS est le serveur principal d'une zone standard, basée sur un fichier, ou un contrôleur de domaine qui représente le serveur de noms d'une zone intégrée à Active Directory.
3. Si la zone est configurée pour des mises à jour dynamiques sécurisées, le serveur DNS refuse la modification. Le client s'authentifie ensuite et renvoie la mise à jour.

Dans certaines configurations, vous ne voulez pas que les clients mettent à jour leurs enregistrements, même dans une zone de mise à jour dynamique. Dans ce cas, vous pouvez configurer le serveur DHCP afin qu'il inscrive les enregistrements pour le compte des clients. Par défaut, un client inscrit qu'il est un enregistrement (hôte/adresse) et le serveur DHCP inscrit l'enregistrement PTR (pointeur/recherche inversée).

Par défaut, les systèmes d'exploitation Windows tentent d'inscrire leurs enregistrements auprès de leur serveur DNS. Vous pouvez modifier ce comportement dans la configuration IP du client ou via une stratégie de groupe. Les contrôleurs de domaine inscrivent également leurs enregistrements SRV dans DNS, en plus de leurs enregistrements d'hôtes. Les enregistrements SRV sont inscrits chaque fois que le service NETLOGON démarre.

Que sont les zones intégrées à Active Directory ?

Un serveur DNS peut stocker des données de zone dans la base de données AD DS à condition que le serveur DNS soit un contrôleur de domaine AD DS. Lorsque le serveur DNS stocke des données de zone de cette façon, cela entraîne la création d'une zone intégrée à Active Directory.



Les avantages d'une zone intégrée à Active Directory sont importants :

- Mises à jour multimaîtres. Contrairement aux zones principales (qui ne peuvent être modifiées que par un seul serveur principal), les zones intégrées à Active Directory sont accessibles en écriture à n'importe quel contrôleur de domaine vers lequel la zone est répliquée. Cela permet d'établir une redondance dans l'infrastructure DNS. En outre, les mises à jour multimaîtres sont particulièrement importantes dans les organisations réparties géographiquement et qui utilisent des zones de mise à jour dynamique, car les clients peuvent mettre à jour leurs enregistrements DNS sans avoir à se connecter à un serveur principal potentiellement éloigné d'un point de vue géographique.
- Réplication des données de zone DNS à l'aide de la réplication AD DS. L'une des caractéristiques de la réplication Active Directory est la réplication au niveau de l'attribut, où seuls les attributs modifiés sont répliqués. Une zone intégrée à Active Directory peut tirer parti des avantages de la réplication Active Directory, au lieu de répliquer l'intégralité du fichier de zone comme dans les modèles classiques de redirection de zone DNS.

- Mises à jour dynamiques sécurisées. Une zone intégrée à Active Directory peut appliquer des mises à jour dynamiques sécurisées.
- Sécurité granulaire. Comme pour d'autres objets Active Directory, une zone intégrée à Active Directory vous permet de déléguer l'administration des zones, des domaines et des enregistrements de ressources en modifiant la liste de contrôle d'accès de la zone.

  Question : Pouvez-vous penser à des inconvénients liés au stockage des informations DNS dans les services AD DS ?

Démonstration : Création d'une zone intégrée à Active Directory

Pour créer une zone intégrée à Active Directory, vous devez installer un serveur DNS sur un contrôleur de domaine. Toutes les modifications apportées à une zone intégrée à Active Directory sont répliquées vers les autres serveurs DNS situés sur les contrôleurs de domaine via le modèle de réplication multimaître des services AD DS.

Dans cette démonstration, vous allez apprendre à :

- promouvoir un serveur en tant que contrôleur de domaine ;
- créer une zone intégrée à Active Directory ;
- créer un enregistrement ;
- vérifier la réplication vers un second serveur DNS.

Procédure de démonstration

Effectuer la promotion de LON-SVR1 en tant que contrôleur de domaine supplémentaire

1. Installez le rôle serveur AD DS.
2. Démarrez l'**Assistant Configuration des services de domaine Active Directory**.
3. Installez le service Serveur DNS.

Créer une zone intégrée à Active Directory

1. Sur LON-DC1, ouvrez la console du **Gestionnaire DNS**.
2. Démarrez l'**Assistant Nouvelle zone**.
3. Créez une zone de recherche directe intégrée à Active Directory.
4. Nommez la zone **Contoso.com**.
5. Autorisez uniquement les mises à jour dynamiques sécurisées.
6. Examinez les enregistrements de la nouvelle zone.

Créer un enregistrement

- Créez un enregistrement **Nouvel hôte** dans la zone Contoso.com nommée **www**, puis faites-le pointer vers **172.16.0.100**.

Vérifier la réplication vers un second serveur DNS

- Vérifiez que le nouvel enregistrement se réplique sur le serveur DNS **LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation de la réplication DNS

Scénario

La société A. Datum Corporation a un bureau et un centre de données informatiques à Londres qui prennent en charge le site de Londres ainsi que d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8. Vous devez configurer le service d'infrastructure pour une nouvelle filiale.

Votre responsable vous a demandé de configurer le contrôleur de domaine de la filiale en tant que serveur DNS. Il vous a également été demandé de créer des enregistrements d'hôtes pour assurer la prise en charge d'une nouvelle application en cours d'installation. Enfin, vous devez configurer la redirection sur le serveur DNS de la filiale pour prendre en charge la résolution de noms Internet.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- installer et configurer le système DNS ;
- créer des enregistrements d'hôtes dans DNS ;
- gérer le cache du serveur DNS.

Configuration de l'atelier pratique

Durée approximative : 40 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-SVR1 22410B-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 débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 : **Administrateur**
    - Mot de passe : **Pa$$w0rd**
    - Domaine : **ADATUM**
5. Répétez les étapes 2 à 4 pour **22410B-LON-SVR1** et **22410B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Installation et configuration du système DNS

Scénario

Dans le cadre de la configuration de l'infrastructure de la nouvelle filiale, vous devez configurer un serveur DNS qui fournira un service de résolution de noms à la filiale. Le serveur DNS de la filiale sera également un contrôleur de domaine. Les zones intégrées à Active Directory, qui sont nécessaires à la prise en charge des ouvertures de session, sont répliquées automatiquement vers la filiale.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer LON-SVR1 en tant que contrôleur de domaine sans installer le rôle serveur DNS (Domain Name System)
2. Créer et configurer la zone nwtraders.msft sur LON-DC1
3. Vérifier les paramètres de configuration sur le serveur DNS existant pour confirmer les indications de racine
4. Ajouter le rôle serveur DNS de la filiale au contrôleur de domaine
5. Vérifier la réplication de la zone intégrée à Active Directory Adatum.com
6. Utiliser Nslookup pour tester une résolution non locale
7. Configurer la résolution de noms Internet pour effectuer une redirection vers le siège
8. Utiliser Nslookup pour confirmer la résolution de noms

▶ Tâche 1 : Configurer LON-SVR1 en tant que contrôleur de domaine sans installer le rôle serveur DNS (Domain Name System)

1. Utilisez **Ajouter des rôles et des fonctionnalités** dans le Gestionnaire de serveur pour ajouter le rôle **Services AD DS** à LON-SVR1.
2. Démarrez l'**Assistant Ajout de rôles et de fonctionnalités** pour promouvoir LON-SVR1 en contrôleur de domaine.
3. Choisissez d'ajouter LON-SVR1 en tant que contrôleur de domaine supplémentaire au domaine **Adatum.com**.
4. N'installez pas le serveur DNS.

▶ Tâche 2 : Créer et configurer la zone nwtraders.msft sur LON-DC1

1. Sur l'ordinateur LON-DC1, ouvrez la console du **Gestionnaire DNS**.
2. Créez une zone de recherche directe avec les paramètres suivants :
   a. Nom de la zone : **nwtraders.msft**
   b. Type de zone : **Zone principale**
   c. Ne stockez pas la zone dans Active Directory.

▶ Tâche 3 : Vérifier les paramètres de configuration sur le serveur DNS existant pour confirmer les indications de racine

1. Dans le Gestionnaire DNS sur LON-DC1, ouvrez la boîte de dialogue **Propriétés** de **LON-DC1**.
2. Examinez les indications de racine et la configuration du redirecteur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Ajouter le rôle serveur DNS de la filiale au contrôleur de domaine

- Utilisez le Gestionnaire de serveur pour ajouter le rôle serveur DNS à LON-SVR1.

▶ Tâche 5 : Vérifier la réplication de la zone intégrée à Active Directory Adatum.com

1. Sur LON-SVR1, ouvrez la console du **Gestionnaire DNS**.
2. Développez **Zones de recherche directes**, puis vérifiez que les zones **Adatum.com** et **_msdcs.Adatum.com** sont répliquées.

   Si vous ne voyez pas ces zones, ouvrez Sites et services Active Directory, forcez la réplication entre **LON-DC1** et **LON-SVR1**, puis réessayez.

▶ Tâche 6 : Utiliser Nslookup pour tester une résolution non locale

1. Sur LON-SVR1, sur la carte réseau **Connexion au réseau local**, dans le champ **Serveur DNS préféré**, supprimez l'adresse IP **172.16.0.10**.
2. Faites de l'adresse **127.0.0.1** le **serveur DNS préféré** de **LON-SVR1**.
3. Ouvrez une fenêtre Windows PowerShell sur **LON-SVR1**, puis essayez de résoudre **www.nwtraders.msft** avec l'applet de commande **Resolve-DNSName**.
4. Vous recevez une réponse négative (cela est prévu).

▶ Tâche 7 : Configurer la résolution de noms Internet pour effectuer une redirection vers le siège

1. Sur LON-SVR1, ouvrez la console du **Gestionnaire DNS**.
2. Configurez un redirecteur afin que **LON-SVR1** corresponde à l'adresse **172.16.0.10**.
3. Redémarrez le service Serveur DNS sur LON-SVR1.

▶ Tâche 8 : Utiliser Nslookup pour confirmer la résolution de noms

- Sur LON-SVR1, dans une fenêtre d'invite de commandes, démarrez l'outil **nslookup**, puis essayez de résoudre **www.nwraders.msft**. Vous devez obtenir une réponse et une adresse IP.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré DNS sur LON-SVR1.

Exercice 2 : Création d'enregistrements d'hôtes dans DNS

Scénario

Plusieurs nouvelles applications Web sont implémentées au siège de la société A. Datum. Chaque application requiert que vous configuriez un enregistrement d'hôte dans DNS. Vous avez été invité à créer les enregistrements d'hôtes de ces applications.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un client pour utiliser LON-SVR1 en tant que serveur DNS
2. Créer plusieurs enregistrements d'hôtes dans le domaine Adatum.com pour des applications Web
3. Vérifier la réplication des nouveaux enregistrements sur LON-SVR1
4. Utilisez la commande ping pour localiser de nouveaux enregistrements de LON-CL1

▶ Tâche 1 : Configurer un client pour utiliser LON-SVR1 en tant que serveur DNS

1. Connectez-vous à LON-CL1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Panneau de configuration**.
3. Ouvrez la boîte de dialogue Propriétés pour la carte **Connexion au réseau local**.
4. Configurez le **serveur DNS préféré** afin qu'il corresponde à l'adresse **172.16.0.21**.

▶ Tâche 2 : Créer plusieurs enregistrements d'hôtes dans le domaine Adatum.com pour des applications Web

1. Sur LON-DC1, ouvrez le **Gestionnaire DNS**.
2. Accédez à la zone de recherche directe **Adatum.com**.
3. Créez un enregistrement nommé **www** avec l'adresse IP **172.16.0.200**.
4. Créez un enregistrement nommé **ftp** avec l'adresse IP **172.16.0.201**.

▶ Tâche 3 : Vérifier la réplication des nouveaux enregistrements sur LON-SVR1

1. Sur LON-SVR1, ouvrez le **Gestionnaire DNS**.
2. Accédez à la zone de recherche directe **Adatum.com**.
3. Assurez-vous que les enregistrements **www** et **ftp** s'affichent. (Vous devrez peut-être actualiser la zone Adatum.com et patienter quelques minutes avant que ces enregistrements n'apparaissent sur LON-SVR1.)

▶ Tâche 4 : Utilisez la commande ping pour localiser de nouveaux enregistrements de LON-CL1

1. Sur LON-CL1, ouvrez une fenêtre d'invite de commandes.
2. Effectuez un test ping de **www.adatum.com**. Assurez-vous que ce test ping résout ce nom en **172.16.0.100**.
3. Effectuez un test ping de **ftp.adatum.com**. Assurez-vous que ce test ping résout ce nom en **172.16.0.200**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré les enregistrements DNS.

Exercice 3 : Gestion du cache d'un serveur DNS

Scénario

Après avoir changé quelques enregistrements d'hôtes dans les zones configurées sur LON-DC1, vous avez remarqué que les clients qui utilisent LON-SVR1 comme serveur DNS continuent à recevoir d'anciennes adresses IP pendant le processus de résolution de noms. Vous voulez identifier le composant qui met en cache ces données.

Les tâches principales de cet exercice sont les suivantes :

1. Utiliser la commande ping pour localiser un enregistrement Internet de LON-CL1
2. Mettre à jour un enregistrement Internet pour pointer vers l'adresse IP de LON-DC1
3. Examiner le contenu du cache DNS
4. Vider le cache et réessayer la commande ping

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MT UNIQUEMENT

▶ Tâche 1 : Utiliser la commande ping pour localiser un enregistrement Internet de LON-CL1

1. Sur LON-CL1, dans la fenêtre d'invite de commandes, utilisez la commande **ping** pour localiser **www.nwtraders.msft**.
2. Assurez-vous que le nom est résolu en une adresse IP, puis documentez l'adresse IP.

▶ Tâche 2 : Mettre à jour un enregistrement Internet pour pointer vers l'adresse IP de LON-DC1

1. Sur LON-DC1, ouvrez la console du **Gestionnaire DNS**.
2. Accédez à la zone de recherche directe **nwtraders.msft**.
3. Remplacez l'adresse IP de l'enregistrement **www** par **172.16.0.10**.
4. À partir de **LON-CL1**, effectuez un test ping de **www.nwtraders.msft**.
5. Notez que cet enregistrement continue d'être résolu avec l'ancienne adresse IP.

▶ Tâche 3 : Examiner le contenu du cache DNS

1. Sur LON-SVR1, dans la console du Gestionnaire DNS, activez **Affichage détaillé**.
2. Parcourez le contenu du conteneur **Recherches mises en cache** pour l'espace de noms msft.
3. Sur LON-CL1, à l'invite de commandes, tapez **ipconfig /displaydns**.
4. Examinez le contenu mis en cache.

▶ Tâche 4 : Vider le cache et réessayer la commande ping

1. Videz le cache sur le serveur DNS LON-SVR1, à l'aide de l'applet de commande **Clear-DNSServerCache**.
2. Réessayez d'effectuer le test ping de **www.nwtraders.msft** sur **LON-CL1** (Le résultat retourne toujours l'ancienne adresse IP.)
3. Videz le cache de résolution du client sur LON-CL1 en tapant **ipconfig /flushdns** dans une fenêtre d'invite de commandes.
4. Sur **LON-CL1**, réessayez d'effectuer le test ping de **www.nwtraders.msft**. (Le résultat devrait être bon.)

Résultats : À la fin de cet exercice, vous aurez examiné le cache du serveur DNS.

▶ 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 **22410B-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 **22410B-LON-SVR1** et **22410B-LON-CL1**.

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Vous résolvez des problèmes liés à la résolution de noms DNS à partir d'un ordinateur client. Que devez-vous penser à faire avant chaque test ?

Question : Vous déployez des serveurs DNS dans un domaine Active Directory et votre client a besoin que l'infrastructure résiste aux points uniques de défaillance. Que devez-vous prendre en compte lors de la planification de la configuration DNS ?

Question : Quels sont les avantages liés à l'utilisation de redirecteurs ?

Outils

Nom de l'outil	Utilisé pour	Emplacement
Console du Gestionnaire DNS	Gérer le rôle serveur DNS	Outils d'administration
Nslookup	Dépanner le système DNS	Outil en ligne de commande
Ipconfig	Dépanner le système DNS	Outil en ligne de commande
Applets de commande Windows PowerShell	Gérer et dépanner le système DNS	Windows PowerShell

Méthode conseillée

Lors de l'implémentation de DNS, utilisez les meilleures pratiques suivantes :

- Utilisez toujours des noms d'hôtes à la place des noms NetBIOS.
- Utilisez des redirecteurs à la place des indications de racine.
- Soyez vigilant face aux problèmes potentiels de mise en cache lors de la résolution de problèmes liés à la résolution de noms.
- Utilisez les zones intégrées à Active Directory au lieu des zones principale et secondaire.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les clients mettent parfois en cache des enregistrements DNS non valides.	
Le serveur DNS s'exécute lentement.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8

Implémentation d'IPv6

Table des matières :

Vue d'ensemble du module	**8-1**
Leçon 1 : Vue d'ensemble du protocole IPv6	**8-2**
Leçon 2 : Adressage IPv6	**8-8**
Leçon 3 : Cohabitation avec le protocole IPv4	**8-15**
Leçon 4 : Technologies de transition IPv6	**8-20**
Atelier pratique : Implémentation d'IPv6	**8-26**
Contrôle des acquis et éléments à retenir	**8-31**

Vue d'ensemble du module

IPv6 est une technologie qui permet à Internet de prendre en charge d'un nombre croissant d'utilisateurs et d'une quantité accrue de périphériques IP. IPv4 a été le protocole Internet sous-jacent pendant près de trois décennies. Sa robustesse, son extensibilité et ses fonctionnalités limitées sont désormais mises à mal face au besoin croissant de nouvelles adresses IP. Ceci est en grande partie dû à l'émergence rapide de nouveaux périphériques réseau.

Objectifs

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

- décrire les fonctionnalités et les avantages du protocole IPv6 ;
- décrire l'adressage IPv6 ;
- décrire la cohabitation d'IPv6 avec IPv4 ;
- décrire les technologies de transition d'IPv6.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble du protocole IPv6

IPv6 a été inclus avec les serveurs et systèmes d'exploitation clients Windows® en commençant par Windows Server® 2008 et Windows Vista®. L'utilisation d'IPv6 devient de plus en plus répandue sur des réseaux d'entreprise et certaines parties d'Internet.

Il est primordial que vous compreniez comment cette technologie affecte les réseaux actuels et comment intégrer IPv6 à ces derniers. Cette leçon présente les avantages d'IPv6 et explique en quoi ce protocole diffère d'IPv4.

Objectifs de la leçon

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

- décrire les avantages d'IPv6 ;
- décrire les principales différences entre IPv4 et IPv6 ;
- décrire le format d'adresse IPv6.

Avantages du protocole IPv6

La prise en charge d'IPv6 est comprise dans Windows Server 2012 et Windows 8. La liste suivante d'avantages explique pourquoi IPv6 est implémenté.

Les avantages du protocole IPv6 incluent les éléments suivants
- Espace d'adressage plus étendu
- Infrastructure d'adressage et de routage hiérarchique
- Configuration d'adresse sans état et avec état
- Prise en charge obligatoire d'IPsec
- Communication de bout en bout
- Prise en charge obligatoire de la qualité de service (QoS)
- Prise en charge améliorée des environnements de sous-réseau unique
- Extensibilité

Espace d'adressage plus étendu

L'espace d'adressage IPv6 est de 128 bits, ce qui est beaucoup plus long grand que l'espace d'adressage de 32 bits d'IPv4. Un espace d'adressage de 32 bits a 2^{32} ou 4 294 967 296 adresses possibles ; un espace d'adressage de 128 bits a 2^{128} ou 340 282 366 920 938 463 463 374 607 431 768 211 456 (ou $3,4x10^{38}$ ou 340 undécillions) adresses possibles. À mesure qu'Internet continue à se développer, IPv6 prévoit l'espace d'adressage plus grand qui est requis.

Infrastructure d'adressage et de routage hiérarchique

L'espace d'adressage IPv6 public est alloué plus efficacement que pour IPv4. Les adresses IPv4 ne sont pas toutes allouées par blocs géographiques, mais les adresses IPv6 publiques le sont. Ceci signifie que quoiqu'il y ait beaucoup plus d'adresses, les routeurs Internet peuvent traiter les données beaucoup plus efficacement en raison de l'optimisation des adresses.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration d'adresse sans état et avec état

IPv6 dispose d'une fonctionnalité de configuration automatique sans protocole DHCP (Dynamic Host Configuration Protocol) et peut détecter des informations sur les routeurs afin de permettre aux hôtes d'accéder à Internet. Cette fonctionnalité est appelée configuration d'adresse *sans état*. Lorsque le protocole DHCPv6 est utilisé, il est question, à l'inverse, d'une configuration d'adresse *avec état*. Cela offre aux administrateurs réseau une meilleure flexibilité dans la façon dont les données de configuration et les adresses IPv6 sont distribuées aux clients.

Prise en charge obligatoire d'IPsec.

Les normes IPv6 requièrent la prise en charge de l'en-tête d'authentification (AH) et des en-têtes ESP (Encapsulating Security Payload) qui sont définis par la sécurité du protocole Internet (IPSec). Bien que la prise en charge des méthodes d'authentification et des algorithmes de chiffrement IPsec spécifiques ne soit pas spécifiée, IPsec est défini dès le début comme manière de protéger les paquets IPv6. Ceci garantit la disponibilité d'IPsec sur tous les hôtes IPv6. La prise en charge d'IPsec n'était pas requise pour les hôtes IPv4, mais elle était généralement implémentée.

Communication de bout en bout

Un des objectifs de conception d'IPv6 est de fournir un espace d'adressage suffisant, de sorte que vous ne deviez pas utiliser de mécanismes de traduction, tels que la traduction d'adresses réseau (NAT). Ceci simplifie la communication, car les hôtes IPv6 peuvent communiquer directement entre eux via Internet. Ceci simplifie également la prise en charge d'applications telles que la vidéoconférence et d'autres applications peer to peer. Cependant, beaucoup d'organisations peuvent choisir de continuer à utiliser des mécanismes de traduction par mesure de sécurité.

Prise en charge obligatoire de la qualité de service (QoS)

Un paquet IPv6 contient un champ Qualité de service (QoS) qui spécifie le délai de traitement du paquet. Ceci permet d'attribuer une priorité au trafic des paquets IPv6. Par exemple, lorsque vous diffusez en continu du trafic vidéo, il est primordial que les paquets arrivent dans le temps imparti. Vous pouvez définir ce champ QoS de façon à vous assurer que les périphériques réseau reconnaissent que la remise des paquets doit être effectuée en un certain temps. La prise en charge de la qualité de service était facultative pour les hôtes IPv4.

Prise en charge améliorée des environnements de sous-réseau unique

Tous les hôtes IPv6 sont configurés automatiquement avec une adresse de liaison locale qui permet à l'hôte pour communiquer sur le sous-réseau local. Cependant, comme pour l'adressage IP privé automatique (APIPA), qui était implémenté de manière facultative dans les environnements IPv4, les ordinateurs ne sont pas configurés automatiquement avec un serveur DNS (Domain Name System) ou une passerelle par défaut.

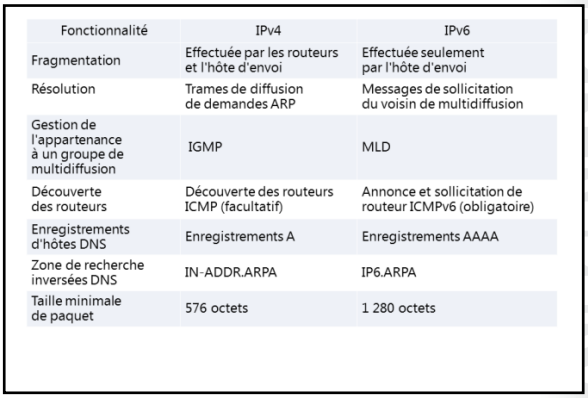
Extensibilité

IPv6 a été conçu pour que les développeurs puissent l'étendre avec beaucoup moins de contraintes que le protocole IPv4. En tant qu'administrateur réseau, vous n'étendrez pas IPv6, mais les applications que vous achetez peuvent tirer profit de ceci pour améliorer les fonctionnalités d'IPv6.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Différences entre les protocoles IPv4 et IPv6

Lorsque fut créé l'espace d'adressage IPv4, il était difficile d'imaginer qu'il pourrait s'épuiser un jour. Toutefois, en raison des avancées technologiques et d'une méthode d'allocation qui n'avait pas prévu le développement des hôtes Internet, la nécessité d'un protocole de remplacement apparut évidente dès 1992.



Fonctionnalité	IPv4	IPv6
Fragmentation	Effectuée par les routeurs et l'hôte d'envoi	Effectuée seulement par l'hôte d'envoi
Résolution	Trames de diffusion de demandes ARP	Messages de sollicitation du voisin de multidiffusion
Gestion de l'appartenance à un groupe de multidiffusion	IGMP	MLD
Découverte des routeurs	Découverte des routeurs ICMP (facultatif)	Annonce et sollicitation de routeur ICMPv6 (obligatoire)
Enregistrements d'hôtes DNS	Enregistrements A	Enregistrements AAAA
Zone de recherche inversées DNS	IN-ADDR.ARPA	IP6.ARPA
Taille minimale de paquet	576 octets	1 280 octets

Quand l'espace d'adressage IPv6 a été conçu, les adresses sont passées à une longueur de 128 bits, de telle sorte que l'espace d'adressage puisse être subdivisé en domaines de routage hiérarchique qui reflètent la topologie d'Internet d'aujourd'hui. Avec 128 bits, il y a assez de bits pour créer plusieurs niveaux de hiérarchie, et il y a suffisamment de flexibilité pour concevoir le routage et l'adressage hiérarchiques. Le Protocole Internet IPv4 est actuellement dépourvu de ces fonctionnalités.

Comparaison entre IPv4 et IPv6

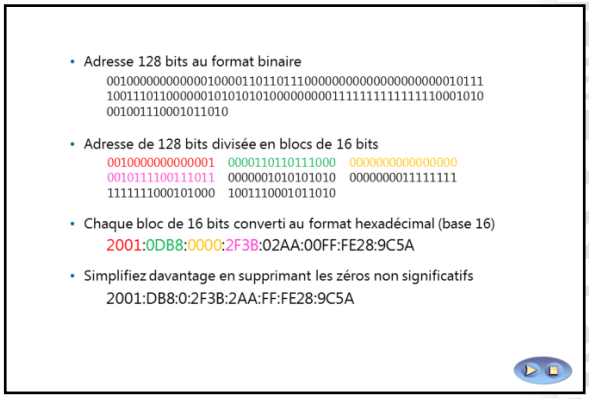
Le tableau suivant souligne des différences supplémentaires existant entre les protocoles IPv4 et IPv6.

IPv4	IPv6
La fragmentation est effectuée par les routeurs et l'hôte d'envoi.	La fragmentation n'est pas réalisée par les routeurs, mais uniquement par l'hôte d'envoi.
Le protocole ARP (Address Resolution Protocol) utilise des trames de diffusion de demandes ARP pour résoudre une adresse IPv4 en une adresse de couche de liaison.	Les trames de demandes ARP sont remplacées par des messages de sollicitation du voisin de multidiffusion.
Le protocole IGMP (Internet Group Management Protocol) gère l'appartenance aux groupes de sous-réseaux locaux.	Le protocole IGMP est remplacé par des messages de découverte d'écouteurs multidiffusion (MLD, Multicast Listener Discovery).
La fonctionnalité facultative de découverte des routeurs ICMP (Internet Control Message Protocol) détermine l'adresse IPv4 de la meilleure passerelle par défaut.	La découverte de routeurs ICMP est remplacée par des messages d'annonce et de sollicitation de routeur ICMP version 6 (v6), qui sont obligatoires.
Utilise des enregistrements de ressources de l'hôte (A) dans le DNS pour mapper des noms d'hôtes aux adresses IPv4.	Utilise des enregistrements de ressources de l'hôte IPv6 (AAAA) dans le DNS pour mapper des noms d'hôtes aux adresses IPv6.
Utilise des enregistrements de ressources du pointeur (PTR) dans le domaine DNS IN-ADDR.ARPA pour mapper des adresses IPv4 aux noms d'hôtes.	Utilise des enregistrements de ressources du pointeur (PTR) dans le domaine DNS IP6.ARPA pour mapper des adresses IPv6 aux noms d'hôtes.
Doit prendre en charge une taille de paquet s'élevant à 576 octets (fragmentation possible).	Doit prendre en charge une taille de paquet s'élevant à 1 280 octets (sans fragmentation).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Format d'adresse IPv6



La fonctionnalité la plus distinctive du protocole IPv6 est sa capacité à utiliser des adresses de taille beaucoup plus importante. Les adresses IPv4 sont exprimées en quatre groupes de nombres décimaux (par exemple, 192.168.1.1). Chaque groupe de nombres représente un octet binaire. En code binaire, 192.168.1.1 se présente comme suit :

11000000.10101000.00000001.00000001
(4 octets = 32 bits)

Toutefois, une adresse IPv6 est quatre fois plus longue qu'une adresse IPv4. Pour cette raison, les adresses IPv6 sont exprimées en code hexadécimal (hexa). Par exemple :

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

Cela peut paraître complexe pour les utilisateurs finaux, mais il faut partir du principe que les utilisateurs auront recours aux noms DNS pour la résolution des hôtes et taperont rarement des adresses IPv6 manuellement. Il est également plus facile d'effectuer la conversion de l'adresse IPv6 hexadécimale entre binaire et hexadécimal que d'effectuer la conversion entre binaire et décimal. Ceci qui simplifie l'utilisation des sous-réseaux et le calcul des hôtes et des réseaux.

Système de numérotation hexadécimal (base 16)

Dans le système de numérotation hexadécimal, certaines lettres représentent des nombres ; ceci est dû au fait que chaque position doit contenir 16 symboles uniques. Du fait que 10 symboles (0 à 9) existent déjà, il doit y avoir six nouveaux symboles pour le système hexadécimal, d'où l'utilisation des lettres A à F. Le nombre hexadécimal 10 est égal au nombre décimal 16.

Remarque : Vous pouvez utiliser l'application de calculatrice fournie avec Windows Server 2012 pour effectuer des conversions entre les nombres binaires, décimaux et hexadécimaux.

Pour convertir une adresse binaire IPv6 d'une longueur de 128 bits, séparez-la en huit blocs de 16 bits. Convertissez ensuite chacun de ces huit blocs de 16 bits en quatre caractères hexadécimaux. Pour chacun des blocs, vous évaluez quatre bits à la fois. Si possible, numérotez chaque section de quatre nombres binaires 1, 2, 4 et 8, en partant de la droite vers la gauche. C'est-à-dire :

- Le premier bit [001**0**] se voit attribuer une valeur de 1.
- Le deuxième bit [00**1**0] se voit attribuer une valeur de 2.
- Le troisième bit [0**0**10] se voit attribuer une valeur de 4.
- Le quatrième bit [**0**010] se voit attribuer une valeur de 8.

Pour calculer la valeur hexadécimale de cette section de quatre bits, ajoutez la valeur de chaque bit défini à 1. Dans l'exemple de 0010, le seul bit défini à 1 est le bit qui se voit attribuer une valeur de 2. Les autres sont définis à zéro. Par conséquent, la valeur hexadécimale de cette section de quatre bits est 2.

Conversion du format binaire à l'hexadécimal

Le tableau suivant décrit la conversion de 8 bits binaires au format hexadécimal pour le nombre binaire [0010] [1111] :

Binaire	0010	1111
Valeurs de chaque position binaire	8421	8421
Ajout de valeurs où le bit est 1	0+0+2+0=2	8+4+2+1=15 ou F hexadécimal

L'exemple ci-après présente une adresse IPv6 unique au format binaire. Notez que la représentation binaire de l'adresse IP est très longue. Les deux lignes de nombres binaires ci-dessous représentent une seule adresse IP :

0010000000000001000011011011100000000000000000000010111100111011
0000001010101010000000001111111111111111000101000100111000101101O

L'adresse de 128 bits est à présent divisée en limites de 16 bits (huit blocs de 16 bits) :

0010000000000001 0000110110111000 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Chaque bloc est lui-même divisé en sections de quatre bits. Le tableau ci-dessous affiche les valeurs binaires de chaque section de quatre bits, ainsi que leurs valeurs hexadécimales correspondantes :

Binaire	Hexadécimal
[0010][0000][0000][0001]	[2][0][0][1]
[0000][1101][1011][1000]	[0][D][B][8]
[0000][0000][0000][0000]	[0][0][0][0]
[0010][1111][0011][1011]	[2][F][3][B]
[0000][0010][1010][1010]	[0][2][A][A]
[0000][0000][1111][1111]	[0][0][F][F]
[1111][1110][0010][1000]	[F][E][2][8]
[1001][1100][0101][1010]	[9][C][5][A]

Chaque bloc de 16 bits est exprimé sous la forme de quatre caractères hexadécimaux, puis séparé par des deux-points. Le résultat obtenu est le suivant :

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

Vous pouvez simplifier davantage la représentation IPv6 en supprimant les zéros non significatifs dans chaque bloc de 16 bits. Toutefois, chaque bloc doit comporter au moins un chiffre. Avec la suppression des zéros non significatifs, la représentation de l'adresse devient la suivante :

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Compression des zéros

Quand plusieurs blocs de zéros contigus se produisent, vous pouvez les compresser et les représenter dans l'adresse sous la forme de double-deux-points (::) ; ceci simplifie encore la notation IPV6. L'ordinateur reconnaît le symbole « :: » et le remplace par le nombre de blocs nécessaire pour former l'adresse IPv6 appropriée.

Dans l'exemple suivant, l'adresse est exprimée en utilisant la compression des zéros :

2001:DB8::2F3B:2AA:FF:FE28:9C5A

Pour déterminer combien de bits 0 sont représentés par le symbole « :: », vous pouvez comptabiliser le nombre de blocs dans l'adresse compressée, soustraire ce nombre du chiffre huit, puis multiplier le résultat par 16. Si nous prenons l'exemple précédent, il y a sept blocs. Soustrayez sept de huit et multipliez le résultat (un) par 16. Il y a donc 16 bits ou 16 zéros dans l'adresse contenant le symbole « double deux-points ».

Vous pouvez ne pouvez utiliser qu'une seule fois la compression des zéros dans une adresse spécifique. Si vous l'utilisez deux fois ou plus, alors il n'y a aucune façon de montrer combien de bits 0 sont représentés par chaque instance du symbole double-deux-points (::).

Pour convertir une adresse au format binaire, appliquez de manière inverse la méthode décrite précédemment :

1. Ajoutez des zéros au moyen de la compression des zéros.
2. Ajoutez des zéros non significatifs.
3. Convertissez chaque nombre 1 au format binaire équivalent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Adressage IPv6

Comprendre les différents types d'adresse et lorsqu'ils sont utilisés constitue un aspect essentiel du protocole IPv6. Ceci vous permet de comprendre le processus de communication global entre les hôtes IPv6 et d'effectuer le dépannage. Vous devez également comprendre les processus disponibles pour configurer un hôte avec une adresse IPv6 afin de vérifier que les hôtes sont configurés correctement.

Objectifs de la leçon

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

- décrire la structure des adresses IPv6 ;
- décrire la structure des adresses monodiffusion globales ;
- décrire les adresses monodiffusion uniques locales ;
- décrire les adresses monodiffusion de liaison locale et les ID de zone.
- décrire la configuration automatique des adresses pour le protocole IPv6 ;
- expliquer comment configurer les paramètres clients IPv6 sur un hôte du réseau.

Structure de l'adresse IPv6

Chaque adresse IPv6 a une longueur de 128 bits. Le préfixe est la partie de l'adresse qui indique les bits qui possèdent des valeurs fixes ou qui appartiennent au préfixe de sous-réseau. C'est l'équivalent de l'ID réseau pour une adresse IPv4.

Les préfixes des sous-réseaux, des itinéraires et des plages d'adresses IPv6 sont exprimés de la même manière que les notations CIDR (Classless Inter-Domain Routing) pour le protocole IPv4. Un préfixe IPv6 respecte la notation adresse/longueur de préfixe. Par exemple, 2001:DB8::/48 et 2001:DB8:0:2F3B::/64 sont des préfixes d'adresse IPv6.

- Le nombre de bits réseau est défini par le préfixe
- Chaque hôte a 64 bits alloués à l'identificateur d'interface

Type d'adresse	Adresse IPv4	Adresse IPv6
Non spécifié	0.0.0.0	::
Bouclage	127.0.0.1	::1
Configuré automatiquement	169.254.0.0/16	FE80::/64
Diffusion	255.255.255.255	Utilise des multidiffusions à la place
Multidiffusion	FF00::/8	FF00::/8

Remarque : IPv6 utilise des préfixes au lieu d'un masque de sous-réseau.

Quand une adresse IPv6 monodiffusion est attribuée à un hôte, le préfixe est de 64 bits. Les 64 bits restants sont alloués à l'identificateur d'interface, qui identifie de façon unique l'hôte sur ce réseau. L'identificateur d'interface peut être généré aléatoirement, attribué par DHCPv6 ou être basé sur l'adresse MAC (Media Access Control) du réseau. Par défaut, les bits d'hôte sont générés aléatoirement à moins qu'ils soient attribués par DHCPv6.

Remarque : Les routes sur un routeur IPv6 ont des tailles de préfixe variables déterminées par la taille du réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

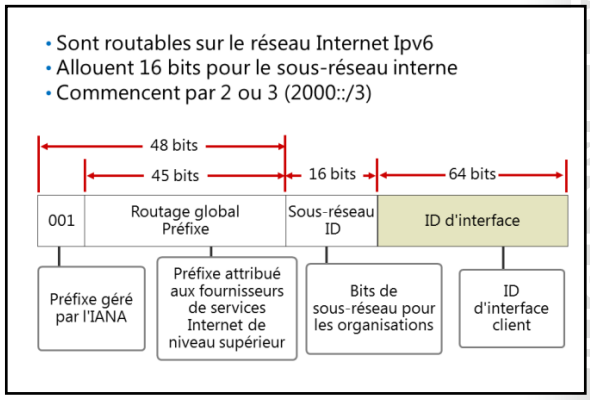
Équivalents IPv6 aux adresses spéciales IPv4

Le tableau suivant montre les équivalents dans le protocole IPv6 à quelques adresses IPv4 courantes.

	Adresse IPv4	Adresse IPv6
Adresse non spécifiée	0.0.0.0	::
Adresse de bouclage	127.0.0.1	::1
Adresses configurées automatiquement	169.254.0.0/16	FE80::/64
Adresse de diffusion	255.255.255.255	Utilise des multidiffusions à la place
Adresses de multidiffusion	224.0.0.0/4	FF00::/8

Adresses monodiffusion globales

Les adresses monodiffusion globales équivalent aux adresses IPv4 publiques qui sont fournies par un fournisseur de services Internet (ISP). Elles peuvent faire l'objet d'un routage et sont accessibles globalement sur la partie IPv6 d'Internet. À la différence du nombre limité d'adresses IPv4 adressables depuis Internet qui demeurent, il y a beaucoup d'adresses monodiffusion globales disponibles.



L'espace d'adresses monodiffusion globales est conçu pour permettre à chaque client du fournisseur de services Internet d'obtenir un grand nombre d'adresses d'IPv6. Les 48 premiers bits sont utilisés pour identifier le site client. Les 16 bits suivants sont alloués pour que le client effectue un sous-réseautage dans son propre réseau.

Remarque : Le réseau 2001:0db8::/32 est réservé à la documentation et n'est pas routable.

La structure d'une adresse monodiffusion globale est la suivante :

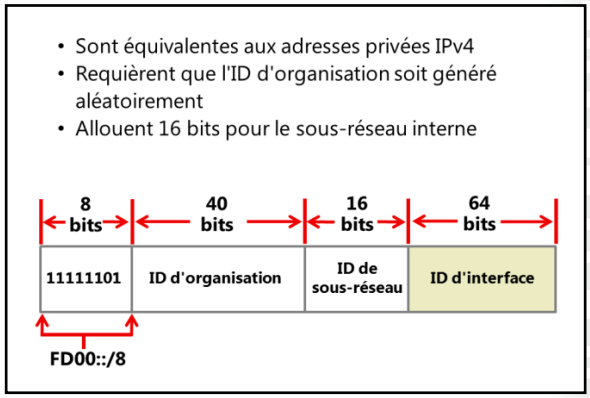
- Partie fixe définie à 001. Les trois bits d'ordre haut sont définis à 001. Le préfixe d'adresse pour les adresses globales actuellement attribuées est 2000::/3. Par conséquent, toutes les adresses monodiffusion globales commencent par 2 ou 3.
- Préfixe de routage global. Ce champ indique le préfixe de routage global pour le site d'une organisation spécifique. La combinaison des trois bits fixes et du préfixe de routage global de 45 bits est utilisée pour créer un préfixe de site de 48 bits attribué au site indépendant d'une organisation. Au moment de l'attribution, les routeurs sur Internet IPv6 acheminent alors le trafic IPv6 qui fait correspondre le préfixe de 48 bits aux routeurs du site de l'organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- ID de sous-réseau. L'ID de sous-réseau est utilisé sur le site d'une organisation pour identifier des sous-réseaux. La taille de ce champ est de 16 bits. Le site de l'organisation peut exploiter ces 16 bits sur son site pour créer 65 536 sous-réseaux, ou plusieurs niveaux dans une hiérarchie d'adressage, ainsi qu'une infrastructure de routage efficace.
- ID d'interface. L'ID d'interface identifie l'interface dans un sous-réseau spécifique sur le site. La taille de ce champ est de 64 bits. Ceci est aléatoirement généré ou attribué par DHCPv6. Auparavant, l'ID d'interface était basé sur l'adresse MAC de la carte d'interface réseau à laquelle l'adresse a été liée.

Adresses de monodiffusion uniques locales

Les adresses locales uniques sont l'équivalent dans le protocole IPv6 des adresses privées IPv4. Ces adresses sont routables dans une organisation, mais pas sur Internet.



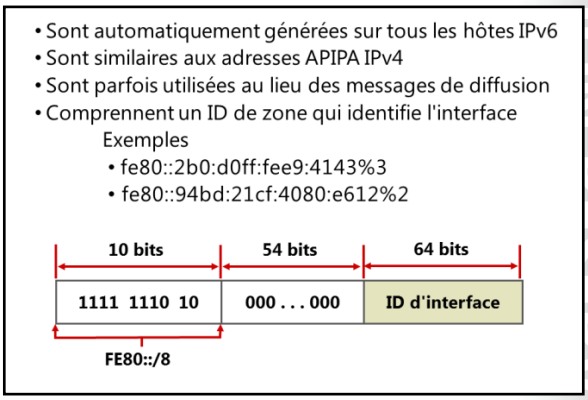
Les adresses IP privées IPv4 représentaient une partie relativement petite de l'espace d'adressage IPv4 global, et beaucoup de sociétés utilisaient le même espace d'adressage. Ceci provoquait des problèmes lorsque des organisations distinctes tentaient de communiquer directement. Cela entraînait également des problèmes lors de la fusion des réseaux de deux organisations, éventuellement suite à une fusion ou un rachat.

Pour éviter les problèmes de duplication rencontrés avec les adresses IPv4 privées, la structure d'adresse locale unique du protocole IPv6 alloue 40 bits à l'identificateur d'une organisation. Cet identificateur d'organisation de 40 bits est aléatoirement généré. La probabilité que deux identificateurs de 40 bits aléatoirement générés soient identiques est très faible. Ceci permet de garantir que chaque organisation a un espace d'adressage unique.

Les sept premiers bits de l'identificateur d'organisation ont la valeur binaire fixe de 1111101. Toutes les adresses locales uniques ont le préfixe d'adresse FC00::/7. L'indicateur local (L) est défini à 1 pour indiquer une adresse locale. Une valeur d'indicateur L définie à 0 n'a pas encore été définie. Par conséquent, les adresses locales uniques avec l'indicateur L défini à 1 ont le préfixe d'adresse FD::/8.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Adresses monodiffusion de liaison locale



Tous les hôtes IPv6 ont une adresse de liaison locale qui est utilisée pour communiquer seulement sur le sous-réseau local. L'adresse de liaison locale est générée automatiquement et est non routable. En cela, les adresses de liaison locale sont similaires aux adresses APIPA IPv4. Cependant, une adresse de liaison locale est une partie essentielle de la communication IPv6.

Des adresses de liaison locale sont utilisées pour la communication dans de nombreux scénarios où IPv4 aurait utilisé des diffusions. Par exemple, des adresses de liaison locale sont utilisées lors de la communication avec un serveur DHCPv6. Les adresses de liaison locale sont également utilisées pour la découverte de voisins, qui est l'équivalent dans le protocole IPv6 de l'ARP dans IPv4.

Le préfixe des adresses de liaison locale est toujours FE80::/64. Les 64 derniers bits sont l'identificateur d'interface.

ID de zone

Quel que soit le nombre d'interfaces réseau dans l'hôte, chaque hôte IPv6 a une adresse de liaison locale unique. Si l'hôte a plusieurs interfaces réseau, la même adresse de liaison locale est réutilisée sur chaque interface réseau. Pour permettre à des hôtes pour identifier la communication de liaison locale sur chaque interface réseau unique, un ID de zone est ajouté à l'adresse de liaison locale.

Un ID de zone est utilisé au format suivant :

Adresse%ID_zone

Chaque hôte expéditeur détermine l'ID de zone qu'il associera à chaque interface. Il n'y a aucune négociation d'ID de zone entre les hôtes. Par exemple, sur le même réseau, l'hôte A pourrait utiliser 3 pour l'ID de zone sur son interface et l'hôte B pourrait utiliser 6 pour l'ID de zone sur son interface.

Un index d'interface unique, qui est un entier, est attribué à chaque interface dans un hôte Windows. Outre les cartes réseau physiques, les interfaces comprennent également des interfaces de bouclage et de tunnel. Les hôtes IPv6 Windows utilisent l'index d'interface d'une interface comme ID de zone pour cette interface.

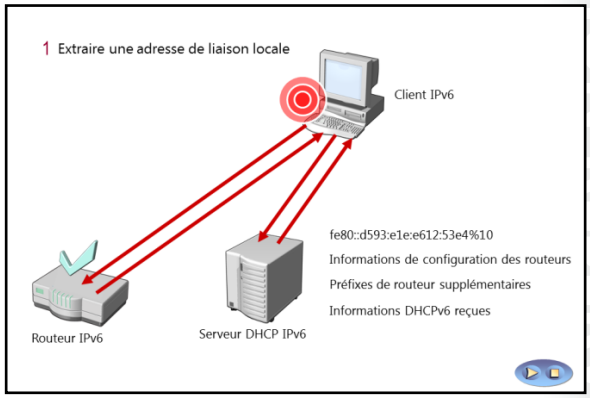
Dans l'exemple suivant, l'ID d'interface pour l'interface réseau est 3.

fe80::2b0:d0ff:fee9:4143%3

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration automatique des adresses IPv6

Dans la plupart des cas, vous utiliserez la configuration automatique pour fournir une adresse IPv6 à des hôtes IPv6. À la différence du protocole IPv4 qui utilise principalement les serveurs DHCP pour fournir des informations d'adressage, IPv6 utilise également les routeurs dans le cadre du processus de configuration automatique. Les routeurs peuvent fournir l'adresse réseau et une passerelle par défaut aux clients dans les messages d'annonce de routeur.



Types de configurations automatiques

Les types de configurations automatiques sont présentés ci-dessous.

- Sans état. Avec la configuration automatique sans état, la configuration d'adresse est uniquement basée sur la réception des messages d'annonce de routeur. La configuration automatique sans état comprend un préfixe de routeur, mais ne comprend pas d'options de configuration supplémentaires, comme des serveurs DNS.
- Avec état. Dans la configuration automatique avec état, la configuration d'adresse se base sur l'utilisation d'un protocole de configuration d'adresse avec état, tel que DHCPv6, pour se procurer des adresses et d'autres options de configuration : Un hôte utilise la configuration d'adresse avec état quand :
  - il reçoit l'instruction de le faire dans des messages d'annonce de routeur ;
  - il n'y a aucun routeur présent sur la liaison locale.
- Les deux types. Avec les deux types, la configuration est basée à la fois sur la réception des messages d'annonce de routeur et sur DHCPv6.

Configuration avec état

Avec la configuration avec état, les organisations peuvent contrôler la manière dont les adresses IPv6 sont affectées au moyen du protocole DHCPv6. S'il existe des options d'étendue spécifiques que vous devez configurer, telles que les adresses IPv6 des serveurs DNS, un serveur DHCPv6 est nécessaire.

Quand le protocole IPv6 tente de communiquer avec un serveur DHCPv6, il utilise des adresses de multidiffusion IPv6. Ce comportement diffère du protocole IPv4 qui utilise des adresses de diffusion IPv4.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

États des adresses configurées automatiquement

Pendant la configuration automatique, l'adresse IPv6 d'un hôte passe par plusieurs états qui définissent le cycle de vie de l'adresse IPv6. Les adresses configurées automatiquement adoptent un ou plusieurs des états suivants :

- Provisoire. Dans l'état provisoire, la vérification a lieu pour déterminer si l'adresse est unique. La détection d'adresses en double se charge de la vérification. Quand une adresse est dans l'état provisoire, un nœud ne peut pas recevoir le trafic de monodiffusion.
- Valide. Dans l'état valide, l'adresse a été vérifiée comme étant unique, et elle peut envoyer et recevoir du trafic de monodiffusion.
- Privilégié. Dans l'état privilégié, l'adresse permet à un nœud d'envoyer et de recevoir des données du trafic de monodiffusion.
- Déconseillé. Dans l'état déconseillé, l'adresse est valide, mais son utilisation est déconseillée pour une nouvelle communication.
- Non valide. Dans l'état non valide, l'adresse ne permet plus à un nœud d'envoyer ou de recevoir le trafic de monodiffusion.

Démonstration : Configuration des paramètres clients IPv6

Dans la plupart des cas, IPv6 est configuré dynamiquement à l'aide de DHCPv6 ou d'annonces de routeur. Cependant, vous pouvez également configurer IPv6 manuellement avec une adresse IPv6 statique. Le processus de configuration d'IPv6 est semblable au processus de configuration d'IPv4.

Dans cette démonstration, vous allez apprendre à :

- afficher la configuration IPv6 à l'aide d'IPconfig ;
- configurer IPv6 sur un contrôleur de domaine et un serveur ;
- vérifier que la communication IPv6 est fonctionnelle.

Procédure de démonstration

Afficher la configuration IPv6 à l'aide d'IPconfig

1. Ouvrez une session sur **LON-DC1** et **LON-SVR1** en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-DC1, ouvrez une invite Windows PowerShell®.
3. Utilisez **ipconfig** pour afficher l'adresse IPv6 de liaison locale sur la connexion au réseau local.
4. Utilisez l'applet de commande **Get-NetIPAddress** pour afficher la configuration réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configurer IPv6 sur LON-DC1

1. Sur LON-DC1, utilisez le Gestionnaire de serveur pour ouvrir la boîte de dialogue **Propriétés du serveur local**, puis cliquez sur **Connexion au réseau local**.
2. Ouvrez la boîte de dialogue **Propriétés IP, version 6 (TCP/IPv6)**, et entrez les informations suivantes :
   - **Utiliser l'adresse IPv6 suivante**
   - Adresse IPv6 : **FD00:AAAA:BBBB:CCCC::A**
   - Longueur du préfixe de sous-réseau : **64**
   - **Utiliser l'adresse de serveur DNS suivante :**
   - Serveur DNS préféré : **::1**

Configurer IPv6 sur LON-SVR1

1. Sur LON-DC1, utilisez le Gestionnaire de serveur pour ouvrir la boîte de dialogue **Propriétés du serveur local**, puis cliquez sur **Connexion au réseau local**.
2. Ouvrez la boîte de dialogue **Propriétés IP, version 6 (TCP/IPv6)**, et entrez les données suivantes :
   - **Utiliser l'adresse IPv6 suivante**
   - Adresse IPv6 : **FD00:AAAA:BBBB:CCCC::15**
   - Longueur du préfixe de sous-réseau : **64**
   - **Utiliser l'adresse de serveur DNS suivante :**
   - Serveur DNS préféré : **FD00:AAAA:BBBB:CCCC::A**

Vérifier que la communication IPv6 est fonctionnelle

1. Sur LON-SVR1, ouvrez une invite Windows PowerShell.
2. Utilisez **ipconfig** pour afficher l'adresse IPv6 pour la connexion au réseau local.
3. Utilisez **ping -6** pour tester la communication IPv6 avec **LON-DC1**.
4. Utilisez **ping -4** pour tester la communication IPv4 avec **LON-DC1**.

Remarque : Laissez tous les ordinateurs virtuels dans leur état actuel pour la démonstration suivante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Cohabitation avec le protocole IPv4

Depuis le début, le protocole IPv6 a été conçu pour la coexistence à long terme avec IPv4 ; dans la plupart des cas, votre réseau utilisera à la fois IPv4 et IPv6 pendant de nombreuses années. En conséquence, vous devez comprendre comment ils coexistent.

Cette leçon propose une vue d'ensemble des technologies qui permettent la cohabitation de ces deux protocoles IP. Cette leçon décrit également les différents types de nœud et les diverses implémentations de pile IP d'IPv6. Enfin, cette leçon explique comment le système DNS résout des noms en adresses IPv6 et les divers types de technologies de transition d'IPv6.

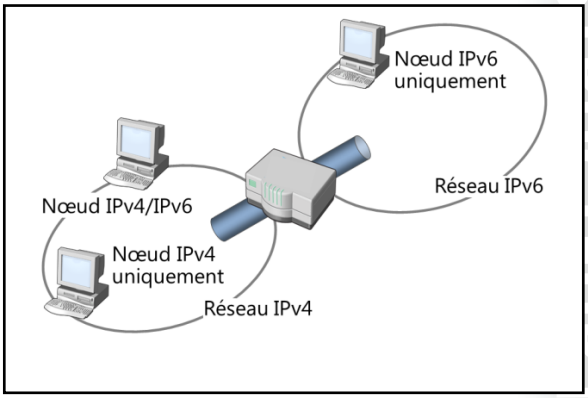
Objectifs de la leçon

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

- décrire les types de nœuds IP ;
- décrire les méthodes qui permettent la cohabitation d'IPv4 et IPv6 ;
- configurer le système DNS pour la prise en charge du protocole IPv6 ;
- expliquer le concept de tunneling IPv6/IPv4.

Quels sont les types de nœuds ?

Lorsque vous planifiez un réseau IPv6, vous devez connaître les types de nœuds ou d'hôtes qui interviennent sur le réseau. Décrire les nœuds d'une manière spécifique permet de définir leurs possibilités sur le réseau. Comprendre les possibilités de chaque type de nœud est important si vous utilisez le tunneling, parce que certaines sortes de tunnels requièrent des types de nœud spécifiques. Voici les descriptions des divers types de nœuds :



- Nœud IPv4 uniquement. C'est un nœud qui implémente uniquement le protocole IPv4 (et dispose seulement d'adresses IPv4) et ne prend pas en charge le protocole IPv6.
- Nœud IPv6 uniquement. C'est un nœud qui implémente uniquement le protocole IPv6 (et dispose seulement d'adresses IPv6) et ne prend pas en charge le protocole IPv4. Ce nœud est capable de communiquer uniquement avec des nœuds et des applications IPv6 et est actuellement peu utilisé. Il risque toutefois de s'imposer davantage puisque les périphériques de plus petite taille (téléphones portables et les ordinateurs de poche, par exemple) utilisent uniquement le protocole IPv6.

- Nœud IPv6/IPv4. C'est un nœud qui implémente à la fois les protocoles IPv4 et IPv6. Windows Server 2008 et les systèmes d'exploitation Windows Server ultérieurs, ainsi que Windows Vista et les systèmes d'exploitation clients ultérieurs utilisent IPv4 et IPv6 par défaut.
- Nœud IPv4. C'est un nœud qui implémente le protocole IPv4. Il peut s'agir d'un nœud IPv4 uniquement ou d'un nœud IPv6/IPv4.
- Nœud IPv6. C'est un nœud qui implémente le protocole IPv6. Il peut s'agir d'un nœud IPv6 uniquement ou d'un nœud IPv6/IPv4.

La cohabitation se produit lorsqu'une majorité de nœuds (nœuds IPv4 ou IPv6) peut communiquer au moyen d'une infrastructure IPv4, d'une infrastructure IPv6 ou d'une infrastructure combinant les protocoles IPv4 et IPv6. Pour accomplir une véritable migration, vous devez convertir tous les nœuds IPv4 en nœuds IPv6 uniquement. Toutefois, dans un avenir prévisible, vous pourrez procéder à une migration effective après avoir converti le plus grand nombre possible de nœuds IPv4 uniquement en nœuds IPv6/IPv4. Les nœuds IPv4 uniquement ne peuvent communiquer avec des nœuds IPv6 uniquement que lorsque vous utilisez un proxy ou une passerelle de traduction IPv4 vers IPv6.

Cohabitation IPv4/IPv6

Plutôt que de remplacer IPv4, la plupart des organisations ajoutent IPv6 à leur réseau IPv4 existant. Depuis Windows Server 2008 et Windows Vista, les systèmes d'exploitation Windows prennent en charge l'utilisation simultanée d'IPv4 et d'IPv6 via une architecture à double couche IP. Les systèmes d'exploitation Windows XP et Windows Server 2003 utilisent une architecture à double pile moins efficace.

Windows Server 2012 utilise une architecture double couche IP qui prend en charge IPv4 et IPv6 dans une pile de protocoles unique

Les enregistrements DNS qui sont requis pour la coexistence sont

- Enregistrements de ressource de l'hôte (a) pour les nœuds IPv4
- Enregistrements de ressource de l'hôte IPv6 (AAAA)
- Enregistrements de ressource de pointeur de recherche inversée (PTR) pour les nœuds IPv4 et IPv6

Architecture à double couche IP

Une architecture à double couche IP a été implémentée à partir de Windows Vista, et jusqu'à Windows Server 2012 et Windows 8. Cette architecture contient des couches Internet IPv4 et IPv6 avec une implémentation unique de protocoles de la couche transport, tels que les protocoles TCP et UDP. La double pile permet une migration plus facile vers IPv6, et il y a moins fichiers à maintenir pour fournir la connectivité d'IPv6. IPv6 est également disponible sans ajout de tous les nouveaux protocoles dans la configuration de carte réseau.

Architecture à double pile

L'architecture à double pile comprend les deux couches Internet IPv4 et IPv6, et a des piles de protocoles séparées qui contiennent des implémentations distinctes de protocoles de la couche transport, tels que les protocoles TCP et UDP. Le pilote de protocole IPv6 Tcpip6.sys disponible dans Windows Server 2003 et Windows XP contient une implémentation distincte des protocoles TCP et UDP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration requise pour l'infrastructure DNS

De la même façon que DNS est utilisé en tant que service de prise en charge sur un réseau IPv4, il est également requis sur un réseau IPv6. Quand vous ajoutez IPv6 au réseau, vous devez vérifier que vous ajoutez les enregistrements qui sont nécessaires pour la prise en charge des résolutions noms/adresses et adresses/noms IPv6. Les enregistrements DNS qui sont requis pour la coexistence sont :

- enregistrements de ressource de l'hôte (a) pour les nœuds IPv4 ;
- enregistrements de ressource de l'hôte IPv6 (AAAA) ;
- enregistrements de ressource de pointeur de recherche inversée (PTR) pour les nœuds IPv4 et IPv6.

Remarque : Dans la plupart des cas, les enregistrements de ressource de l'hôte IPv6 (AAAA) requis par les nœuds IPv6 sont enregistrés dans le DNS dynamiquement.

Quand un nom peut être résolu à la fois en adresse IPv4 et en adresse IPv6, les deux adresses sont retournées au client. Le client choisit alors l'adresse à utiliser en fonction des stratégies de préfixes. Dans ces stratégies de préfixes, un niveau de priorité est attribué à chaque préfixe. Une priorité plus élevée est préférée à une priorité inférieure. Le tableau suivant présente les stratégies générales de préfixes pour Windows Server 2012.

Préfixe	Ordre de priorité	Label	Description
::1/128	50	0	Bouclage IPv6
::/0	40	1	Passerelle par défaut
::ffff:0:0/96	10	4	Adresse compatible IPv4
2002::/16	7	2	6to4
2001::/32	5	5	Teredo
FC00::/7	3	13	Locale unique
::/96	1	3	Adresse compatible IPv4 (abandonné)
fec0::/10	1	11	Locale de site (abandonné)
3ffe::/16	1	12	6Bone (abandonné)

Remarque : Vous pouvez afficher les stratégies de préfixes dans Windows Server 2012 à l'aide de l'applet de commande Windows PowerShell **Get-NetPrefixPolicy**.

Documentation supplémentaire : Pour plus d'informations sur les stratégies de préfixes, consultez la rubrique « Sélection d'adresses source et de destination pour IPv6 » à l'adresse http://go.microsoft.com/fwlink/?LinkId=269711.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration du système DNS pour la prise en charge du protocole IPv6

De même que les nœuds IPv4, les nœuds IPv6 utilisent les enregistrements d'hôtes créés automatiquement sur un DNS dynamique. Vous pouvez également créer manuellement les enregistrements hôte pour les adresses IPv6. Un enregistrement de ressource hôte IPv6 (AAAA) est un type d'enregistrement unique et est différent d'un enregistrement de ressource hôte IPv4 (A).

Dans cette démonstration, vous allez apprendre à :

- configurer un enregistrement de ressource hôte IPv6 (AAAA) pour une adresse IPv6 ;
- vérifier la résolution des noms pour un enregistrement de ressource hôte IPv6 (AAAA).

Procédure de démonstration

Configurer un enregistrement de ressource hôte IPv6 (AAAA)

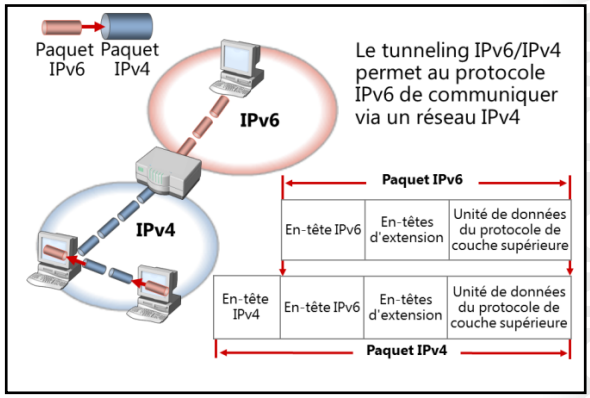
1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez l'outil DNS et accédez à la zone de recherche directe Adatum.com.
2. Dans le Gestionnaire DNS, vérifiez que des adresses IPv6 ont été enregistrées dynamiquement pour LON-DC1 et LON-SVR1.
3. Créez un nouvel enregistrement d'hôte dans Adatum.com en utilisant les paramètres suivants :
   - Nom : **WebApp**
   - Adresse IP : **FD00:AAAA:BBBB:CCCC::A**

Vérifier la résolution des noms pour un enregistrement de ressource hôte IPv6 (AAAA)

1. Sur LON-SVR1, si nécessaire, ouvrez une invite Windows PowerShell.
2. Utilisez **ping** pour tester la communication avec **WebApp.adatum.com**.

Qu'est-ce que le tunneling IPv6/IPv4 ?

Le tunneling IPv6/IPv4 désigne le processus qui consiste à encapsuler des paquets IPv6 au moyen d'un en-tête IPv4 dans le but de transmettre ces paquets IPv6 sur une infrastructure IPv4 uniquement. Les caractéristiques à relever dans l'en-tête IPv4 sont les suivantes :



- Le champ **Protocole IPv4** est défini à **41** pour indiquer un paquet IPv6 encapsulé.
- Les champs **Source** et **Destination** sont définis sur les adresses IPv4 des points de terminaison de tunnel. Vous pouvez configurer des points de terminaison de tunnel manuellement dans le cadre de l'interface de tunnel ; ou sinon, ils peuvent être dérivés automatiquement.

Contrairement au tunneling pour les protocoles PPTP (Point-to-Point Tunneling Protocol) et L2TP (Layer Two Tunneling Protocol), il n'y a aucun échange de messages pour la configuration, la maintenance ou l'arrêt des tunnels. Qui plus est, le tunneling IPv6/IPv4 n'offre aucune sécurité pour les paquets IPv6 transmis par tunnel, ce qui signifie que lorsque vous faites appel au tunneling IPv6, ce dernier n'a pas besoin d'établir d'abord une connexion protégée.

Vous pouvez configurer manuellement le tunneling IPv6/IPv4, ou utiliser des technologies automatisées, telles que Teredo, ISATAP ou 6to4, qui implémentent le tunneling IPv6/IPv4.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Technologies de transition IPv6

La transition d'IPv4 à IPv6 requiert la coexistence entre les deux protocoles. Trop d'applications et de services sont basés sur IPv4 pour que ce protocole soit supprimé rapidement. Cependant, il existe plusieurs technologies qui facilitent cette transition en permettant la communication entre les hôtes IPv4-uniquement et IPv6-uniquement. Il existe également des technologies qui permettent la communication IPv6 sur des réseaux IPv4.

Cette leçon fournit des informations sur ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 6to4 et Teredo, qui aident à fournir la connectivité entre les technologies IPv4 et IPv6. Cette leçon traite également de PortProxy, qui rend les applications compatibles.

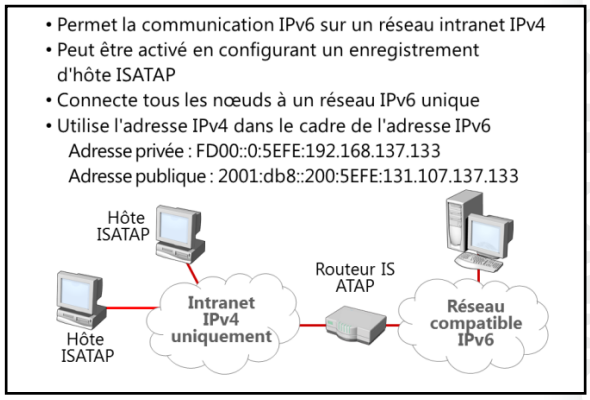
Objectifs de la leçon

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

- décrire ISATAP ;
- décrire 6to4 ;
- décrire Teredo ;
- décrire PortProxy ;
- décrire le processus de transition du protocole IPv4 vers le protocole IPv6.

Qu'est-ce qu'ISATAP ?

ISATAP est une technologie d'affectation d'adresses que vous pouvez utiliser pour assurer la connectivité IPv6 monodiffusion entre des hôtes IPv6/IPv4 sur un intranet IPv4. Les paquets IPv6 sont encapsulés dans des paquets IPv4 afin d'être transmis sur le réseau. La communication peut s'effectuer directement entre deux hôtes ISATAP sur un réseau IPv4, ou peut passer par un routeur ISATAP si un réseau n'a que des hôtes IPv6-uniquement.



Les hôtes ISATAP ne nécessitent aucune configuration manuelle et peuvent créer des adresses ISATAP en utilisant des mécanismes de configuration automatique d'adresses standard. Bien que le composant ISATAP soit activé par défaut, il attribue des adresses ISATAP seulement s'il peut résoudre le nom ISATAP sur votre réseau.

Une adresse ISATAP basée sur une adresse IPv4 privée est mise en forme comme dans l'exemple suivant :

[préfixe monodiffusion 64 bits]:0:5EFE:w.x.y.z

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une adresse ISATAP basée sur une adresse IPv4 publique est mise en forme comme dans l'exemple suivant :

[préfixe monodiffusion 64 bits]:200:5EFE:w.x.y.z

Par exemple, FD00::5EFE:192.168.137.133 est un exemple d'adresse IPv4 privée, et 2001:db8::200:5EFE:131.107.137.133 est un exemple d'adresse IPv4 publique.

Qu'est-ce qu'un routeur ISATAP ?

S'il n'y a aucun hôte IPv6-uniquement, alors le routeur ISATAP publie le préfixe IPv6 qui est utilisé par les clients ISATAP. L'interface ISATAP sur les ordinateurs client est configurée pour utiliser ce préfixe. Quand les applications utilisent l'interface ISATAP pour remettre des données, le paquet IPV6 est encapsulé dans un paquet IPv4 pour être remis à l'adresse IPv4 de l'hôte de destination ISATAP.

S'il y a des hôtes IPv6-uniquement, alors le routeur ISATAP décompacte également les paquets IPv6. Les hôtes ISATAP envoient les paquets à l'adresse IPv4 du routeur ISATAP. Le routeur ISATAP décompacte alors les paquets IPv6 et les envoie sur le réseau IPv6-uniquement.

Comment activer le tunneling ISATAP

Vous pouvez initier le tunneling ISATAP de plusieurs manières, mais la manière la plus simple consiste à configurer un enregistrement d'hôte ISATAP dans le DNS qui le résout en l'adresse IPv4 du routeur ISATAP. Les hôtes Windows qui peuvent résoudre ce nom commencent automatiquement à utiliser le routeur ISATAP spécifié. En utilisant cette méthode, vous pouvez configurer le protocole ISATAP pour plusieurs ordinateurs simultanément.

Vous pouvez également définir la résolution de noms ISATAP dans un fichier Hosts, mais cette méthode n'est pas recommandée, car elle est difficile de gérer.

Remarque : Par défaut, les serveurs DNS sur Windows Server 2008 ou les systèmes d'exploitation Windows Server plus récents ont une liste rouge de requêtes globales qui empêche la résolution ISATAP, même si l'enregistrement d'hôte est créé et correctement configuré. Vous devez supprimer ISATAP de la liste rouge de requêtes globales dans le DNS si vous utilisez un enregistrement d'hôte ISATAP pour configurer des clients ISATAP.

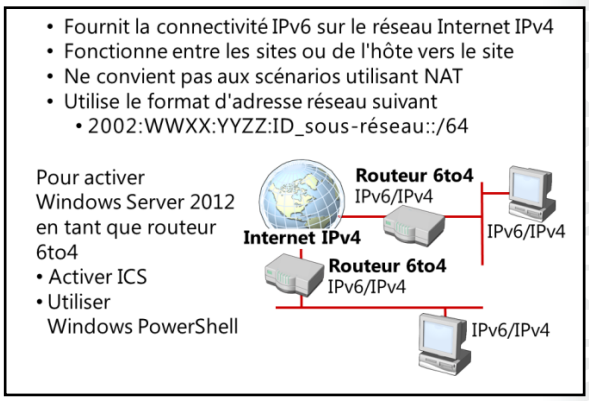
Voici d'autres façons de configurer des hôtes avec un routeur ISATAP :

- utilisez l'applet de commande Windows PowerShell **Set-NetIsatapConfiguration -Router *x.x.x.x*** ;
- utilisez **Netsh Interface IPv6 ISATAP Set Router *x.x.x.x*** ;
- configurez le paramètre de stratégie de groupe **ISATAP *Nom du routeur***.

Remarque : Tous les nœuds ISATAP sont connectés à un sous-réseau IPv6 unique. Ceci signifie que tous les nœuds ISATAP font partie du même site Active Directory® Domain Services (AD DS), ce qui peut ne pas être souhaitable.

Vous devriez donc utiliser ISATAP seulement pour des tests limités. Pour un déploiement à l'échelle de l'intranet, vous devriez plutôt déployer la prise en charge du protocole IPv6 en mode natif.

Qu'est-ce que 6to4 ?



6to4 est une technologie que vous utilisez pour assurer la connectivité IPv6 monodiffusion sur le réseau Internet IPv4. Vous pouvez utiliser 6to4 pour fournir la connectivité IPv6 entre deux sites IPv6, ou entre un hôte IPv6 et un site IPv6. Cependant, 6to4 n'est pas adapté aux scénarios qui requièrent le processus de traduction NAT.

Un routeur 6to4 assure à un site la connectivité IPv6 sur le réseau Internet IPv4. Le routeur 6to4 a une adresse IPv4 publique qui est configurée sur l'interface externe, et une adresse IPv6 6to4 qui est configurée sur l'interface interne. Pour configurer des ordinateurs client, l'interface interne publie le réseau 6to4. Tout ordinateur client qui commence à utiliser l'adresse réseau 6to4 est un hôte 6to4. Les hôtes 6to4 du site envoient les paquets 6to4 au routeur 6to4 en vue de leur remise à d'autres sites sur le réseau Internet IPv4.

L'adresse réseau IPv6 qui est utilisée pour 6to4 est basée sur l'adresse IPv4 de l'interface externe sur un routeur IPv6. Le format de l'adresse IPv6 est 2002:WWXX:YYZZ:ID_sous-réseau:ID_Interface, où WWXX:YYZZ est la représentation hexadécimale séparée par un signe deux-points de w.x.y.z, une adresse IPv4 publique.

Quand un hôte unique sur le réseau Internet IPv4 participe à 6to4, il est configuré en tant qu'hôte/routeur. Un hôte/routeur 6to4 n'effectue pas le routage pour d'autres hôtes, mais génère son propre réseau Ipv6 utilisé pour 6to4.

Activation des fonctionnalités des routeurs 6to4 dans les systèmes d'exploitation Windows

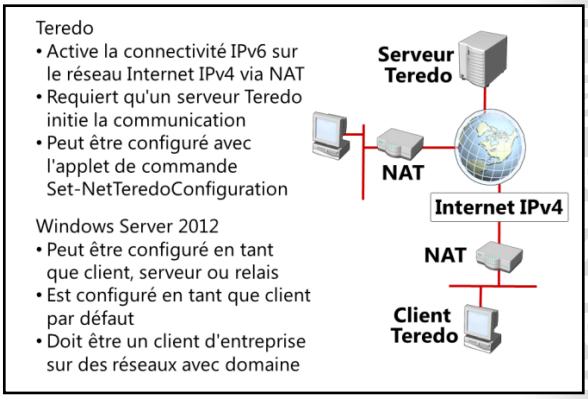
Dans la plupart des cas, vous utilisez les composants de l'infrastructure réseau existante pour agir en tant que routeur 6to4. Cependant, vous pouvez configurer Windows Server 2012 en tant que routeur 6to4 de différentes façons :

- Activez le partage de connexion Internet (ICS). Quand vous activez ICS, Windows Server 2012 est configuré automatiquement en tant que routeur 6to4.
- Utilisez Windows PowerShell. Vous pouvez utiliser l'applet de commande **Set-Net6to4Configuration** pour configurer 6to4.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que Teredo ?

Teredo est semblable à 6to4 en ce qu'il vous permet de transmettre par tunnel des paquets IPv6 sur le réseau Internet IPv4. Cependant, Teredo fonctionne correctement même lorsque la traduction d'adresses réseau est utilisée pour la connectivité Internet. Teredo est nécessaire parce que beaucoup d'organisations utilisent des adresses IP privées, qui nécessitent la traduction d'adresses réseau pour accéder à Internet. Si un périphérique NAT peut être configuré en tant que routeur 6to4, alors Teredo n'est pas requis.



Remarque : Teredo est utilisé uniquement si le protocole ISATAP, 6to4 ou IPv6 en mode natif n'assure pas la connectivité.

La communication IPv6 entre deux clients Teredo sur le réseau Internet IPv4 requiert un serveur Teredo hébergé sur le réseau Internet IPv4. Le serveur Teredo facilite la communication entre les deux clients Teredo en servant de point central pour l'initialisation de la communication. En général, les hôtes derrière un périphérique NAT sont autorisés à initier les communications sortantes, mais ne sont pas autorisés à accepter les communications entrantes. Pour contourner ce problème, les deux clients Teredo initient la communication avec le serveur Teredo. Une fois que la connexion avec le serveur Teredo est établie, et que le périphérique NAT a autorisé les communications sortantes, toutes les communications ultérieures s'établissent directement entre les deux clients Teredo.

Remarque : Plusieurs serveurs Teredo publics sont disponibles sur Internet. Les systèmes d'exploitation Windows utilisent par défaut le serveur Teredo fourni par Microsoft à l'adresse teredo.ipv6.microsoft.com.

Teredo peut également faciliter la communication avec des hôtes IPv6-uniquement sur le réseau Internet IPv6 via un relais Teredo. Le relais Teredo transfère des paquets d'un client Teredo au réseau Internet IPv6.

Vous pouvez configurer Windows Server 2012 en tant que client Teredo, relais Teredo ou serveur Teredo. Pour configurer Teredo, utilisez l'applet de commande Windows PowerShell **Set-NetTeredoConfiguration**. Teredo est configuré par défaut en tant que client. Quand il est configuré en tant que client, Teredo est désactivé lorsqu'il est lié à un réseau avec domaine. Pour activer Teredo sur un réseau avec domaine, vous devez le configurer en tant que client d'entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

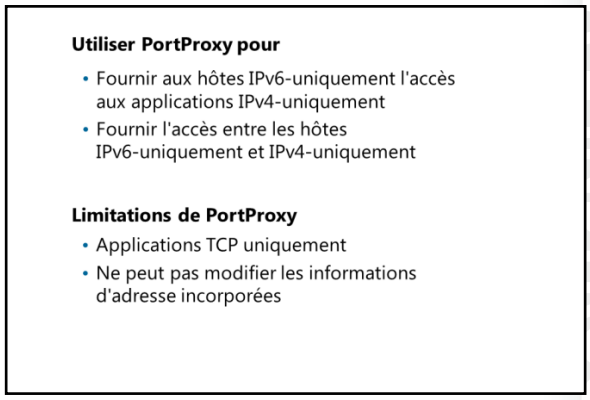
Structure de l'adresse Teredo

Une adresse Teredo est une adresse IPv6 128 bits, mais elle utilise une structure différente des adresses IPv6 monodiffusion typiques. La structure est la suivante :

- 2001::/32 (32 bits). C'est le préfixe spécifique à Teredo qui est utilisé par toutes les adresses Teredo.
- Adresse IPv4 du serveur Teredo (32 bits). Ceci identifie le serveur Teredo.
- Options (16 bits). Il existe plusieurs options qui décrivent la configuration de communication, si le client est derrière un périphérique NAT, par exemple.
- Port externe masqué (16 bits). C'est le port externe utilisé pour la communication par le périphérique NAT pour cette communication. Il est masqué pour empêcher le périphérique NAT de le traduire.
- Adresse IP externe masquée (32 bits). C'est l'adresse IP externe du périphérique NAT. Il est masqué pour empêcher le périphérique NAT de le traduire.

Qu'est-ce que PortProxy ?

Les développeurs d'applications utilisent des API de réseau spécifiques pour accéder à des ressources réseau quand ils écrivent des applications. Les API modernes peuvent utiliser IPv4 ou IPv6, et laissent le système d'exploitation choisir la version du protocole IP. Cependant, quelques applications plus anciennes utilisent des API qui peuvent seulement utiliser IPv4.



Vous utilisez le service PortProxy pour permettre aux applications qui ne prennent pas en charge le protocole IPv6 de communiquer avec des hôtes IPv6. Vous activez PortProxy sur le serveur où l'application s'exécute. Les paquets IPv6 entrants de l'application sont traduits dans le protocole IPv4, puis passés à l'application.

Vous pouvez également utiliser PortProxy comme proxy entre des hôtes IPv4-uniquement et des hôtes IPv6-uniquement. Pour ce faire, vous devez configurer le DNS pour résoudre le nom de l'hôte distant comme étant l'adresse de l'ordinateur PortProxy. Par exemple, un hôte IPv4-uniquement résoudrait le nom d'un hôte IPv6-uniquement comme étant l'adresse IPv4 de l'ordinateur de PortProxy. Les paquets seraient ensuite envoyés à l'ordinateur PortProxy, qui les transmettrait par proxy à l'ordinateur IPv6-uniquement.

PortProxy a les limitations suivantes :

- Il est limité aux connexions TCP seulement. Il ne peut pas être utilisé pour les applications qui utilisent UDP.
- Il ne peut pas modifier les informations d'adresses qui sont incorporées dans la partie données du paquet. Si l'application (FTP (File Transfer Protocol), par exemple) incorpore les informations d'adresses dans la partie données, alors elle ne fonctionnera pas.

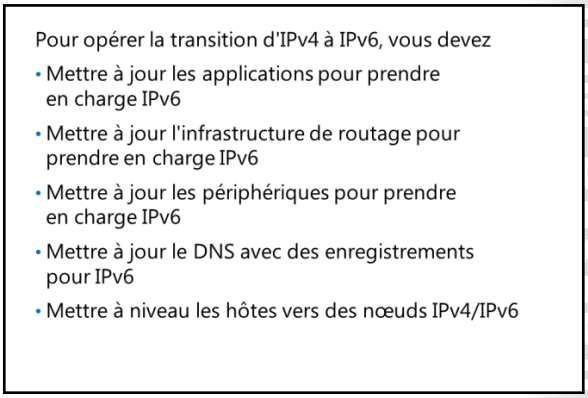
Vous pouvez configurer PortProxy sur Windows Server 2012 à l'aide de **netsh interface portproxy**. Cependant, il est en général préférable d'utiliser une technologie de tunneling au lieu de PortProxy.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Processus de transition vers IPv6

La transition de l'industrie du protocole IPv4 au protocole IPv6 devrait prendre un temps considérable. Ce paramètre a été pris en considération lors de la conception du protocole IPv6. Le programme de transition vers IPv6 est donc un processus à plusieurs étapes qui permet une cohabitation étendue.



Pour parvenir au développement d'un environnement IPv6-uniquement, suivez les instructions générales suivantes :

- Mettez à niveau vos applications pour les rendre indépendantes des protocoles IPv6 ou IPv4. Par exemple, vous pouvez modifier les applications pour l'emploi de nouvelles API Windows Sockets afin que la résolution de noms, la création de sockets et d'autres fonctions demeurent indépendantes, que vous utilisiez le protocole IPv4 ou bien le protocole IPv6.
- Mettez à niveau l'infrastructure de routage pour le routage IPv6 natif. Vous devez mettre à niveau des routeurs capables de prendre en charge à la fois les protocoles de routage IPv6 et IPv6 natif.
- Effectuez la mise à niveau des périphériques pour prendre en charge IPv6. La majorité du matériel réseau actuel prend en charge IPv6, mais beaucoup d'autres types de périphériques ne font pas. Vous devez vérifier que tous les périphériques liés au réseau, tels que les imprimantes et les scanneurs, prennent également en charge IPv6.
- Mettez à jour l'infrastructure DNS pour la prise en charge des enregistrements de ressource du pointeur (PTR) et d'adresse IPv6. Vous devrez peut-être mettre l'infrastructure DNS pour prendre en charge les nouveaux enregistrements de ressource de l'adresse de l'hôte IPv6 (AAAA) (obligatoire) et les enregistrements de ressource du pointeur (PTR) dans le domaine inverse IP6.ARPA, mais c'est facultatif. De plus, assurez-vous que les serveurs DNS prennent en charge le trafic DNS sur IPv6, et la mise à jour dynamique du système DNS pour les enregistrements de ressource de l'adresse de l'hôte IPv6 (AAAA) afin que les hôtes IPv6 puissent enregistrer automatiquement leurs noms et leurs adresses IPv6.
- Mettez à niveau les hôtes vers des nœuds IPv6/IPv4. Vous devez mettre les hôtes à niveau pour utiliser IPv4 et IPv6. Ceci permet aux hôtes d'accéder à la fois aux ressources IPv4 et IPv6 pendant le processus de migration.

La plupart des organisations ajouteront probablement IPv6 à un environnement IPv4 existant et continueront à avoir faire coexister ces deux protocoles pendant longtemps. Beaucoup d'applications et de périphériques hérités qui ne prennent pas en charge IPv6 existent toujours, et la coexistence est beaucoup plus simple que l'utilisation de technologies de transition telles qu'ISATAP. Vous devriez supprimer IPv4 uniquement après que les ressources qui dépendent de ce protocole aient été soit supprimées, soit mises à jour afin d'utiliser IPv6.

IPv6 est activé par défaut pour Windows Vista et les systèmes d'exploitation clients Windows ultérieurs, et Windows Server 2008 et les systèmes d'exploitation clients Windows Server ultérieurs. Il est recommandé de ne pas désactiver IPv6 à moins qu'il y ait une raison technique de le faire. Certaines fonctionnalités des systèmes d'exploitation Windows sont basées sur IPv6.

Atelier pratique : Implémentation d'IPv6

Scénario

La société A. Datum Corporation a un bureau et un centre de données informatiques à Londres qui prennent en charge le site de Londres ainsi que d'autres sites. Ils ont récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8. Vous devez à présent configurer le service d'infrastructure pour une nouvelle filiale.

Le responsable informatique chez A. Datum a reçu des instructions de plusieurs éditeurs d'applications au sujet de la prise en charge d'IPv6 récemment ajoutée dans leurs produits. A. Datum n'a pas mis en place la prise en charge d'IPv6 pour le moment. Le responsable informatique voudrait que vous configuriez un environnement de test qui utilise IPv6. Dans le cadre de la configuration de l'environnement de test, vous devez également configurer ISATAP afin de permettre la communication entre un réseau IPv4 et un réseau IPv6.

Ceci est la structure de l'environnement de test complété.

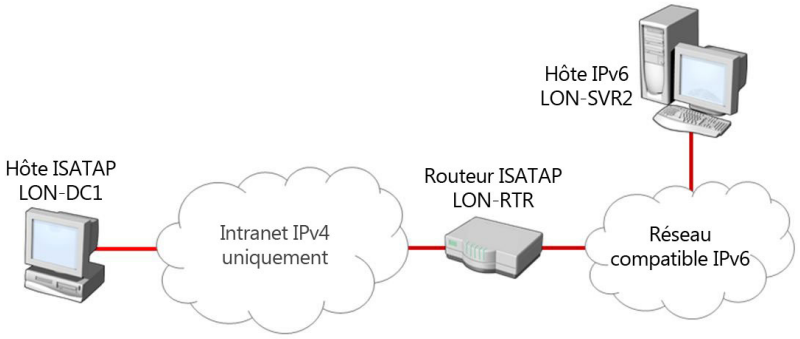


FIGURE 8.1 : RÉSULTAT FINAL DE L'ATELIER PRATIQUE

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer un réseau IPv6 ;
- configurer un routeur ISATAP.

Configuration de l'atelier pratique

Durée approximative : 30 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-RTR 22410B-LON-SVR2
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur Gestionnaire Hyper-V®.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
5. Répétez les étapes 2 à 4 pour **22410B-LON-RTR** et **22410B-LON-SVR2**.

Exercice 1 : Configuration d'un réseau IPv6

Scénario

Pour la première étape de la configuration de l'environnement de test, vous devez configurer LON-DC1 comme nœud IPv4-uniquement et LON-SVR2 comme nœud IPv6-uniquement. Vous devez également configurer LON-RTR afin de prendre en charge le routage IPv6 en ajoutant un réseau à une interface sur le réseau IPv6, et en activant les annonces de routage. Les annonces de routage permettent aux clients IPv6 sur le réseau IPv6 d'obtenir automatiquement le réseau IPv6 correct via la configuration sans état.

Les tâches principales de cet exercice sont les suivantes :

1. Vérifier le routage IPv4
2. Désactiver le protocole IPv6 sur LON-DC1
3. Désactiver le protocole IPv4 sur LON-SVR2
4. Configurer un réseau IPv6 sur LON-RTR
5. Vérifier IPv6 sur LON-SVR2

▶ Tâche 1 : Vérifier le routage IPv4

1. Sur LON-SVR2, ouvrez une invite Windows PowerShell.
2. Utiliser la commande Ping sur **LON-DC1** pour vérifier le routage d'IPv4 via LON-RTR.
3. Utilisez la commande **ipconfig** pour vérifier que LON-SVR2 a seulement une adresse IPv6 de liaison locale qui ne peut pas être routée.

▶ Tâche 2 : Désactiver le protocole IPv6 sur LON-DC1

1. Sur LON-DC1, dans le Gestionnaire de serveur, sur le **Serveur local**, ouvrez les propriétés **Connexion au réseau local**.
2. Désactivez IPv6 pour la connexion au réseau local pour faire de LON-DC1 un hôte IPv4-uniquement.

▶ Tâche 3 : Désactiver le protocole IPv4 sur LON-SVR2

1. Sur LON-SVR2, dans le Gestionnaire de serveur, sur le **Serveur local**, ouvrez les propriétés de **Connexion au réseau local**.
2. Désactivez IPv4 pour la connexion au réseau local afin de faire de LON-SVR2 un hôte IPv6-uniquement.

▶ Tâche 4 : Configurer un réseau IPv6 sur LON-RTR

1. Sur LON-RTR, ouvrez **Windows PowerShell**.
2. Configurez une adresse réseau qui sera utilisée sur le réseau IPv6 en utilisant l'applet de commande **New-NetRoute** suivante de Windows PowerShell pour ajouter un réseau IPv6 sur la connexion au réseau local 2 à la table de routage locale :

```
New-NetRoute -InterfaceAlias "Connexion au réseau local 2" -DestinationPrefix
2001:db8:0:1::/64 -Publish Yes
```

3. Autorisez les clients à obtenir l'adresse de réseau IPv6 automatiquement à partir de LON-RTR en utilisant l'applet de commande **Set-NetIPInterface** suivante pour activer les annonces de routeur sur la connexion au réseau local 2 :

```
Set-NetIPInterface -InterfaceAlias "Connexion au réseau local 2" -AddressFamily IPv6
-Advertising Enabled
```

4. Utilisez **ipconfig** pour vérifier que la connexion au réseau local 2 a une adresse IPv6 sur le réseau **2001:db8:0:1::/64**. Cette adresse est utilisée pour la communication sur le réseau IPv6-uniquement.

▶ Tâche 5 : Vérifier IPv6 sur LON-SVR2

- Sur LON-SVR2, utilisez **ipconfig** pour vérifier que la connexion au réseau local a une adresse IPv6 sur le réseau 2001:db8:0:1::/64. L'adresse réseau a été obtenue à partir du routeur via la configuration sans état.

Résultats : À la fin de cet exercice, les stagiaires auront configuré un réseau IPv6-uniquement.

Exercice 2 : Configuration d'un routeur ISATAP

Scénario

Après la configuration de l'infrastructure pour un réseau IPv4-uniquement et un réseau IPv6-uniquement, vous devez configurer LON-RTR en tant que routeur ISATAP pour prendre en charge la communication entre les nœuds IPv4-uniquement et les nœuds IPv6-uniquement.

Pour configurer LON-RTR en tant que routeur ISATAP, vous devez activer l'interface IPv4 en tant que routeur ISATAP. Ensuite, vous configurez un réseau IPv6 sur l'interface ISATAP et activez l'annonce de la route réseau qui comprend ce réseau. Les clients ISATAP obtiendront le réseau IPv6 automatiquement à partir des annonces.

Pour activer ISATAP automatiquement sur les clients, vous devez créer un enregistrement d'hôte ISATAP dans le DNS. Les clients qui peuvent résoudre ce nom automatiquement deviennent des clients ISATAP. Pour autoriser les clients à résoudre ce nom, vous devez supprimer ISATAP de la liste rouge de requêtes globales sur le serveur DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter un enregistrement d'hôte ISATAP au DNS
2. Activer le routeur ISATAP sur LON-RTR
3. Supprimer ISATAP de la liste rouge de requêtes globales
4. Activer LON-DC1 en tant que client ISATAP
5. Tester la connectivité

▶ Tâche 1 : Ajouter un enregistrement d'hôte ISATAP au DNS

1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez l'outil **DNS**.
2. Ajoutez un enregistrement d'hôte **ISATAP** dans le domaine Adatum.com qui est résolu en **172.16.0.1**. Les clients ISATAP résolvent ce nom d'hôte pour rechercher le routeur ISATAP.

▶ Tâche 2 : Activer le routeur ISATAP sur LON-RTR

1. Sur LON-RTR, configurez l'adresse IP de la connexion au réseau local en tant que routeur ISATAP. Utilisez l'applet de commande **Set-NetIsatapConfiguration** suivante pour activer ISATAP :

```
Set-NetIsatapConfiguration -Router 172.16.0.1
```

2. Utilisez l'applet de commande **Get-NetIPAddress** suivante pour identifier l'index d'interface de l'interface ISATAP avec 172.16.0.1 dans l'adresse de liaison locale.

```
Get-NetIPAddress | Format-Table InterfaceAlias,InterfaceIndex,IPv6Address
```

Enregistrez l'index d'interface ici :	

3. Utilisez l'applet de commande **Get-NetIPInterface** pour vérifier les options suivantes sur l'interface ISATAP :
   - La fonctionnalité de transfert est activée
   - La fonctionnalité d'annonce est désactivée

```
Get-NetIPInterface -InterfaceIndex IndexYouRecorded -PolicyStore ActiveStore |
Format-List
```

4. L'interface ISATAP d'un routeur ISATAP doit avoir la fonctionnalité de transfert activée et la fonctionnalité d'annonce désactivée. Utilisez l'applet de commande **Set-NetIPInterface** suivante pour activer les annonces de routeur sur l'interface ISATAP :

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Enabled
```

5. Créez un nouveau réseau IPv6 qui sera utilisé pour le réseau ISATAP. Utilisez l'applet de commande **New-NetRoute** suivante pour configurer une route réseau pour l'interface ISATAP :

```
New-NetRoute -InterfaceIndex IndexYouRecorded -DestinationPrefix 2001:db8:0:2::/64 -
Publish Yes
```

6. Utilisez l'applet de commande **Get-NetIPAddress** suivante pour vérifier que l'interface ISATAP a une adresse IPv6 sur le réseau 2001:db8:0:2::/64 :

```
Get-NetIPAddress -InterfaceIndex IndexYouRecorded
```

▶ Tâche 3 : Supprimer ISATAP de la liste rouge de requêtes globales

1. Sur LON-DC1, ouvrez **Regedit** et accédez à **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters**.
2. Modifiez **GlobalQueryBlockList** pour supprimer **isatap** de la liste.
3. Redémarrer le service **DNS**.
4. Exécutez la commande Ping sur **isatap** pour vérifier qu'il peut être résolu. Le nom devrait se résoudre et vous devriez recevoir quatre réponses de 172.16.0.1.

▶ Tâche 4 : Activer LON-DC1 en tant que client ISATAP

1. Sur LON-DC1, utilisez l'applet de commande **Set-NetIsatapConfiguration** suivante pour activer ISATAP :

```
Set-NetIsatapConfiguration -State Enabled
```

2. Utilisez ipconfig pour vérifier que la carte tunnel pour ISATAP a une adresse IPv6 sur le réseau 2001:db8:0:2/64. Notez que cette adresse comprend l'adresse IPv4 de LON-DC1.

▶ Tâche 5 : Tester la connectivité

1. Sur LON-SVR2, utilisez la commande Ping suivante pour tester la connectivité à l'adresse ISATAP de LON-DC1 :

```
ping 2001:db8:0:2:0:5efe:172.16.0.10
```

2. Utilisez le Gestionnaire de serveur pour modifier les propriétés de TCP/IPv6 sur la connexion au réseau local et ajoutez **2001:db8:0:2:0:5efe:172.16.0.10** en tant que serveur DNS préféré.
3. Utilisez la commande ping pour tester la connectivité à **LON-DC1**.

Remarque : Une commande ping de LON-DC1 à LON-SVR2 ne répond pas, parce que la configuration du pare-feu sur LON-SVR2 bloque les demandes ping.

Résultats : À la fin de cet exercice, les stagiaires auront configuré un routeur ISATAP sur LON-RTR pour permettre la communication entre un réseau IPv6-uniquement et un réseau IPv4-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 **22410B-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 **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quelle est la différence principale entre 6to4 et Teredo ?

Question : Comment pouvez-vous fournir un serveur DNS à un hôte IPv6 de façon dynamique ?

Question : Votre organisation envisage d'implémenter IPv6 en interne. Après quelques recherches, vous avez identifié les adresses IPv6 locales uniques comme étant le type d'adresses IPv6 adéquat à utiliser pour un réseau privé. Pour utiliser des adresses IPv6 locales uniques, vous devez sélectionner un identificateur de 40 bits qui fasse partie du réseau. Un collègue propose d'utiliser tous les zéros pour les 40 bits. Pourquoi cela n'est-il pas une bonne idée ?

Question : Avec combien d'adresses IPv6 un nœud IPv6 devrait-il être configuré ?

Méthode conseillée

Utilisez les méthodes conseillées suivantes lorsque vous implémentez IPv6 :

- ne désactivez pas IPv6 sur Windows 8 ou Windows Server 2012 ;
- activez la coexistence d'IPv4 et IPv6 dans votre organisation au lieu d'utiliser des technologies de transition ;
- utilisez des adresses IPv6 locales uniques sur votre réseau interne ;
- utilisez Teredo pour implémenter la connectivité IPv6 sur le réseau Internet IPv4.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9

Implémentation d'un système de stockage local

Table des matières :

Vue d'ensemble du module **9-1**

Leçon 1 : Vue d'ensemble du stockage **9-2**

Leçon 2 : Gestion des disques et des volumes **9-13**

Leçon 3 : Implémentation d'espaces de stockage **9-25**

Atelier pratique : Implémentation d'un système de stockage local **9-30**

Contrôle des acquis et éléments à retenir **9-36**

Vue d'ensemble du module

Le stockage est l'un des éléments clés que vous devez prendre en compte lors de la planification et du déploiement d'un système d'exploitation Windows Server® 2012. La plupart des organisations requièrent une grande quantité d'espace de stockage, car les utilisateurs utilisent régulièrement des applications qui créent des fichiers nécessitant d'être stockés dans un emplacement central. Lorsque les utilisateurs conservent leurs fichiers plus longtemps, les besoins en matière de stockage augmentent. Chaque fois qu'un utilisateur se connecte à un serveur, un journal d'audit est créé dans un journal des événements, ce qui utilise également du stockage. Même les processus de création, de copie et de déplacement de fichiers requièrent du stockage.

Ce module vous présente différentes technologies de stockage. Il explique comment implémenter les solutions de stockage dans Windows Server 2012 et comment utiliser les espaces de stockage, une nouvelle fonctionnalité que vous pouvez utiliser pour regrouper des disques en pools qui sont ensuite gérés automatiquement.

Objectifs

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

- Décrire les différentes technologies de stockage.
- Expliquer comment gérer les disques et les volumes.
- Expliquer comment implémenter des espaces de stockage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble du stockage

Lorsque vous organisez un déploiement de serveur, l'un des éléments clés dont vous avez besoin est le stockage. Vous pouvez utiliser différents types de stockage, du stockage en local au stockage accessible à distance via Ethernet, ou même du stockage connecté à l'aide de la fibre optique. Il est important que vous connaissiez les avantages et les inconvénients de chaque solution.

Lors de la préparation du déploiement du stockage pour votre environnement, vous devrez prendre quelques décisions importantes. Cette leçon aborde des questions que vous êtes susceptible d'examiner, notamment les suivantes :

- Le stockage doit-il être rapide ?
- Le stockage doit-il être hautement disponible ?
- Quelle capacité de stockage votre déploiement requiert-il réellement ?
- Combien de résilience devez-vous ajouter au stockage initial requis pour garantir la fiabilité de votre investissement dans le temps ?

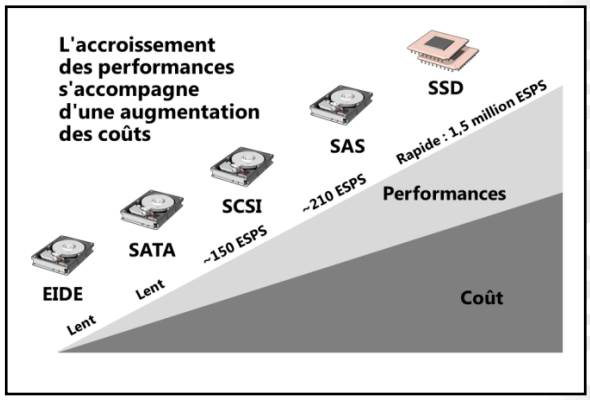
Objectifs de la leçon

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

- Décrire les types et les performances de disque.
- Décrire le stockage à connexion directe.
- Décrire le stockage réseau (NAS, Network-Attached Storage).
- Décrire un réseau de zone de stockage (SAN, Storage Area Network).
- Décrire un système RAID (Redundant Array of Independent Disks).
- Décrire les niveaux de RAID.

Types et performances de disque

Il existe différents types de disque que vous pouvez utiliser pour fournir un espace de stockage aux systèmes serveur et client. La vitesse des disques est mesurée en entrées/sorties par seconde. Les types de disque les plus courants sont les suivants :



- *Disques IDE (Integrated Drive Electronics) améliorés.* Les disques IDE améliorés sont basés sur des normes créées en 1986. L'interface IDE (Integrated Drive Electronics) prend en charge les normes ATA-2 et ATAPI. *« L'amélioration »* fait référence à la norme ATA-2 (ATA rapide). En raison des normes d'adressage de cette technologie, la capacité des systèmes de stockage utilisant l'IDE amélioré est limitée à 128 gigaoctets (Go). En outre, la vitesse des disques IDE améliorés ne peut pas dépasser 133 mégaoctets (Mo) par seconde. À l'heure actuelle, les lecteurs IDE améliorés ne sont presque jamais utilisés sur des serveurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Disques SATA (Serial Advanced Technology Attachment).* SATA est une interface de bus d'ordinateur, ou un canal, permettant de connecter les cartes de carte mère ou de périphérique à des périphériques de stockage de masse tels que des lecteurs de disque dur et des lecteurs de disque optique. La norme SATA a été conçue pour remplacer la norme IDE amélioré. Elle peut utiliser les mêmes commandes de bas niveau, mais les cartes et les périphériques hôtes SATA communiquent par l'intermédiaire d'un câble série ultra-rapide comportant deux paires de conducteurs. La norme SATA a été introduite en 2003. Elle peut fonctionner à des vitesses de 1,5, 3 et 6 Go par seconde, selon la révision de la norme (SATA 1, 2 ou 3 respectivement). Les lecteurs SATA sont moins chers que d'autres options de lecteurs, mais ils sont également moins performants. Les organisations peuvent choisir de déployer des lecteurs SATA lorsqu'elles ont besoin de grandes capacités de stockage mais pas de performances élevées. Les disques SATA sont généralement des disques peu coûteux qui permettent un stockage de masse. Toutefois, leur fiabilité est également moindre que celle des disques SAS (Serial Attached SCSI).

  eSATA est une variation de l'interface SATA, conçue pour permettre un accès rapide aux lecteurs SATA externes.

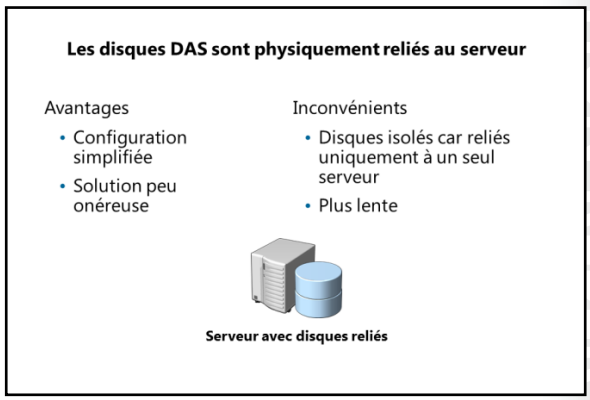
- *SCSI (Small Computer System Interface).* SCSI est un ensemble de normes permettant de connecter et de transférer physiquement des données entre des ordinateurs et des périphériques. La norme SCSI a été introduite pour la première fois en 1978. Il s'agissait d'une interface de communication de niveau inférieur nécessitant moins de puissance de traitement tout en permettant d'exécuter des transactions à des vitesses plus élevées. SCSI est devenu une norme en 1986. Similaire à EIDE, SCSI a été conçu pour s'exécuter sur des câbles parallèles, mais son utilisation a récemment été étendue de manière à pouvoir s'exécuter sur d'autres supports. La spécification SCSI parallèle de 1986 avait une vitesse de transfert initiale de 5 Mo par seconde. L'implémentation SCSI de 2003, la norme Ultra 640, également appelée Ultra 5, peut transférer des données à la vitesse de 640 Mo par seconde. Les disques SCSI offrent des performances plus élevées que celles des disques SATA, mais ils sont également plus chers.

- *SAS.* SAS est une autre implémentation de la norme SCSI. SAS dépend d'un protocole série point par point qui remplace la technologie des bus SCSI parallèles et utilise l'ensemble des commandes de la norme SCSI. SAS offre une compatibilité descendante avec les lecteurs SATA de seconde génération. Les lecteurs SAS sont fiables et conçus pour fonctionner 24 heures sur 24, 7 jours sur 7 (24/7) dans des centres de données. Avec jusqu'à 15 000 tours/minute, ces disques sont également les disques durs classiques les plus rapides.

- *Disques SSD (Solid State Drives).* Les disques SSD sont des dispositifs de stockage de données qui utilisent une mémoire à semi-conducteurs pour enregistrer les données plutôt que d'utiliser les disques à rotation et les têtes de lecture-écriture mobiles utilisés dans d'autres disques. Les disques SSD utilisent des microprocesseurs pour stocker les données et ils ne contiennent aucune pièce mobile. Ils permettent un accès disque rapide, consomment moins d'énergie et sont moins susceptibles d'avoir des défaillances s'ils tombent que les disques durs traditionnels (tels que les lecteurs SAS), mais ils sont également beaucoup plus coûteux par Go de stockage. Les disques SSD utilisent généralement une interface SATA, ce qui permet habituellement de remplacer des lecteurs de disque dur par des disques SSD sans aucune modification.

Remarque : Les disques Fibre Channel, Firewire ou USB sont également des options de stockage possibles. Ils définissent le bus de transport ou le type de disque. Par exemple, les disques USB utilisent principalement des lecteurs SATA ou SSD pour enregistrer les données.

Qu'est-ce que le stockage DAS ?



Presque tous les serveurs comportent un système de stockage intégré. Ce type de stockage est appelé *stockage à connexion directe* (DAS, Direct Attached Storage). Les systèmes de stockage DAS peuvent comprendre des disques qui se trouvent physiquement à l'intérieur du serveur ou qui se connectent directement à un tableau externe, ou encore des disques qui se connectent au serveur à l'aide d'un câble USB ou d'une autre méthodologie de communication. Le stockage DAS est principalement connecté physiquement au serveur. Pour cette raison, si le serveur subit une panne d'alimentation, le stockage n'est pas disponible. Les stockage DAS se présentent sous différents types de disque tels que les disques SATA, SAS ou SSD, qui affectent la vitesse et les performances du stockage, et présente à la fois des avantages et des inconvénients.

Avantages de l'utilisation d'un stockage DAS

Un système DAS type se compose d'un dispositif de stockage de données comprenant plusieurs lecteurs de disque dur qui se connectent directement à un ordinateur via un adaptateur de bus hôte (HBA, Host Bus Adapter). Entre le système DAS et l'ordinateur, il n'y a aucun périphérique réseau tel qu'un concentrateur, un commutateur ou un routeur. À la place, le stockage est connecté directement au serveur qui l'utilise, faisant de DAS le système de stockage le plus facile à déployer et à gérer.

De plus, à l'heure actuelle, le système DAS constitue généralement le stockage le moins coûteux et il est largement disponible en différentes vitesses et tailles de manière à s'adapter à diverses installations. Outre son coût peu élevé, il est très facile à configurer. Dans la plupart des instances, il suffit de brancher le périphérique, de vérifier que le système d'exploitation Windows® en cours d'exécution l'identifie, puis d'utiliser Gestion des disques pour configurer les disques.

Inconvénients de l'utilisation d'un stockage DAS

L'enregistrement des données en local sur un système DAS rend la centralisation des données plus difficile, car celles-ci se trouvent sur plusieurs serveurs. Cela peut rendre plus complexe la sauvegarde des données et, pour les utilisateurs, la localisation des données qu'ils recherchent. En outre, si l'un des périphériques auxquels le système DAS est connecté subit une panne de courant, le stockage sur cet ordinateur n'est plus disponible.

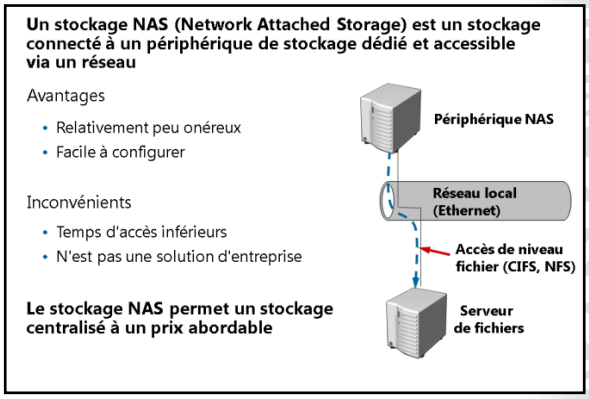
Le système DAS présente également des inconvénients en matière de méthodologies d'accès. En raison de la façon dont le système d'exploitation du serveur gère les accès en lecture et en écriture, le système DAS peut être plus lent que d'autres technologies de stockage. Un autre inconvénient réside dans le fait que le système DAS partage la puissance de traitement et la mémoire du serveur auquel il est connecté. Ceci signifie que sur les serveurs très occupés, l'accès disque peut être plus lent lorsque le système d'exploitation est surchargé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que le stockage NAS ?

Un stockage NAS (Network Attached Storage) est un stockage connecté à un périphérique de stockage dédié et accessible via un réseau. Un stockage NAS diffère d'un stockage DAS dans la mesure où le stockage n'est pas directement connecté à chaque serveur individuel mais qu'il est accessible à de nombreux serveurs via un réseau. Le système NAS comporte deux solutions distinctes : un dispositif bas de gamme (NAS uniquement) et un système NAS d'entreprise qui s'intègre à SAN.



Chaque périphérique NAS dispose d'un système d'exploitation dédié qui contrôle uniquement l'accès aux données sur ce périphérique, ce qui réduit la charge système associée au partage du périphérique de stockage avec d'autres services de serveur. Un exemple de logiciel de NAS est Windows Storage Server, une fonctionnalité de Windows Server 2012.

Pour activer le stockage NAS, vous avez besoin d'un périphérique de stockage. Ces périphériques sont souvent des appareils qui ne disposent d'aucune interface de serveur telle qu'un clavier, une souris et un écran. Pour configurer le périphérique, vous indiquez une configuration réseau, puis vous accédez au périphérique via le réseau. Vous pouvez ensuite créer des partages réseau sur le périphérique à l'aide du nom du NAS et du partage créés. Ces partages sont alors accessibles aux utilisateurs sur le réseau.

Aujourd'hui, la plupart des solutions SAN comportent à la fois un système SAN et un système NAS. Les unités principales, les disques et les technologies sont identiques. La seule différence réside dans la méthode d'accès. Les entreprises permettent souvent aux serveurs d'accéder au stockage des réseaux SAN à l'aide de FCOE (Fibre Channel over Ethernet) ou d'iSCSI (Internet Small Computer System Interface), tandis que les services NAS sont rendus accessibles par l'intermédiaire du protocole CIFS et du système NFS ; les lecteurs de disques (agrégats), les méthodes d'écriture, la surcharge système et la fiabilité sont identiques.

Avantages de l'utilisation d'un stockage NAS

Le stockage NAS est le choix idéal pour les organisations qui recherchent une manière simple et rentable de permettre à plusieurs clients d'accéder rapidement à des données au niveau des fichiers. Les utilisateurs du stockage NAS obtiennent des gains en matière de performance et de productivité, car la puissance de traitement du périphérique NAS est uniquement dédiée à la distribution des fichiers.

Les systèmes de stockage NAS, en tant que solutions de moyenne de gamme, sont également bien positionnés sur le marché. Il ne sont pas coûteux et répondent à davantage de besoins que les systèmes de stockage DAS de différentes façons :

- Le stockage NAS est habituellement beaucoup plus important que le stockage DAS.
- Le stockage NAS fournit un emplacement unique pour tous les fichiers critiques, contrairement au stockage DAS qui les disperse sur différents serveurs ou périphériques.

- Le stockage NAS permet un stockage centralisé à un prix abordable.
- Les unités de stockage NAS sont accessibles de n'importe quel système d'exploitation. Elles prennent souvent en charge plusieurs protocoles et peuvent servir des données par l'intermédiaire du protocole CIFS et de NFS simultanément. Par exemple, des hôtes Windows et Linux peuvent accéder simultanément à une unité de stockage NAS.

Le stockage NAS peut également être considéré comme une solution prête à l'emploi, facile installer, à déployer et à gérer, avec ou sans personnel informatique sur site.

Inconvénients de l'utilisation d'un stockage NAS

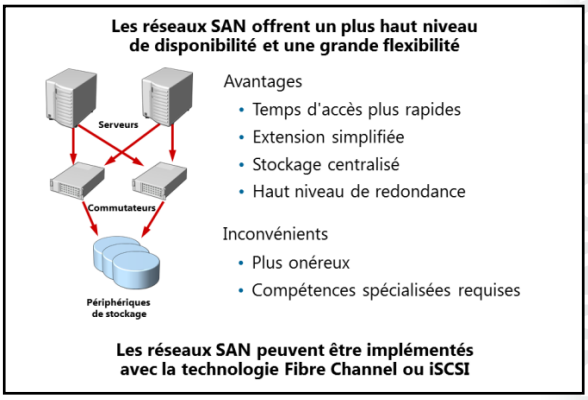
Le stockage NAS est plus lent que les technologies SAN. Le stockage NAS est fréquemment accessible via protocoles Ethernet. Pour cette raison, il repose principalement sur le réseau prenant en charge la solution NAS. Il est donc généralement utilisé comme solution de partage/stockage de fichiers et ne doit pas être utilisé avec des applications nécessitant de nombreuses données telles que Microsoft® Exchange Server et Microsoft SQL Server®.

Le stockage NAS est abordable pour les petites et moyennes entreprises et, semblable au stockage DAS, offre les traitements d'un système d'exploitation qui lit et écrit des données différemment d'une solution SAN. En tant que tels, les systèmes de stockage NAS sont plus fréquemment sujets à d'éventuelles pertes de données, en fonction de la taille des données à copier.

Documentation supplémentaire : Pour plus d'informations sur Windows Storage Server 2012, voir http://go.microsoft.com/fwlink/?LinkID=199647.

Qu'est-ce qu'un réseau SAN ?

Les réseaux SAN constituent le troisième type de<stockage. Un réseau SAN est un réseau à haut débit qui connecte des systèmes informatiques ou des serveurs hôtes à des sous-systèmes de stockage hautes performances. Un réseau SAN comprend habituellement divers composants tels que des adaptateurs de bus hôte, des commutateurs spéciaux pour aider à router le trafic, et des baies de disque de stockage avec des numéros d'unité logique pour le stockage.



Un réseau SAN permet à plusieurs serveurs d'accéder à un pool du stockage dans lequel n'importe quel serveur peut potentiellement accéder à n'importe quelle unité de stockage. Un réseau SAN utilise un réseau comme n'importe quel autre réseau, tel qu'un réseau local (LAN). Vous pouvez donc utiliser un réseau SAN pour connecter de nombreux périphériques et hôtes différents et permettre d'accéder à n'importe quel périphérique de n'importe où.

À la différence des systèmes DAS ou NAS, un réseau SAN est contrôlé par un périphérique matériel, offre l'accès le plus rapide au stockage, et fournit des méthodes permettant de réduire la charge système (à l'aide de disques bruts, par exemple).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avantages de l'utilisation d'un stockage SAN

Les technologies SAN lisent et écrivent au niveau des blocs, ce qui rend l'accès aux données beaucoup plus rapide. Par exemple, avec la plupart des solutions DAS et NAS, si vous écrivez un fichier de 8 Go, la totalité du fichier doit être lue/écrite et sa somme de contrôle calculé. Avec une solution SAN, le fichier est écrit sur le disque en fonction de la longueur de bloc pour laquelle la solution est configurée. Cette vitesse est obtenue grâce à des méthodologies d'accès par fibre et de l'écriture au niveau du bloc, au lieu de devoir lire/écrire un fichier entier à l'aide d'une somme de contrôle.

Les réseaux SAN permettent également de bénéficier des avantages suivants :

- Centralisation du stockage dans un pool unique, qui permet à des ressources de stockage et à des ressources de serveur de se développer de manière indépendante. Ils permettent également au stockage d'être affecté dynamiquement à partir du pool lorsque cela est nécessaire. Le stockage sur un serveur donné peut être augmenté ou réduit autant que nécessaire sans reconfiguration complexe ou recâblage de périphériques.
- Infrastructure courante pour connecter le stockage, laquelle active un modèle de gestion courant unique pour la configuration et le déploiement.
- Dispositifs de stockage partagés de manière inhérente par plusieurs systèmes.
- Transfert de données directement de périphérique à périphérique sans intervention de serveur.
- d'un haut niveau de redondance. La plupart des solutions SAN sont déployées avec plusieurs périphériques et chemins d'accès réseau via le réseau. Le dispositif de stockage contient également des composants redondants tels que des sources d'alimentation et des disques durs.

Inconvénients de l'utilisation d'un stockage SAN

L'inconvénient majeur de la technologie SAN réside dans la complexité de la configuration, les réseaux SAN nécessitant souvent des outils de gestion et un bon niveau d'expertise. En outre, cette solution est considérablement plus coûteuse que les solutions DAS ou NAS ; une solution SAN d'entrée de gamme peut souvent coûter aussi cher qu'un serveur entièrement chargé avec un périphérique DAS ou NAS, et cela sans aucune configuration ou aucun disque SAN.

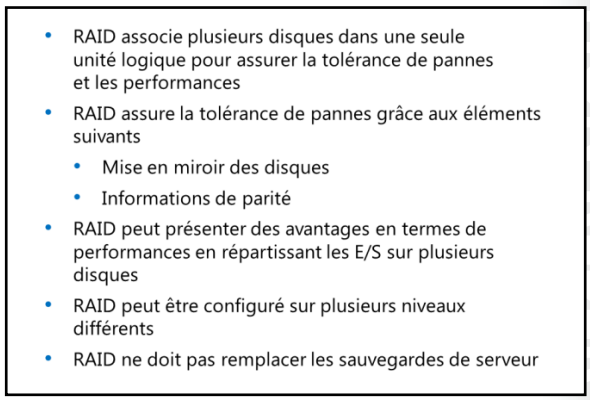
Pour gérer un réseau SAN, vous utilisez souvent des outils de ligne de commande. Vous devez avoir une solide compréhension de la technologie sous-jacente, y compris de la configuration du numéro d'unité logique, du réseau Fibre Channel, du dimensionnement des blocs et d'autres facteurs. En outre, chaque fournisseur de stockage implémente souvent les solutions SAN en utilisant des fonctionnalités et des outils différents. Pour cette raison, les organisations disposent fréquemment d'un personnel entièrement dédié à la gestion du déploiement SAN.

Remarque : Vous pouvez implémenter un réseau SAN à l'aide de nombreuses technologies. Les options les plus courantes sont Fibre Channel et iSCSI.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que RAID ?

RAID est une technologie que vous pouvez utiliser pour configurer des systèmes de stockage présentant une grande fiabilité et (potentiellement) des performances élevées. RAID implémente des systèmes de stockage en combinant plusieurs disques en une seule unité logique appelée *contrôleur RAID*. Selon la configuration, un contrôleur RAID peut résister à la défaillance d'un ou plusieurs des disques durs physiques, ou offrir des performances plus élevées qu'avec un seul disque.



La technologie RAID offre un composant important, la redondance, que vous pouvez utiliser lors de la planification et du déploiement de serveurs Windows Server 2012. Dans la plupart des organisations, il est important que les serveurs soient disponibles en permanence. La plupart des serveurs fournissent des composants très redondants tels que des sources d'alimentation redondantes et des cartes réseau redondantes. L'objectif de cette redondance est de s'assurer que le serveur reste disponible même lorsqu'un seul composant sur le serveur échoue. En implémentant la technologie RAID, vous pouvez fournir le même niveau de redondance pour le système de stockage.

Fonctionnement de RAID

La technologie RAID active la tolérance de pannes en utilisant des disques supplémentaires afin de garantir que le sous-système de disque peut continuer à fonctionner même si un ou plusieurs disques du sous-système tombent en panne. RAID utilise deux options pour activer la tolérance de pannes :

- Mise en miroir des disques. Grâce à cette option, toutes les informations qui sont écrites sur un disque le sont également sur un autre disque. En cas de défaillance de l'un des disques, l'autre disque reste disponible.
- Informations de parité. Les informations de parité sont utilisées en cas de défaillance de disque pour calculer les informations qui ont été stockées sur un disque. Si vous utilisez cette option, le serveur ou le contrôleur RAID calcule les informations de parité pour chaque bloc de données écrit sur les disques, puis stocke ces informations sur un autre disque ou sur plusieurs disques. En cas de défaillance de l'un des disques du contrôleur RAID, le serveur peut utiliser les données encore disponibles sur les disques qui fonctionnent avec les informations de parité pour recréer les données stockées sur le disque défectueux.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les sous-systèmes RAID peuvent également offrir de meilleures performances que les disques uniques en répartissant les lectures et écritures de disque entre plusieurs disques. Par exemple, lors de l'implémentation de l'agrégation de disques, le serveur peut lire les informations de tous les disques durs dans l'agrégat par bandes. Combiné avec plusieurs contrôleurs de disque, cette technologie peut apporter d'importantes améliorations en termes de performance du disque.

Remarque : Bien que RAID offre un niveau de tolérance supérieur pour les défaillances de disque, ne l'utilisez pas pour remplacer les sauvegardes classiques. Si un serveur subit une surtension ou une défaillance majeure et que tous les disques tombent en panne, vous devrez toujours compter sur les sauvegardes standards.

RAID matériel et RAID logiciel

Pour implémenter un volume RAID matériel, vous installez un contrôleur RAID sur le serveur, puis procédez à la configuration RAID à l'aide de l'outil de configuration du contrôleur RAID. Avec cette implémentation, la configuration RAID est masquée du système d'exploitation, mais les baies RAID sont exposées au système d'exploitation en tant que disques uniques. La seule configuration à effectuer dans le système d'exploitation est de créer des volumes sur les disques.

L'implémentation d'un volume RAID logiciel s'effectue en exposant tous les disques qui sont disponibles sur le serveur au système d'exploitation, puis en procédant à la configuration RAID dans le système d'exploitation. Windows Server 2012 prend en charge l'utilisation d'un volume RAID logiciel et vous pouvez utiliser l'outil de gestion des disques pour configurer plusieurs niveaux de RAID différents.

Lorsque vous choisissez d'implémenter un volume RAID matériel ou logiciel, tenez compte des éléments suivants :

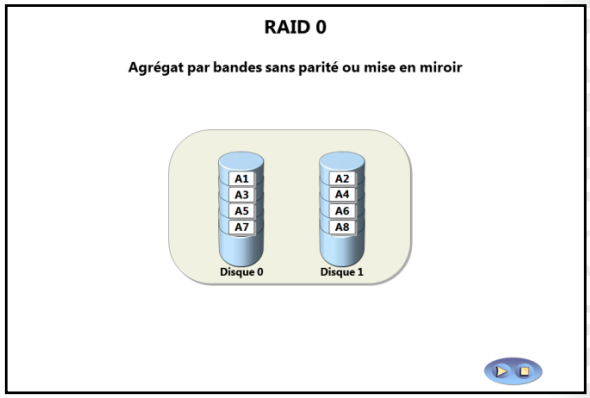
- Un volume RAID matériel requiert des contrôleurs de disque compatibles RAID. La plupart des contrôleurs de disque fournis avec de nouveaux serveurs disposent de cette fonctionnalité.
- Pour configurer un volume RAID matériel, vous devez accéder au programme de gestion de contrôleur de disque. Normalement, vous pouvez y accéder lors du processus de démarrage du serveur ou à l'aide d'une page Web exécutant un logiciel de gestion.
- L'implémentation de la mise en miroir des disques pour le disque contenant le système et le volume de démarrage avec le volume RAID logiciel peut nécessiter une configuration supplémentaire si un disque est défaillant. Dans la mesure où la configuration RAID est gérée par le système d'exploitation, vous devez configurer l'un des disques mis en miroir comme disque de démarrage. Si ce disque est défaillant, il se peut que vous deviez modifier la configuration de démarrage du serveur pour démarre ce dernier. Ce n'est pas un problème avec un volume RAID matériel, car le contrôleur de disque accède au disque disponible et l'expose au système d'exploitation.
- Sur les serveurs plus anciens, il est possible que vous obteniez de meilleures performances avec un volume RAID logiciel lorsque vous utilisez la parité, car le processeur de serveur peut calculer la parité plus rapidement que le contrôleur de disque. Ce n'est plus un problème avec les serveurs plus récents, lesquels vous permettent d'obtenir de meilleures performances étant donné que vous pouvez décharger les calculs de parité sur le contrôleur de disque.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Niveaux RAID

Lorsque vous implémentez la technologie RAID, vous devez décider du niveau à mettre en œuvre.

Le tableau ci-dessous présente les fonctionnalités pour chaque niveau RAID.



Niveau	Description	Performances	Espace utilisé	Redondance	Commentaires
RAID 0	Agrégat par bandes sans parité ou mise en miroir Les données sont écrites séquentiellement sur chaque disque	Performances élevées en lecture/écriture	La totalité de l'espace des disques est disponible	La défaillance d'un seul disque entraîne la perte de toutes les données	À utiliser seulement dans les situations où vous avez besoin de performances élevées et pouvez tolérer la perte de données
RAID 1	Agrégat mis en miroir sans parité ou agrégation par bandes Les données sont écrites sur les deux disques simultanément	Bonnes performances	Peut seulement utiliser la quantité d'espace qui est disponible sur le plus petit disque	Peut tolérer la défaillance d'un seul disque	Fréquemment utilisé pour les volumes système et de démarrage dotés de RAID matériel
RAID 2	Les données sont écrites en bits sur chaque disque avec la parité écrite sur un ou plusieurs disques distincts	Performances extrêmement élevées	Utilise un ou plusieurs disques pour la parité	Peut tolérer la défaillance d'un seul disque	Requiert que tous les disques soient synchronisés Non utilisé actuellement
RAID 3	Les données sont écrites en octets sur chaque disque avec la parité écrite sur un ou plusieurs disques distincts	Performances très élevées	Utilise un disque pour la parité	Peut tolérer la défaillance d'un seul disque	Requiert que tous les disques soient synchronisés Rarement utilisé

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Niveau	Description	Performances	Espace utilisé	Redondance	Commentaires
RAID 4	Les données sont écrites en blocs sur chaque disque avec la parité écrite sur un disque dédié	Bonnes performances en termes de lecture, performances médiocres en termes d'écriture	Utilise un disque pour la parité	Peut tolérer la défaillance d'un seul disque	Rarement utilisé
RAID 5	Agrégat par bandes avec parité distribuée Les données sont écrites en blocs sur chaque disque avec la parité répartie entre tous les disques	Bonnes performances en termes de lecture, performances médiocres en termes d'écriture	Utilise l'équivalent d'un disque pour la parité	Peut tolérer la défaillance d'un seul disque	Généralement utilisé pour le stockage des données lorsque les performances ne sont pas critiques, mais que l'optimisation de l'utilisation du disque est importante
RAID 6	Agrégat par bandes avec double parité distribuée Les données sont écrites en blocs sur chaque disque avec la double parité écrite sur tous les disques	Bonnes performances en termes de lecture, performances médiocres en termes d'écriture	Utilise l'équivalent de deux disques pour la parité	Peut tolérer les défaillances de deux disques	Généralement utilisé pour le stockage des données lorsque les performances ne sont pas critiques, mais que l'optimisation de l'utilisation du disque et la disponibilité sont importantes
RAID-0+1	Agrégats par bandes dans un agrégat mis en miroir Un ensemble de lecteurs est agrégé par bandes, puis l'agrégation par bandes est mise en miroir	Excellentes performances en lecture et écriture	Seule la moitié de l'espace disque est disponible en raison de la mise en miroir	Peut tolérer la défaillance d'au moins deux disques si tous les disques défectueux se trouvent dans le même agrégat par bandes	Utilisé peu fréquemment

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Niveau	Description	Performances	Espace utilisé	Redondance	Commentaires
RAID 1+0 (ou 10)	Agrégat mis en miroir dans un agrégat par bandes Plusieurs lecteurs sont mis en miroir dans un deuxième ensemble de lecteurs, puis un lecteur de chaque miroir est agrégé par bandes	Excellentes performances en lecture et écriture	Seule la moitié de l'espace disque est disponible en raison de la mise en miroir	Peut tolérer la défaillance d'au moins deux disques s'il ne s'agit pas de deux disques d'un même miroir	Fréquemment utilisé dans les scénarios où les performances et la redondance sont critiques, et le coût des disques supplémentaires requis acceptable
RAID 5+0 (ou 50)	Agrégat par bandes avec parité distribuée dans un agrégat par bandes Les lecteurs sont agrégés par bandes avec RAID 5, puis agrégés par bandes sans parité	Bonnes performances en termes de lecture et meilleures performances en termes d'écriture que RAID 5	L'équivalent d'au moins deux disques est utilisé pour la parité	Fournit une meilleure tolérance de pannes qu'un seul niveau RAID	Ce niveau est recommandé pour les applications qui requièrent des performances élevées en termes de tolérance de pannes, de capacité et de positionnement aléatoire Nécessite au moins six lecteurs

Remarque : Les niveaux RAID les plus courants sont RAID 1 (également appelé mise en miroir), RAID 5 (également appelé agrégat par bandes avec parité distribuée) et RAID 1+0 (également appelé agrégat en miroir dans un agrégat par bandes).

Question : Tous les disques doivent-ils être configurés avec la même quantité de tolérance de pannes ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Gestion des disques et des volumes

Le choix de la technologie de stockage que vous souhaitez déployer est la première étape critique à effectuer pour vous assurer que votre environnement répond aux impératifs de stockage des données. Toutefois, il s'agit seulement de la première étape. Vous devez également en effectuer d'autres dans le cadre de la préparation aux spécifications de stockage des données.

Par exemple, une fois que vous avez identifié la meilleure solution de stockage, ou que vous avez choisi une combinaison de solutions de stockage, vous devez trouver le meilleur moyen de gérer ce stockage. Posez-vous les questions suivantes :

- Quels disques allouerez-vous à un pool de stockage ?
- Le type de système de fichiers sera-t-il le même pour tous les disques ?

Ce cours aborde ces questions ainsi que d'autres questions semblables, notamment pourquoi il est important de gérer les disques et quels outils vous avez besoin pour les gérer.

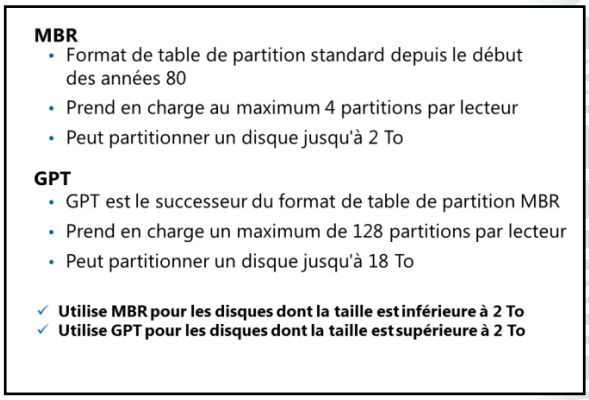
Objectifs de la leçon

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

- Expliquer comment sélectionner un format de table de partition.
- Décrire la différence entre un disque de base et un disque dynamique
- Expliquer comment sélectionner un système de fichiers.
- Décrire un système de fichiers résilient.
- Décrire des points de montage et des liens.
- Expliquer comment créer des points de montage et des liens.
- Décrire les processus d'extension et de réduction de volumes.

Sélection d'un format de table de partition

Un format de table de partition, ou *style de partition*, fait référence à la méthode qu'un système d'exploitation tel que Windows Server 2012 utilise pour organiser les partitions ou les volumes sur un disque. Pour les systèmes d'exploitation Windows, vous avez le choix entre un enregistrement de démarrage principal (MBR, Master Boot Record) ou une table de partition GUID (GPT, GUID Partition Table).



MBR

Le *format de table de partition MBR* est le mode de partitionnement standard utilisé sur les disques durs depuis l'apparition des premiers ordinateurs personnels dans les années 1980. Le format de table de partition MBR présente les caractéristiques suivantes :

- Une partition prend en charge un maximum de quatre partitions principales par lecteur.
- Une partition peut avoir un maximum de 2 téraoctets (To) (2,19 octets x 10^12 octets).
- Si vous initialisez un disque de plus de 2 To à l'aide du mode MBR, le disque stockera un volume maximal de 2 To et le reste du stockage ne sera pas utilisé. Vous devez convertir le disque au mode GPT si vous souhaitez utiliser l'intégralité de l'espace disponible.

Remarque : Utilisez le format de table de partition MBR pour les lecteurs de disques dont la taille ne dépasse jamais 2 To. Vous bénéficierez ainsi d'un peu plus d'espace, car le mode GPT requiert plus d'espace disque que le mode MBR. Cependant, Microsoft recommande de toujours utiliser le mode GPT dans la mesure du possible.

GPT

Le mode GPT a été introduit avec Windows Server 2003 et l'édition 64 bits de Windows XP afin de contourner les limitations de MBR et de répondre aux besoins des disques de plus grande capacité. Il présente les caractéristiques suivantes :

- GPT est le successeur du format de table de partition MBR.
- Le mode GPT prend en charge un maximum de 128 partitions par lecteur.
- Une partition peut contenir jusqu'à 8 zettaoctets (Zo).
- Un disque dur peut contenir jusqu'à 18 exaoctets (Eo), avec 512 kilo-octets (Ko) d'adressage de blocs logiques (LBA, Logical Block Addressing).
- Pour démarrer à partir d'une table de partition GPT, votre BIOS doit prendre en charge le mode GPT.

Remarque : Si votre disque dur fait plus de 2 To, vous devez utiliser le format de table de partition GPT.

Documentation supplémentaire : Pour consulter la Foire aux questions sur l'architecture du disque de table de partition GUID, voir http://go.microsoft.com/fwlink/?LinkID=266748.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sélection d'un type de disque

Lorsque vous sélectionnez un type de disque pour une utilisation dans Windows Server 2012, vous avez le choix entre des disques de base et des disques dynamiques.

Les disques de base sont
- Des disques initialisés pour le stockage de base
- Le système de stockage par défaut pour le système d'exploitation Windows

Les disques dynamiques peuvent
- Être modifiés sans redémarrage de Windows
- Proposer plusieurs options pour la configuration des volumes

Un volume de disque nécessite
- Un volume système pour les fichiers spécifiques au matériel qui sont nécessaires au démarrage du serveur
- Un volume de démarrage pour les fichiers du système d'exploitation Windows

Disque de base

Le stockage de base utilise des tables de partition normales utilisées par toutes les versions du système d'exploitation Windows. Un disque initialisé pour le stockage de base est appelé *disque de base*. Un disque de base contient des partitions de base, telles que des partitions principales et des partitions étendues. Vous pouvez subdiviser des partitions étendues en lecteurs logiques.

Par défaut, lorsque vous initialisez un disque dans le système d'exploitation Windows, ce disque est configuré en tant que disque de base. Vous pouvez facilement convertir des disques de base en disques dynamiques sans aucune perte de données. En revanche, si vous convertissez un disque dynamique en disque de base, toutes les données sur le disque seront perdues.

La conversion de disques de base en disques dynamiques ne procure aucun gain de performances, et certaines applications ne peuvent pas traiter les données qui sont stockées sur des disques dynamiques. C'est pourquoi la plupart des administrateurs ne convertissent pas les disques de base en disques dynamiques sauf s'ils doivent utiliser certaines des options de configuration de volume supplémentaires, disponibles avec les disques dynamiques.

Disque dynamique

Le stockage dynamique a été introduit dans le système d'exploitation Microsoft Windows 2000 Server. Un disque initialisé pour le stockage dynamique est appelé *disque dynamique*. Un disque dynamique contient des volumes dynamiques. Avec le stockage dynamique, vous pouvez gérer les disques et les volumes sans devoir redémarrer les ordinateurs exécutant des systèmes d'exploitation Windows.

Lorsque vous configurez des disques dynamiques, vous créez des volumes au lieu de partitions. Un *volume* est une unité de stockage constituée à partir d'espace disponible sur un ou plusieurs disques. Vous pouvez formater ce volume avec un système de fichiers et vous pouvez lui attribuer une lettre de lecteur ou le configurer avec un point de montage.

Liste des volumes dynamiques disponibles :

- *Volumes simples.* Un volume simple utilise l'espace disponible d'un seul disque. Cet espace peut être une seule région d'un disque ou être constitué de plusieurs régions concaténées. Un volume simple peut être étendu sur le même disque ou sur des disques supplémentaires. Si un volume simple est étendu sur plusieurs disques, il devient un volume fractionné.
- *Volumes fractionnés*. Un volume fractionné est créé à partir de l'espace disque disponible provenant de plusieurs disques. Vous pouvez étendre un volume fractionné sur un nombre maximal de 32 disques. Un volume fractionné ne peut pas être mis en miroir et ne tolère pas les pannes ; par conséquent, si vous perdez un disque, vous perdez l'intégralité du volume fractionné.

- *Volumes agrégés par bandes*. Un volume agrégé par bandes est un volume dont les données sont réparties sur au moins deux disques physiques. Les données présentes sur ce type de volume sont allouées successivement et uniformément à chacun des disques physiques. Un volume agrégé par bandes ne peut pas être mis en miroir ou étendu et il n'est pas tolérant aux pannes. Cela signifie que la perte d'un disque provoque la perte immédiate de toutes les données. L'agrégation par bandes est également appelée *RAID-0*.
- *Volumes en miroir*. Un volume en miroir est un volume à tolérance de pannes qui duplique les données sur deux disques physiques. Toute les données présentes sur un volume sont copiées sur un autre disque afin d'implémenter une redondance de données. Si l'un des disques est défaillant, les données sont encore accessibles à partir du disque restant. Un volume en miroir ne peut pas être étendu. La mise en miroir est également appelée *RAID-1*.
- *Volumes RAID-5*. Un volume RAID-5 est un volume à tolérance de pannes dont les données sont agrégées par bandes sur au moins trois disques. La parité est également agrégée par bandes sur la baie de disques. Si un disque physique est défaillant, la partie du volume RAID-5 qui se trouvait sur ce disque défaillant peut être recréée à partir des données restantes et de la parité. Un volume RAID-5 ne peut pas être mis en miroir ou étendu.

Volumes de disque requis

Quel que soit le type de disque que vous utilisez, vous devez configurer un volume système et un volume de démarrage sur un des disques durs du serveur :

- *Volumes système*. Le volume système contient les fichiers propres au matériel qui sont nécessaires pour charger le système d'exploitation Windows (par exemple, Bootmgr et BOOTSECT.bak). Le volume système peut être le même volume que le volume de démarrage. Ce n'est toutefois pas obligatoire.
- *Volumes de démarrage*. Le volume de démarrage contient les fichiers du système d'exploitation Windows qui sont situés dans les dossiers %Systemroot% et %Systemroot%\System32. Le volume de démarrage peut être le même volume que le volume système. Ce n'est toutefois pas obligatoire.

Remarque : Lorsque vous installez le système d'exploitation Windows 8 ou Windows Server 2012 dans une nouvelle installation, un volume système distinct est créé pour autoriser le chiffrement du volume de démarrage à l'aide du chiffrement de lecteur Windows BitLocker®.

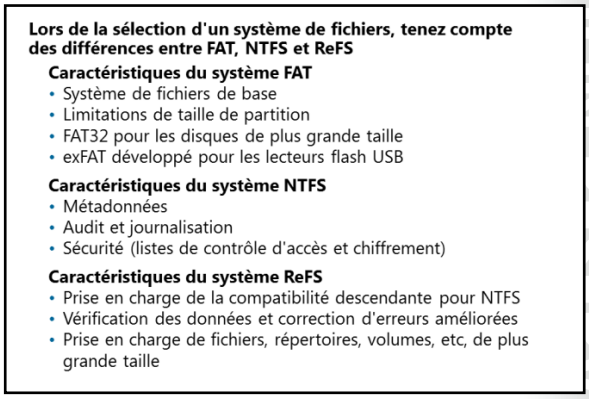
Documentation supplémentaire :

- Pour plus d'informations sur le fonctionnement des disques et volumes de base, voir http://go.microsoft.com/fwlink/?LinkID=199648.
- Pour plus d'informations sur le fonctionnement des disques et volumes dynamiques, voir http://go.microsoft.com/fwlink/?LinkID=199649.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Choix d'un système de fichiers

Lorsque vous configurez vos disques dans Windows Server 2012, vous pouvez choisir entre la table d'allocation des fichiers (FAT), le système de fichiers NTFS, et les systèmes de fichiers ReFS.



FAT

Le système de fichiers FAT est le plus simple des systèmes de fichiers pris en charge par les systèmes d'exploitation Windows. Le système de fichiers FAT est caractérisé par une table qui réside dans la partie supérieure du volume. Afin de protéger le volume, deux copies du système de fichiers FAT sont conservées au cas où l'une d'elles serait endommagée. En outre, les tables d'allocation des fichiers et le répertoire racine doivent être stockées dans un emplacement fixe afin que les fichiers de démarrage du système puissent être correctement localisés.

Un disque formaté avec le système de fichiers FAT est alloué en clusters, dont la taille est déterminée par la taille du volume. Lorsqu'un fichier est créé, une entrée est également créée dans le répertoire et le numéro du premier cluster contenant des données est établi. Cette entrée dans la table indique qu'il s'agit du dernier cluster du fichier, ou qu'elle pointe vers le cluster suivant. Aucune organisation ne régit la structure de répertoires FAT, et les fichiers se voient octroyer le premier emplacement ouvert sur le lecteur.

En raison de la limitation de taille avec la table d'allocation des fichiers, la version originale de FAT pouvait uniquement accéder aux partitions dont la taille était inférieure à 2 Go. Pour accéder aux disques de plus grande capacité, Microsoft a développé FAT32. FAT32 prend en charge les partitions de taille inférieure ou égale à 2 To.

FAT ne fournit aucune sécurité pour les fichiers qui se trouvent sur la partition. N'utilisez jamais FAT ou FAT32 comme système de fichiers pour les disques connectés aux serveurs Windows Server 2012. L'utilisation de FAT ou FAT32 peut être envisagée pour formater des medias externes tels que des supports flash USB.

Le système FAT étendue (exFAT) est un système de fichiers conçu spécialement pour les lecteurs flash. Il peut être utilisé lorsque FAT32 n'est pas approprié, par exemple lorsque vous avez besoin d'un format de disque fonctionnant avec un téléviseur, qui requiert un disque de plus de 2 To. Plusieurs périphériques multimédias prennent en charge exFAT, comme les écrans plats des téléviseurs actuels, les centres multimédias et les lecteurs multimédias portables.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

NTFS

NTFS est le système de fichiers standard pour tous les systèmes d'exploitation Windows à partir de Windows NT® Server 3.1. À la différence de FAT, le disque ne contient aucun objet spécial et il n'existe aucune dépendance vis-à-vis du matériel sous-jacent, comme des secteurs de 512 octets. En outre, NTFS n'utilise aucun emplacement spécial sur le disque, tel que les tables.

NTFS est une amélioration de FAT à plusieurs égards. Il offre notamment une meilleure prise en charge des métadonnées et l'utilisation de structures de données avancées permettant d'améliorer les performances, la fiabilité et l'utilisation de l'espace disque. NTFS comporte également des extensions supplémentaires telles que des listes de contrôle d'accès (ACL) de sécurité, que vous pouvez utiliser pour l'audit, la journalisation des systèmes de fichiers et le chiffrement.

NTFS est requis pour plusieurs rôles et fonctionnalités de Windows Server 2012 tel que les services de domaine Active Directory® (AD DS), les services VSS (Volume Shadow Services), le système de fichiers distribués (DFS) et les services de réplication de fichiers (FRS). NTFS offre un niveau de sécurité beaucoup plus élevé que FAT ou FAT 32.

Système ReFS (Resilient File System)

Ce système a été introduit avec Windows Server 2012 pour améliorer les fonctionnalités de NTFS. ReFS a été développé pour améliorer NTFS grâce à des capacités maximales plus importantes pour les fichiers individuels, les répertoires, les volumes de disque et d'autres éléments. En outre, ReFS offre une résilience supérieure, ce qui signifie une meilleure vérification des données, correction des erreurs et évolutivité.

Utilisez ReFS avec les volumes très importants et les partages de fichier très volumineux de manière à éviter la limitation de NTFS en matière de vérification et de correction des erreurs. Dans la mesure où ReFS n'était pas disponible avant Windows Server 2012 (le seul choix était NTFS), il est conseillé d'utiliser ReFS, et non NTFS, avec Windows Server 2012 afin de bénéficier d'une meilleure vérification des erreurs, d'une plus grande fiabilité et d'un endommagement minimal.

Documentation supplémentaire :

- Pour plus d'informations sur le fonctionnement de FAT, voir http://go.microsoft.com/fwlink/?LinkID=199652.
- Pour plus d'informations sur le fonctionnement de NTFS, voir http://go.microsoft.com/fwlink/?LinkID=199654.

Question : Quel système de fichiers utilisez-vous actuellement sur votre serveur de fichiers ? Continuerez-vous à l'utiliser ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que le système de fichiers ReFS ?

ReFS est une nouvelle fonctionnalité dans Windows Server 2012. Ce système est basé sur le système de fichiers NTFS et offre les avantages suivants :

- Intégrité des métadonnées avec sommes de contrôle
- Protection étendue contre l'endommagement des données
- Optimisation de la fiabilité, particulièrement lors d'une panne d'alimentation (NTFS est connu pour endommager des données dans des circonstances semblables)

ReFS est un nouveau système de fichiers intégré à Windows Server 2012. Il présente les avantages suivants

- Intégrité des métadonnées avec sommes de contrôle
- Flux d'intégrité avec intégrité des données utilisateur
- Modèle transactionnel d'allocation à l'écriture
- Tailles importantes de volumes, fichier et répertoire (2^78 avec une taille de cluster de 16 Ko)
- Pool de stockage et virtualisation
- Répartition des données pour performances et redondance
- Nettoyage des disques pour les protéger contre les erreurs de disque latentes
- Résilience aux dommages avec récupération
- Pools de stockage partagés sur les ordinateurs

- Grandes tailles de volumes, de fichiers et de répertoires
- Pool de stockage et virtualisation, qui simplifient la création et la gestion des systèmes de fichiers
- Agrégation par bandes des données pour de meilleures performances (la bande passante peut être gérée)
- Redondance de la tolérance de pannes
- Nettoyage des disques pour les protéger contre les erreurs de disque latentes
- Résilience aux dommages avec récupération pour une disponibilité maximale des volumes
- Pools de stockage partagés sur les ordinateurs pour une tolérance de pannes et un équilibrage de la charge supplémentaires.

Le système ReFS hérite de certaines fonctionnalités de NTFS, notamment les fonctionnalités suivantes :

- Chiffrement de lecteur BitLocker
- Listes de contrôle d'accès pour la sécurité
- Journal du nombre de séquences de mise à jour (USN, Update Sequence Number)
- Notifications de modification
- Liens symboliques, points de jonction, points de montage et points d'analyse
- Captures instantanées de volume
- Identificateurs de fichier

Étant donné que ReFS utilise un sous-ensemble des fonctionnalités de NTFS, il est conçu pour conserver une compatibilité descendante avec NTFS. Par conséquent, les applications qui s'exécutent sur Windows Server 2012 peuvent accéder à des fichiers sur ReFS comme elles le feraient sur NTFS. Toutefois, un lecteur au format ReFS n'est pas reconnu lorsqu'il se trouve dans des ordinateurs exécutant des systèmes d'exploitation Windows Server antérieurs à Windows Server 2012.

Avec NTFS, vous pouvez modifier la taille d'un cluster ; en revanche, avec ReFS, chaque cluster a une taille fixe de 64 Ko, que vous ne pouvez pas modifier. Le système de fichiers chiffrés (EFS, Encrypted File System) n'est pas pris en charge dans ReFS.

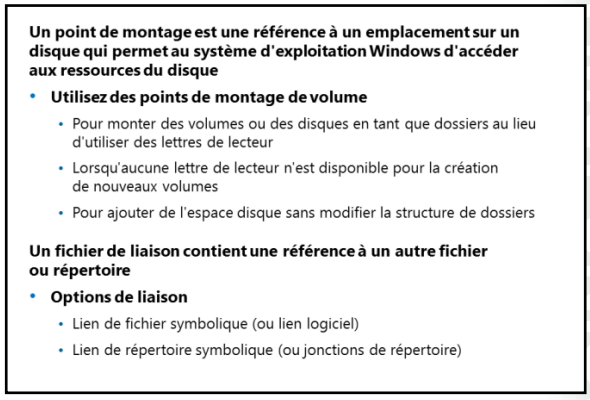
Comme l'indique son nom, le nouveau système de fichiers offre une résilience accrue, ce qui signifie une meilleure vérification des données, correction des erreurs et évolutivité.

Outre sa résilience supérieure, ReFS surpasse également NTFS en offrant des tailles maximales supérieures pour les différents fichiers, répertoires, volumes de disque et d'autres éléments, qui sont répertoriés dans le tableau ci-dessous.

Attribut	Limite
Taille maximale d'un fichier unique	Approximativement 16 Eo (18.446.744.073.709.551.616 octets)
Taille maximale d'un volume unique	2^78 octets avec une taille de cluster de 16 Ko (2^64 * 16 * 2^10) L'adressage de pile Windows autorise 2^64 octets
Nombre maximal de fichiers dans un répertoire	2^64
Nombre maximal de répertoires dans un volume	2^64
Longueur maximale d'un nom de fichier	32 000 caractères Unicode
Longueur maximale d'un chemin d'accès	32,000
Taille maximale d'un pool de stockage	4 pétaoctets (Po)
Nombre maximal de pools de stockage dans un système	Aucune limite
Nombre maximal d'espaces dans un pool de stockage	Aucune limite

Que sont les points de montage et les liens ?

Avec les systèmes NTFS et ReFS, vous pouvez créer des points de montage et des liens de manière à ce qu'ils fassent référence à des fichiers, des répertoires et des volumes.



Points de montage

Les points de montage sont utilisés dans les systèmes d'exploitation Windows pour rendre une partie ou la totalité d'un disque utilisable par le système d'exploitation. Généralement, les points de montage sont associés à des mappages de lettres de lecteur de sorte que le système d'exploitation puisse accéder au disque via la lettre de lecteur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Depuis l'introduction de Windows 2000 Server, vous pouvez activer des points de montage de volume, que vous pouvez ensuite utiliser pour monter un disque dur sur un dossier vide situé sur un autre lecteur. Par exemple, si vous ajoutez un nouveau disque dur sur un serveur, plutôt que de monter le lecteur en utilisant une lettre de lecteur, vous pouvez attribuer un nom de dossier tel que C:\datadrive au lecteur. Lorsque vous procédez ainsi, chaque fois que vous accédez au dossier C:\datadrive, vous accédez en réalité au nouveau disque dur.

Les points de montage de volume peuvent être utiles dans les scénarios suivants :

- Lorsque l'espace disque devenant insuffisant sur un serveur, vous souhaitez en ajouter sans modifier l'arborescence. Vous pouvez ajouter le disque dur et configurez un dossier de manière à ce qu'il pointe vers le disque dur.
- Lorsque vous êtes à court de lettres disponibles à attribuer aux partitions ou aux volumes. Si vous avez plusieurs disques durs connectés au serveur, vous pouvez manquer de lettres disponibles dans l'alphabet pour attribuer des lettres de lecteur. À l'aide d'un point de montage de volume, vous pouvez ajouter des partitions ou des volumes supplémentaires sans utiliser plus de lettres de lecteur.
- Lorsque vous devez séparer les entrées/sorties de disque (E/S) dans une arborescence. Par exemple, si vous utilisez une application qui requiert une structure de fichier spécifique, mais qui utilise les disques durs de manière intensive, vous pouvez séparer l'E/S de disque en créant un point de montage de volume dans l'arborescence.

Remarque : Vous pouvez attribuer des points de montage de volume uniquement aux dossiers vides sur une partition NTFS. Cela signifie que si vous souhaitez utiliser un nom du dossier existant, vous devez d'abord renommer ce dossier, créer et monter le disque dur en utilisant le nom du dossier requis, puis copier les données sur le dossier monté.

Liens

Un *lien* est un type particulier de fichier qui contient une référence à un autre fichier ou répertoire sous la forme d'un chemin d'accès relatif ou absolu. Windows prend en charge les deux types de lien suivants :

- Un lien de fichier symbolique (également appelé *lien logiciel*)
- Un lien de répertoire symbolique (également appelé *jonction de répertoire*)

Un lien stocké sur un partage de serveur pourrait renvoyer à un répertoire figurant sur un client non réellement accessible à partir du serveur sur lequel le lien est stocké. Dans la mesure où le traitement de lien est effectué à partir du client, le lien fonctionnerait correctement pour accéder au client, bien que le serveur ne puisse pas accéder au client.

Les liens fonctionnent d'une manière transparente. Les applications qui lisent ou écrivent dans des fichiers nommés par un lien se comportent comme si elles fonctionnaient directement sur le fichier cible. Par exemple, vous pouvez utiliser un lien symbolique vers un fichier de disque dur virtuel parent Hyper-V® (.vhd) à partir d'un autre emplacement. Hyper-V utilise le lien pour travailler avec le disque dur virtuel parent (VHD) comme il le ferait avec le fichier d'origine. L'avantage d'utiliser des liens symboliques est que vous n'avez pas besoin de modifier les propriétés de votre disque dur virtuel de différenciation.

Remarque : Dans Hyper-V, vous pouvez utiliser un disque dur virtuel (VHD) de différenciation pour économiser de l'espace en appliquant les modifications au disque dur virtuel enfant uniquement, lorsque le disque dur virtuel enfant fait partie d'une relation de disque dur virtuel parent/enfant.

Les liens sont parfois plus facile gérer que les points de montage. Les points de montage vous forcent à placer les fichiers à la racine des volumes, tandis que les liens vous permettent plus de flexibilité quant à l'emplacement où vous enregistrez les fichiers.

Vous pouvez créer des liens à l'aide de la commande mklink dans l'application Invite de commandes.

Démonstration : Création de points de montage et de liens

Dans cette démonstration, vous allez apprendre à :

- créer un point de montage ;
- créer une jonction de répertoire pour un dossier ;
- créer un lien physique pour un fichier.

Procédure de démonstration

Créer un point de montage

1. Ouvrez une session sur **LON-SVR1** avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Ouvrez **Gestion de l'ordinateur**, puis développez **Gestion des disques**.
3. Dans Gestion des disques, initialisez **Disque 2** avec **Partition GPT (GUID Partition Table)**.
4. Sur Disque 2, créez un volume simple avec les paramètres suivants :
   - Taille : **4000** Mo
   - **Ne pas attribuer de lettre de lecteur ni de chemin d'accès de lecteur**
   - Système de fichiers : **NTFS**
   - Nom de volume : **MountPoint**
5. Attendez que le volume soit créé, cliquez avec le bouton droit sur **MountPoint**, puis cliquez sur **Modifier la lettre de lecteur et le chemin d'accès**.
6. Changez la lettre de lecteur comme suit :
   - **Monter dans le dossier NTFS vide suivant**
   - Créez le dossier **C:\MountPointFolder** et utilisez-le comme point de montage.
7. Dans la barre des tâches, ouvrez une fenêtre de l'Explorateur de fichiers, puis cliquez sur **Disque local (C:)**. Vous devriez maintenant voir le dossier MountPoint avec une taille de 4 095 996 Ko. Vous pouvez voir l'icône attribuée au point de montage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Créer une jonction de répertoire pour un dossier

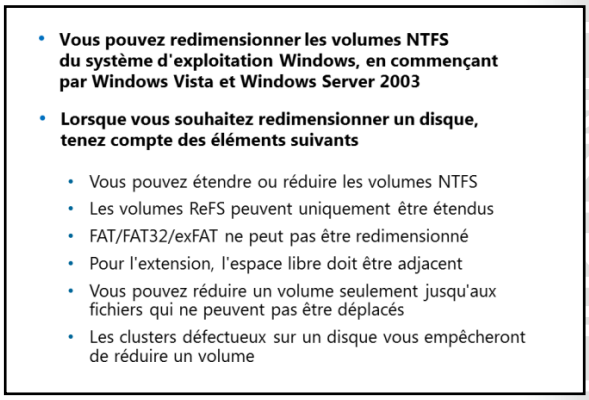
1. Ouvrez une fenêtre d'invite de commandes.
2. Créez un dossier dans C:\ appelé **CustomApp** et exécutez la commande suivante : **copy C:\windows\system32\notepad.exe C:\CustomApp**.
3. À l'invite de commandes, tapez **mklink /j AppLink CustomApp**, puis appuyez sur Entrée.
4. Dans une fenêtre de l'Explorateur de fichiers, accédez à **C:\AppLink**. Remarquez que comme il s'agit d'un lien, le chemin du répertoire dans la barre d'adresses n'est pas mis à jour avec C:\CustomApp.

Créer un lien physique pour un fichier

1. À partir d'une invite de commandes, tapez **mklink /h C:\AppLink\Notepad2.exe C:\AppLink\Notepad.exe**.
2. Dans l'Explorateur de fichiers, remarquez que Notepad2.exe s'affiche exactement comme Notepad.exe. Les deux noms de fichier pointent vers le même fichier.

Extension et réduction de volumes

Dans les versions de Windows antérieures à Windows Server 2008 ou Windows Vista®, vous aviez besoin de logiciels supplémentaires pour réduire ou étendre un volume sur votre disque. Depuis Windows Server 2008 et Windows Vista, cette fonctionnalité est comprise dans le système d'exploitation Windows et vous pouvez utiliser le composant logiciel enfichable de gestion des disques pour redimensionner des volumes NTFS.



Lorsque vous souhaitez redimensionner un volume, vous devez prendre en compte les éléments suivants :

- Vous pouvez uniquement réduire ou étendre des volumes NTFS. Les volumes FAT, FAT32 ou exFAT ne peuvent pas être redimensionnés.
- Vous pouvez uniquement étendre des volumes ReFS, vous ne pouvez pas les réduire.
- Vous pouvez étendre un volume en utilisant l'espace libre se trouvant sur le même disque et sur d'autres disques. Lorsque vous étendez un volume avec d'autres disques, vous créez un disque dynamique avec un volume fractionné. Si un disque d'un volume fractionné subit une défaillance, toutes les données du volume sont perdues. En outre, un volume fractionné ne peut pas contenir de partitions de démarrage ou de partitions système. Vous ne pouvez donc pas étendre vos partitions de démarrage à l'aide d'un autre disque.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Si des clusters défectueux existent sur la partition, vous ne pouvez pas la réduire.
- Lorsque vous souhaitez réduire une partition, les fichiers fixes, tels que les fichiers d'échange, ne sont pas relocalisés. Autrement dit, vous ne pouvez pas récupérer d'espace au delà de l'emplacement où se trouvent ces fichiers sur le volume. Si vous avez besoin de réduire davantage une partition, vous devez supprimer ou déplacer les fichiers fixes. Par exemple, vous pouvez supprimer le fichier d'échange, réduire le volume, puis ajouter à nouveau le fichier d'échange.

Remarque : Dans la mesure du possible, pour réduire des volumes, défragmentez les fichiers sur ces volumes avant de réduire ces derniers. Cette méthode renvoie la quantité maximale d'espace disque libre. Durant le processus de défragmentation, vous pouvez identifier tous les fichiers fixes.

Pour modifier un volume, vous pouvez utiliser les outils Gestion des disques, Diskpart.exe, ou l'applet de commande **Resize-Partition** dans Windows PowerShell®.

Documentation supplémentaire :

- Pour plus d'informations sur la manière d'étendre un volume de base, voir http://go.microsoft.com/fwlink/?LinkID=266749.
- Pour plus d'informations sur la manière de réduire un volume de base, voir http://go.microsoft.com/fwlink/?LinkID=266750.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Implémentation d'espaces de stockage

La gestion des disques physiques connectés directement à un serveur s'est révélée être une tâche pénible pour les administrateurs. Pour surmonter ce problème, de nombreuses organisations utilisent des réseaux SAN qui, pour l'essentiel, regroupent des disques physiquement.

Les réseaux SAN nécessitent une configuration et parfois du matériel spécifiques. Ils sont donc chers. Pour surmonter ces problèmes, vous pouvez utiliser Espaces de stockage, qui est une fonctionnalité de Windows Server 2012 rassemblant les disques en pools et les présentant au système d'exploitation comme un disque unique. Cette leçon explique comment configurer et implémenter la fonctionnalité Espaces de stockage.

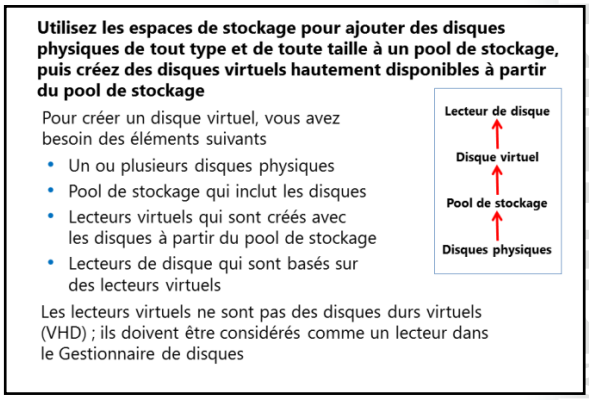
Objectifs de la leçon

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

- Décrire la fonctionnalité Espaces de stockage.
- Décrire les diverses options pour configurer les disques virtuels.
- Décrire les options de gestion avancée pour les espaces de stockage.
- Configurer des espaces de stockage.

Qu'est-ce que la fonctionnalité Espaces de stockage ?

Espaces de stockage est une fonctionnalité de virtualisation de stockage intégrée à Windows Server 2012 et Windows 8. Il s'agit d'une fonctionnalité disponible pour les volumes NTFS et ReFS, pouvant assurer la redondance et fournir un pool de stockage à différents disques internes et externes de différentes tailles et interfaces. Vous pouvez utiliser cette fonctionnalité pour ajouter des disques physiques de tout type et de toute taille à un pool de stockage, puis créer des disques virtuels hautement disponibles à partir du pool de stockage. L'avantage principal des espaces de stockage est que vous ne gérez pas de disques uniques, mais que vous pouvez gérer plusieurs disques comme une seule unité.



Pour créer un disque virtuel hautement disponible, vous devez disposer des éléments suivants :

- Lecteur de disque. Il s'agit d'un volume auquel vous pouvez accéder à partir de votre système d'exploitation Windows, par exemple, à l'aide d'une lettre de lecteur.
- Disque virtuel (ou espace de stockage). Ce disque est semblable à un disque physique pour les utilisateurs et les applications. Mais les disques virtuels sont plus souples car ils comprennent l'allocation dynamique (ou les allocations juste-à-temps) et la résilience aux défaillances de disque physique avec une fonctionnalité intégrée, par exemple la mise en miroir.

- Pool de stockage. Un pool de stockage est une collection d'un ou plusieurs disques physiques que vous pouvez utiliser pour créer des disques virtuels. Vous pouvez ajouter à un pool de stockage tout disque physique disponible qui n'est pas formaté ou connecté à un autre pool de stockage.
- Disque physique. Les disques physiques sont des disques tels que les disques SATA ou SAS. Pour être ajoutés à un pool de stockage, les disques physiques doivent répondre aux conditions suivantes :
  - Un disque physique est requis pour créer un pool de stockage. Au moins deux disques physiques sont requis pour créer un disque virtuel en miroir résilient.
  - Au moins trois disques physiques sont requis pour créer un disque virtuel avec une résilience par parité.
  - La mise en miroir triple requiert au moins cinq disques physiques.
  - Les disques doivent être vierges et non formatés. Ils ne doivent contenir aucun volume.
  - Les disques peuvent être connectés à l'aide de diverses interfaces de bus, notamment SAS, SATA, SCSI et USB. Si vous souhaitez utiliser le clustering avec basculement avec des pools de stockage, vous ne pouvez pas utiliser de disques SATA, USB ou SCSI.

Options de configuration des disques virtuels

Vous pouvez créer des disques virtuels à partir de pools de stockage. Si votre pool de stockage contient plus d'un disque, vous pouvez également créer les disques virtuels redondants. Pour configurer des disques virtuels ou des espaces de stockage dans le Gestionnaire de serveur ou dans Windows PowerShell, vous devez tenir compte des fonctionnalités suivantes et de leurs fonctionnalités de redondance.

Fonctionnalité	Options
Disposition du stockage	• Simple • Miroir bidirectionnels ou tridirectionnel • Parité
Taille des secteurs de disque	• 512 ou 512e
Allocation de lecteurs	• Magasin de données • Manuel • Échange à chaud

Disposition du stockage

Cette fonctionnalité définit le nombre de disques du pool de stockage qui sont alloués. Les options valides sont les suivantes :

- Simple. Un espace simple utilise l'agrégation par bandes des données mais pas la redondance. Dans l'agrégation par bandes des données, les données logiquement séquentielles sont segmentées sur tous les disques de façon à permettre aux différents disques de stockage physiques d'accéder à ces segments séquentiels. L'agrégation par bandes permet d'accéder simultanément à plusieurs segments de données. N'hébergez des données importantes sur un volume simple, car il ne fournit pas de fonctionnalités de basculement lorsque le disque sur lequel les données sont stockées subit une défaillance.
- Miroirs doubles et triples. Les espaces en miroir gèrent deux ou trois copies des données qu'ils hébergent (deux copies de données pour les miroirs doubles et trois copies de données pour les miroirs triples). La duplication se produit avec chaque écriture de manière à s'assurer que toutes les copies de données sont actualisées en permanence. Les espaces en miroir répartissent aussi les données sur différents disques physiques. Ils offrent l'avantage d'un débit de données élevé et d'une faible latence d'accès. Ils ne présentent également aucun risque d'endommagement des données au repos et ne nécessitent pas de phase de journalisation supplémentaire lors de l'écriture des données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Parité. Un espace à parité est semblable à RAID 5. Les données et les informations de parité sont agrégées par bandes sur plusieurs disques physiques. La parité permet aux espaces de stockage de continuer à traiter les demandes de lecture et d'écriture même si un disque est défectueux. Elle fait toujours une rotation entre les disques disponibles pour optimiser les E/S. Les espaces de stockage requièrent au moins trois disques physiques pour les espaces à parité. Les espaces à parité ont augmenté la résilience via la journalisation.

Taille des secteurs de disque

La taille de secteur d'un pool de stockage est définie lors de la création du pool de stockage. Si la liste des lecteurs utilisés ne contient que des lecteurs 512 et/ou 512e, la valeur par défaut attribuée au pool est 512e. Un lecteur 512 utilise des secteurs de 512 octets. Un lecteur 512e est un disque dur comportant des secteurs de 4 096 octets qui émule des secteurs de 512 octets. Si la liste contient au moins un disque de 4 Ko, la taille de secteur du pool est définie par défaut sur 4 Ko. Un administrateur peut éventuellement définir explicitement la taille de secteur héritée par tous les espaces contenus dans le pool. Une fois qu'un administrateur a défini la taille de secteur, le système d'exploitation Windows vous autorise uniquement à ajouter des lecteurs qui ont une taille de secteur conforme, c'est-à-dire : 512 ou 512e pour un pool de stockage 512e, et 512, 512e ou 4 Ko pour un pool de 4 Ko.

Allocation de lecteurs

Les paramètres ci-dessous définissent l'allocation du disque au pool. Les options sont les suivantes :

- *Automatique*. Il s'agit de l'allocation par défaut lorsque un disque est ajouté à un pool. Les espaces de stockage peuvent sélectionner automatiquement la capacité disponible sur les disques des magasins de données, à la fois pour la création d'espace de stockage et pour l'allocation juste-à-temps.
- *Échange à chaud*. Les disques ajoutés à un pool en tant que disques d'échange à chaud sont des disques de réserve qui ne sont pas utilisés pour la création d'un espace de stockage. Si une défaillance se produit sur un disque qui héberge les colonnes d'un espace de stockage, un disque de réserve est invité à remplacer ce disque défectueux.

Modèles d'approvisionnement

Vous pouvez approvisionner un disque virtuel à l'aide de l'un ou l'autre des modèles suivants :

- *Espace à allocation dynamique*. L'allocation dynamique est un mécanisme qui permet à un stockage d'être alloué facilement sur la base du juste assez et du juste-à-temps. La capacité de stockage du pool est organisée en sections d'approvisionnement qui ne sont pas allouées tant que la taille des groupes de données ne nécessite pas de stockage. Contrairement à la méthode d'allocation de stockage fixe classique dans laquelle de grands pools de capacité de stockage sont alloués mais peuvent rester inutilisés, l'allocation dynamique optimise l'utilisation du stockage disponible. Les organisations peuvent aussi réduire les frais d'exploitation, tels que l'électricité et la surface occupée liées au fonctionnement de disques inutilisés. L'allocation dynamique offre toutefois des performances de disque inférieures.
- *Espace à allocation fixe*. Avec les espaces de stockage, les espaces à allocation fixe utilisent également les sections d'approvisionnement flexible. La différence entre l'allocation dynamique et un espace à allocation fixe est que la capacité de stockage dans l'espace d'allocation fixe est allouée au moment où l'espace est créé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration requise pour un disque de cluster

Le clustering avec basculement empêche l'interruption des charges de travail ou des données en cas de défaillance d'un ordinateur. Pour qu'un pool prenne en charge le basculement, le clustering de tous les disques attribués doit prendre en charge un protocole multi-initiateurs, par exemple SAS.

Remarque : Vous pouvez utiliser les espaces de stockage pour créer des disques virtuels à allocation dynamique et à allocation fixe dans le même pool de stockage. Le fait de disposer des deux types d'allocation dans le même pool de stockage est pratique, en particulier lorsqu'ils concernent la même charge de travail. Par exemple, vous pouvez choisir d'avoir un espace à allocation dynamique pour héberger une base de données et un espace à allocation fixe pour héberger son journal.

Question : Quel est le nom d'un disque virtuel qui est plus grand que la quantité d'espace disque disponible sur la partie disques physiques du pool de stockage ?

Options de gestion avancée pour les espaces de stockage

Le Gestionnaire de serveur effectue une gestion de base des disques virtuels et des pools de stockage. Il vous permet de créer des pools de stockage, d'ajouter et supprimer des disques physiques des pools, et de créer, gérer et supprimer des disques virtuels. Par exemple, le Gestionnaire de serveur vous permet d'afficher les disques physiques liés à un disque virtuel. Si l'un de ces disques est défectueux, vous verrez une icône représentant un disque défectueux en regard du nom de ce disque.

- La gestion de base pour les espaces de stockage est disponible dans le Gestionnaire de serveurs
- En cas de défaillance du disque
  - N'utilisez pas chkdsk ou l'analyse de disque
  - Remplacez le lecteur par un nouveau
- La gestion avancée a besoin de Windows PowerShell

Applet de commande Windows PowerShell	Description
Get-StoragePool	Liste des pools de stockage
Repair-VirtualDisk	Réparation d'un disque virtuel
Get-PhysicalDisk | Where{$_.HealthStatus -ne "Healthy"}	Liste des disques physiques défectueux
Reset-PhysicalDisk	Retrait d'un disque physique d'un pool de stockage
Get-VirtualDisk | Get-PhysicalDisk	Liste des disques physiques utilisés pour un disque virtuel

Pour corriger un disque défectueux dans un disque virtuel ou un pool de stockage, vous devez supprimer le disque qui provoque le problème. Les outils de défragmentation, d'analyse de disque, ou **chkdsk** ne peuvent pas réparer un pool de stockage. Pour remplacer un disque défectueux, vous devez ajouter un nouveau disque au pool. Le nouveau disque se resynchronise automatiquement au cours de la maintenance du disque qui a lieu lors de la maintenance quotidienne. Vous pouvez également déclencher la maintenance du disque manuellement.

Windows PowerShell fournit des options de gestion avancée pour les disques virtuels et les pools de stockage. Le tableau ci-dessous contient des exemples d'applets de commande de gestion.

Applet de commande Windows PowerShell	Description
Get-StoragePool	Répertorie les pools de stockage
Get-VirtualDisk	Répertorie les disques virtuels
Repair-VirtualDisk	Répare un disque virtuel

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Applet de commande Windows PowerShell	Description
Get-PhysicalDisk | Where{$_.HealthStatus –ne "Healthy"}	Répertorie les disques physiques défectueux
Reset-PhysicalDisk	Supprime un disque physique d'un pool de stockage
Get-VirtualDisk | Get-PhysicalDisk	Répertorie les disques physiques utilisés pour un disque virtuel

Documentation supplémentaire : Pour en savoir plus sur les applets de commande de stockage dans Windows PowerShell, voir http://go.microsoft.com/fwlink/?LinkID=266751.

Démonstration : Configuration d'espaces de stockage

Dans cette démonstration, vous allez apprendre à :

- créer un pool de stockage ;
- créer un disque virtuel et un volume.

Procédure de démonstration

Créer un pool de stockage

1. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-SVR1, dans le Gestionnaire de serveur, accédez à **Service de fichiers et de stockage**, et **Pools de stockage**.
3. Dans le volet POOLS DE STOCKAGE, créez un **Nouveau pool de stockage** nommé **StoragePool1**, puis ajoutez tous les disques disponibles.

Créer un disque virtuel et un volume

1. Dans le volet DISQUES VIRTUELS, créez un **Nouveau disque virtuel** avec les paramètres suivants :
   - Pool de stockage : **StoragePool1**
   - Nom du disque : **vDisk simple**
   - Disposition du stockage : **simple**
   - Type d'approvisionnement : **Fin**
   - Taille : **2 Go**
2. Sur la page **Afficher les résultats**, attendez que la tâche se termine, puis assurez-vous que la case à cocher **Créez un volume lorsque l'Assistant se ferme** est activée.
3. Dans l'Assistant Nouveau volume, créez un volume avec les paramètres suivants :
   - Disque virtuel : **vDisk simple**
   - Système de fichiers : **ReFS**
   - Nom de volume : **volume simple**
4. Attendez que la tâche soit terminée, puis cliquez sur **Fermer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation d'un système de stockage local

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

Vous avez travaillé pour A. Datum pendant plusieurs années en tant que spécialiste du support technique. Votre fonction consistait à examiner les ordinateurs de bureau pour résoudre les problèmes d'application et les problèmes réseau. Vous avez récemment accepté une promotion au sein de l'équipe d'assistance technique des serveurs. L'une de vos premières missions consiste à configurer le service d'infrastructure pour une nouvelle filiale.

Votre responsable vous a demandé d'ajouter de l'espace disque sur un serveur de fichiers. Après la création des volumes, votre responsable vous a également demandé de redimensionner ces volumes en fonction des dernières informations dont il dispose. Enfin, vous devez rendre le stockage des données redondant en créant un disque virtuel en miroir triple.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- Installer et configurer un nouveau disque.
- Redimensionner des volumes.
- Configurer un espace de stockage redondant.

Configuration de l'atelier pratique

Durée approximative : 30 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-SVR1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.

1. Dans le Gestionnaire Hyper-V, cliquez sur **22410A-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
2. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
4. Répétez les étapes 1 à 3 pour 22410A-LON-SVR1.

Exercice 1 : Installation et configuration d'un nouveau disque

Scénario

Le serveur de fichiers de votre filiale ne dispose plus de suffisamment d'espace disque. Vous devez ajouter un nouveau disque au serveur et créer des volumes en vous basant sur les spécifications fournies par votre responsable.

Les tâches principales de cet exercice sont les suivantes :

1. Initialiser un nouveau disque
2. Créer et formater deux volumes simples sur le disque
3. Vérifier la lettre de lecteur dans une fenêtre de l'Explorateur de fichiers

▶ Tâche 1 : Initialiser un nouveau disque

1. Ouvrez une session sur **LON-SVR1** avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, ouvrez **Gestion de l'ordinateur**, puis accédez à **Gestion des disques**.
3. Initialisez **Disque 2** et configurez-le pour utiliser **Partition GPT (GUID Partition Table)**.

▶ Tâche 2 : Créer et formater deux volumes simples sur le disque

1. Dans la console Gestion de l'ordinateur, sur Disque2, créez un **Volume simple** avec les attributs suivants :
   - Taille du volume : **4000** Mo
   - Lettre de lecteur : **F**
   - Système de fichiers : **NTFS**
   - Nom de volume : **Volume1**
2. Dans la console Gestion de l'ordinateur, sur Disque2, créez un **Volume simple** avec les attributs suivants :
   - Taille du volume : **5000** Mo
   - Lettre de lecteur : **G**
   - Système de fichiers : **ReFS**
   - Nom de volume : **Volume2**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérifier la lettre de lecteur dans une fenêtre de l'Explorateur de fichiers

1. Utilisez l'Explorateur de fichiers pour vérifier que vous pouvez accéder aux volumes suivants :
   - **Volume1 (F:)**
   - **Volume2 (G:)**
2. Sur Volume2 (G:), créez un dossier nommé **Dossier1**.

Résultats : À la fin de cet exercice, vous devez avoir initialisé un nouveau disque, créé deux volumes simples et les avoir formatés. Vous devez également avoir vérifié que les lettres de lecteur sont disponibles dans l'Explorateur de fichiers.

Exercice 2 : Redimensionnement des volumes

Scénario

Après l'installation du nouveau disque dans votre serveur de fichiers, votre responsable vous contacte pour signaler que les informations qu'il vous a données étaient incorrectes. Il est maintenant nécessaire de redimensionner les volumes sans perdre de données.

Les tâches principales de cet exercice sont les suivantes :

1. Réduire Volume1
2. Étendre Volume2

▶ Tâche 1 : Réduire Volume1

- Utilisez l'outil Gestion des disques pour réduire **Volume1 (F:)** de sorte qu'il fasse **3 000** Mo.

▶ Tâche 2 : Étendre Volume2

1. Utilisez l'outil Gestion des disques pour étendre **Volume2 (G:)** de **1 000** Mo.
2. Utilisez l'Explorateur de fichiers pour vérifier que le dossier **Dossier1** se trouve toujours sur le lecteur **G**.

Résultats : À la fin de cet exercice, vous devez avoir réduit un volume et étendu un autre.

Exercice 3 : Configuration d'un espace de stockage redondant

Scénario

Votre serveur ne dispose pas d'une carte RAID basée sur le matériel, mais vous devez configurer un stockage redondant. Pour prendre en charge cette fonctionnalité, vous devez créer un pool de stockage.

Après la création du pool de stockage, vous devez également créer un disque virtuel redondant. Comme il s'agit de données critiques, la demande de stockage redondant indique que vous devez utiliser un volume en miroir triple. Peu de temps après la mise en service du volume, un disque est tombé en panne et vous devez ajouter un autre disque au pool de stockage pour le remplacer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Créer un pool de stockage à partir de cinq disques connectés au serveur
2. Créer un disque virtuel en miroir triple
3. Copier un fichier sur le volume et vérifier qu'il est visible dans l'Explorateur de fichiers
4. Supprimer un disque physique
5. Vérifier que le fichier write.exe est toujours accessible
6. Ajouter un disque au pool de stockage et supprimer un disque endommagé

▶ Tâche 1 : Créer un pool de stockage à partir de cinq disques connectés au serveur

1. Sur LON-SVR1, ouvrez le **Gestionnaire de serveur**.
2. Dans le volet gauche, cliquez sur **Service de fichiers et de stockage**, puis dans le volet Serveurs, cliquez sur **Pools de stockage**.
3. Créez un pool de stockage avec les paramètres suivants :
   - Nom : **StoragePool1**
   - Disques physiques :
     - **PhysicalDisk3 (LON-SVR1)**
     - **PhysicalDisk4 (LON-SVR1)**
     - **PhysicalDisk5 (LON-SVR1)**
     - **PhysicalDisk6 (LON-SVR1)**
     - **PhysicalDisk7 (LON-SVR1)**

▶ Tâche 2 : Créer un disque virtuel en miroir triple

1. Sur LON-SVR1, dans le Gestionnaire de serveur, dans le volet DISQUES VIRTUELS, créez un disque virtuel avec les paramètres suivants :
   - Pool de stockage : **StoragePool1**
   - Nom : **Disque en miroir**
   - Disposition du stockage : **Miroir**
   - Paramètres de résilience : **Miroir triple**
   - Type d'approvisionnement : **Fin**
   - Taille du disque virtuel : **10 Go**
2. Dans l'Assistant Nouveau volume, créez un volume avec les paramètres suivants :
   - Disque virtuel : **Disque en miroir**
   - Lettre de lecteur : **H**
   - Système de fichiers : **ReFS**
   - Nom de volume : **Volume en miroir**

▶ Tâche 3 : Copier un fichier sur le volume et vérifier qu'il est visible dans l'Explorateur de fichiers

1. Ouvrez une fenêtre d'invite de commandes.
2. Tapez la commande suivante :

```
Copy C:\windows\system32\write.exe H:\
```

3. Ouvrez l'**Explorateur de fichiers** à partir de la barre des tâches, puis accédez au **Volume en miroir (H:)**. Vous devez maintenant voir **write.exe** dans la liste des fichiers.

▶ Tâche 4 : Supprimer un disque physique

- Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V, dans le volet Ordinateurs virtuels, remplacez les paramètres de **22410B-LON-SVR1** par les suivants :
  - Supprimez le disque dur commençant par **22410B-LON-SVR1-Disk5**.

▶ Tâche 5 : Vérifier que le fichier write.exe est toujours accessible

1. Basculez vers **LON-SVR1**.
2. Ouvrez l'**Explorateur de fichiers** et accédez à **H:\write.exe** pour vérifier que l'accès au fichier est toujours possible.
3. Dans le Gestionnaire de serveur, dans le volet POOLS DE STOCKAGE, sur la barre de menus, cliquez sur le bouton **Actualiser « Pools de stockage »**. Notez l'avertissement qui s'affiche en regard de Disque en miroir.
4. Ouvrez la boîte de dialogue **Propriétés de Disque en miroir**, puis accédez au volet Intégrité. Notez que l'état d'intégrité signale un avertissement. L'état opérationnel doit indiquer **Incomplet** ou **Détérioré**.

▶ Tâche 6 : Ajouter un disque au pool de stockage et supprimer un disque endommagé

1. Basculez vers **LON-SVR1**.
2. Dans le Gestionnaire de serveur, dans le volet POOLS DE STOCKAGE, sur la barre de menus, cliquez sur le bouton **Actualiser « Pools de stockage »**.
3. Dans le volet POOLS DE STOCKAGE, cliquez avec le bouton droit sur **StoragePool1**, cliquez sur **Ajouter un disque physique**, puis sur **PhysicalDisk8 (LON-SVR1)**.
4. Dans le volet DISQUES PHYSIQUES, cliquez avec le bouton droit sur le disque en regard duquel s'affiche un avertissement, puis sélectionnez **Supprimer le disque**.
5. Cliquez sur le bouton **Actualiser « Pools de stockage »** pour faire disparaître les avertissements.

Résultats : À la fin de cet exercice, vous devez avoir créé un pool de stockage et lui avoir ajouté cinq disques. Vous devez ensuite avoir créé un disque virtuel en miroir triple alloué dynamiquement à partir du pool de stockage. Vous devez également avoir copié un fichier sur le nouveau volume et vérifié qu'il est accessible. Ensuite, après avoir supprimé un disque physique, vous devez avoir vérifié que le disque virtuel était toujours disponible et accessible. Enfin, vous devez avoir ajouté un autre disque physique au pool de stockage.

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 des ordinateurs virtuels, cliquez avec le bouton droit sur **22410B-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 **22410B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Votre volume actuel manque d'espace disque. Vous avez un autre disque disponible dans le même serveur. Quelles actions pouvez-vous effectuer dans le système d'exploitation Windows pour vous aider à ajouter de l'espace disque ?

Question : Quels sont les deux différents types de disque dans l'outil Gestion des disques ?

Question : Quelles sont les implémentations de système RAID les plus importantes ?

Question : Vous connectez cinq disques de 2 To à votre ordinateur Windows Server 2012. Vous souhaitez les gérer presque automatiquement et, an cas de défaillance d'un disque, vous souhaitez vous assurer que les données ne seront pas perdues. Quelle fonctionnalité pouvez-vous implémenter pour y parvenir ?

Outils

Outil	Utilisation	Emplacement
Gestion des disques	• Initialiser des disques • Créer et modifier des volumes	Dans le menu Outils du Gestionnaire de serveur (dans la console Gestion de l'ordinateur)
Diskpart.exe	• Initialiser des disques • Créer et modifier des volumes à partir d'une invite de commandes	Invite de commandes
Mklink.exe	• Créer un lien symbolique vers un fichier ou un dossier	Invite de commandes
Chkdsk.exe	• Vérifier un disque pour un volume au format NTFS • Ne peut pas être utilisé pour des disques virtuels ou ReFS	Invite de commandes
Defrag.exe	• Outil de défragmentation de disque pour les volumes au format NTFS • Ne peut pas être utilisé pour des disques virtuels ou ReFS	Invite de commandes

Méthode conseillée

Voici les meilleures pratiques recommandées :

- Si vous souhaitez réduire un volume, commencez par le défragmenter afin de pouvoir récupérer plus d'espace de ce volume.
- Utilisez le format de table de partition GPT pour des disques de plus de 2 To.
- Pour les volumes très importants, utilisez le format ReFS.
- N'utilisez pas FAT ou FAT32 sur les disques du système d'exploitation Windows Server.
- Utilisez la fonctionnalité Espaces de stockage pour que le système d'exploitation Windows gère vos disques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10

Implémentation des services de fichier et d'impression

Table des matières :

Vue d'ensemble du module **10-1**

Leçon 1 : Sécurisation des fichiers et des dossiers **10-2**

Leçon 2 : Protection des fichiers et des dossiers partagés à l'aide de clichés instantanés **10-17**

Leçon 3 : Configuration de l'impression réseau **10-21**

Atelier pratique : Implémentation des services de fichier et d'impression **10-28**

Contrôle des acquis et éléments à retenir **10-35**

Vue d'ensemble du module

L'accès aux fichiers et aux imprimantes dans le réseau représente l'une des activités les plus courantes dans l'environnement Windows Server®. Un accès fiable et sécurisé aux fichiers et dossiers, ainsi qu'aux ressources d'impression constitue souvent la première exigence d'un réseau basé sur Windows Server 2012. Pour fournir l'accès aux ressources de fichier et d'impression dans votre réseau, vous devez comprendre comment configurer ces ressources sur le serveur Windows Server 2012 et comment configurer l'accès approprié aux ressources pour les utilisateurs dans votre environnement.

Ce module explique comment fournir ces ressources de fichier et d'impression importantes à l'aide de Windows Server 2012. Vous apprendrez comment activer et configurer des services de fichiers et d'impression dans Windows Server 2012 et vous découvrirez des considérations importantes et les meilleures pratiques pour utiliser ces services de fichiers et d'impression.

Objectifs

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

- sécuriser les fichiers et les dossiers partagés ;
- protéger les fichiers et dossiers partagés à l'aide de clichés instantanés ;
- configurer l'impression réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Sécurisation des fichiers et des dossiers

Les fichiers et les dossiers que vos serveurs stockent contiennent en général les données fonctionnelles et métier de votre organisation. La fourniture d'un accès approprié à ces fichiers et dossiers, habituellement via le réseau, constitue une part importante de la gestion des services de fichiers et d'impression dans Windows Server 2012.

Cette leçon vous fournit les informations nécessaires pour sécuriser les fichiers et les dossiers sur vos serveurs Windows Server 2012, afin que les données de votre organisation soient disponibles tout en étant protégées.

Objectifs de la leçon

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

- décrire les autorisations NTFS ;
- décrire un dossier partagé ;
- décrire l'héritage des autorisations ;
- décrire l'efficacité des autorisations quand vous accédez à des dossiers partagés ;
- décrire l'énumération basée sur l'accès ;
- décrire les fichiers hors connexion ;
- expliquer comment créer et configurer un dossier partagé.

Que sont les autorisations NTFS ?

Des autorisations NTFS sont attribuées aux fichiers et dossiers sur un lecteur de stockage au format NTFS. Les autorisations que vous attribuez aux fichiers et dossiers NTFS régissent l'accès utilisateur à ces fichiers et dossiers.

Les points suivants décrivent les aspects clé des autorisations NTFS :

- Les autorisations NTFS peuvent être configurées pour un fichier ou un dossier individuel ou pour des ensembles de fichiers ou de dossiers.

Les autorisations NTFS contrôlent l'accès des fichiers et des dossiers sur les volumes de stockage au format NTFS

Les autorisations NTFS
- Sont configurées pour les fichiers ou les dossiers
- Peuvent être accordées ou refusées
- Sont héritées des dossiers parents

Priorité de conflit d'autorisations
1. Refus explicitement attribué
2. Autorisation explicitement attribuée
3. Refus hérité
4. Autorisation héritée

- Les autorisations NTFS peuvent être attribuées individuellement à des objets qui incluent des utilisateurs, des groupes ou des ordinateurs.
- Les autorisations NTFS sont contrôlées en refusant ou en accordant des types spécifiques d'accès aux fichiers et dossiers NTFS, tels que Lecture ou Écriture.
- Les autorisations NTFS peuvent être héritées des dossiers parents. Par défaut, les autorisations NTFS qui sont attribuées à un dossier sont également attribuées aux dossiers et fichiers nouvellement créés au sein de ce dossier parent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Types d'autorisation NTFS

Il existe deux types d'autorisations NTFS attribuables : les autorisations standard et avancées.

Autorisations standard

Les autorisations standard fournissent les paramètres d'autorisation les plus couramment utilisés pour les fichiers et les dossiers. Vous attribuez des autorisations standard dans la fenêtre Attribution des autorisations NTFS.

Le tableau ci-dessous détaille les options d'autorisation standard pour les fichiers et les dossiers NTFS.

Autorisations sur les fichiers	Description
Contrôle total	Accorde à l'utilisateur un contrôle complet du fichier ou du dossier, y compris le contrôle des autorisations.
Modification	Accorde à l'utilisateur l'autorisation de lire, écrire ou supprimer un fichier ou un dossier, y compris de créer un fichier ou un dossier. Il accorde également l'autorisation d'exécuter des fichiers.
Lecture et exécution	Accorde à l'utilisateur l'autorisation de lire un fichier et de démarrer des programmes.
Lecture	Accorde à l'utilisateur l'autorisation d'afficher le contenu d'un fichier ou d'un dossier.
Écriture	Accorde à l'utilisateur l'autorisation d'écrire dans un fichier.
Affichage du contenu du dossier (dossiers uniquement)	Accorde à l'utilisateur l'autorisation d'afficher la liste du contenu du dossier.

Remarque : Accorder à des utilisateurs les autorisations Contrôle total sur un fichier ou un dossier leur donne la capacité d'exécuter n'importe quelle opération de système de fichiers sur l'objet, ainsi que la capacité de modifier les autorisations sur l'objet. Ils peuvent également supprimer des autorisations sur la ressource pour tous les utilisateurs qu'ils souhaitent, y compris vous.

Autorisations avancées

Les autorisations avancées peuvent fournir un niveau de contrôle nettement supérieur sur les fichiers et dossiers NTFS. Les autorisations avancées sont accessibles en cliquant sur le bouton **Avancé** dans l'onglet **Sécurité** de la boîte de dialogue **Propriétés** d'un fichier ou d'un dossier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le tableau ci-dessous détaille les autorisations avancées pour les fichiers et les dossiers NTFS.

Autorisations sur les fichiers	Description
Parcours du dossier/exécuter le fichier	L'autorisation Parcours du dossier s'applique uniquement aux dossiers. Cette autorisation autorise ou non l'utilisateur à parcourir les dossiers pour atteindre d'autres fichiers ou dossiers, même si l'utilisateur n'a pas d'autorisation sur les dossiers parcourus. L'autorisation Parcours du dossier entre en vigueur seulement lorsque le droit d'utilisateur Contourner la vérification de parcours n'est pas accordé au groupe ou à l'utilisateur. Par défaut, le groupe Tout le monde dispose du droit d'utilisateur Contourner la vérification de parcours. L'autorisation Exécuter le fichier permet ou non d'exécuter les fichiers programmes. Si vous définissez l'autorisation Parcours du dossier sur un dossier, l'autorisation Exécuter le fichier n'est pas automatiquement définie sur tous les fichiers de ce dossier.
Liste du dossier/lecture de données	L'autorisation Liste du dossier accorde à l'utilisateur l'autorisation d'afficher les noms des fichiers et des sous-dossiers. L'autorisation Liste du dossier s'applique uniquement à des dossiers et affecte uniquement le contenu du dossier ; elle ne détermine pas si le dossier lui-même sera répertorié. En outre, ce paramètre n'a aucun effet sur l'affichage de la structure de fichiers à partir d'une interface de ligne de commande. L'autorisation Lecture de données accorde ou refuse à l'utilisateur l'autorisation d'afficher les données dans les fichiers. L'autorisation Lecture de données s'applique uniquement aux fichiers.
Lecture d'attributs	L'autorisation Lecture d'attributs accorde à l'utilisateur l'autorisation d'afficher les attributs élémentaires d'un fichier ou d'un dossier, tels que les attributs Lecture seule et Caché. Les attributs sont définis par NTFS.
Lecture des attributs étendus	L'autorisation Lecture des attributs étendus accorde à l'utilisateur l'autorisation d'afficher les attributs étendus d'un fichier ou d'un dossier. Les attributs étendus sont définis par les applications et peuvent varier selon l'application.
Création de fichiers/écriture de données	L'autorisation Création de fichiers s'applique uniquement aux dossiers et accorde à l'utilisateur l'autorisation de créer des fichiers dans le dossier. L'autorisation Écriture de données accorde à l'utilisateur l'autorisation d'apporter des modifications au fichier et de remplacer le contenu existant par NTFS. L'autorisation Écriture de données s'applique uniquement aux fichiers.
Création de dossiers/ajout de données	L'autorisation Création de dossiers accorde à l'utilisateur l'autorisation de créer des dossiers dans le dossier. L'autorisation Création de dossiers s'applique uniquement aux dossiers. L'autorisation Ajout de données accorde à l'utilisateur l'autorisation d'apporter des modifications à la fin du fichier, mais pas de supprimer ni de remplacer les données existantes. L'autorisation Ajout de données s'applique uniquement aux fichiers.
Écriture d'attributs	L'autorisation Écriture d'attributs accorde à l'utilisateur l'autorisation de modifier les attributs élémentaires d'un fichier ou d'un dossier, tels que Lecture seule et Caché. Les attributs sont définis par NTFS. L'autorisation Écriture d'attributs n'implique pas que vous pouvez créer ou supprimer des fichiers ou des dossiers ; elle inclut uniquement l'autorisation de modifier les attributs d'un fichier ou d'un dossier. Pour accorder les autorisations de création et de suppression, reportez-vous aux entrées Création de fichiers/écriture de données, Création de dossiers/ajout de données, Suppression de sous-dossiers et de fichiers, et Suppression de ce tableau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Autorisations sur les fichiers	Description
Écriture d'attributs étendus	L'autorisation Écriture d'attributs étendus accorde à l'utilisateur l'autorisation de modifier les attributs étendus d'un fichier ou d'un dossier. Les attributs étendus sont définis par les programmes et peuvent varier selon le programme. L'autorisation Écriture d'attributs étendus n'implique pas que l'utilisateur peut créer ou supprimer des fichiers ou des dossiers ; elle inclut uniquement l'autorisation de modifier les attributs d'un fichier ou d'un dossier. Pour accorder les autorisations de création et de suppression, reportez-vous aux entrées Création de fichiers/écriture de données, Création de dossiers/ajout de données, Suppression de sous-dossiers et de fichiers, et Suppression de ce tableau.
Suppression de sous-dossiers et de fichiers	L'autorisation Suppression de sous-dossiers et de fichiers accorde à l'utilisateur l'autorisation de supprimer des sous-dossiers et des fichiers, même si l'autorisation Supprimer n'est pas accordée sur les sous-dossiers ou les fichiers. L'autorisation Suppression de sous-dossiers et de fichiers s'applique uniquement aux dossiers.
Suppression	L'autorisation Suppression accorde à l'utilisateur l'autorisation de supprimer le fichier ou le dossier. Si l'autorisation Suppression ne vous a pas été accordée sur un fichier ou un dossier, vous pouvez quand même supprimer le fichier ou le dossier si vous disposez de l'autorisation Suppression de sous-dossiers et de fichiers sur le dossier parent.
Lire les autorisations	L'option Lire les autorisations accorde à l'utilisateur l'autorisation de lire les autorisations concernant le fichier ou le dossier, telles que Contrôle total, Lecture et Écriture.
Modifier les autorisations	L'option Modifier les autorisations accorde à l'utilisateur l'autorisation de modifier les autorisations portant sur le fichier ou le dossier, telles que Contrôle total, Lecture et Écriture.
Appropriation	L'autorisation Appropriation accorde à l'utilisateur l'autorisation de s'approprier le fichier ou le dossier. Le propriétaire d'un fichier ou d'un dossier peut modifier les autorisations s'y rapportant, quelles que soient les autorisations existantes qui protègent le fichier ou le dossier.
Synchronisation	L'autorisation Synchronisation autorise des threads différents à attendre le handle de fichier ou de dossier, puis à se synchroniser avec un autre thread qui peut le signaler. Cette autorisation s'applique uniquement aux programmes multithreads et à plusieurs processus.

Remarque : Les autorisations standard sont des combinaisons de plusieurs autorisations avancées individuelles, groupées dans des scénarios d'utilisation courante de fichiers et de dossiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exemples d'autorisations NTFS

Voici quelques exemples élémentaires d'attribution d'autorisations NTFS :

- Pour le dossier Images marketing, un administrateur a choisi d'attribuer à Adam Carter des autorisations Autoriser pour le type d'autorisation Lecture. Comme comportement par défaut lié aux autorisations NTFS, Adam Carter aura un accès en lecture aux fichiers et aux dossiers contenus dans le dossier Images marketing.
- Lors de l'application des autorisations NTFS, les résultats sont cumulatifs. Par exemple, dans l'exemple précédent, supposons qu'Adam Carter appartient également au groupe Marketing. Le groupe marketing a reçu des autorisations en écriture sur le dossier Images marketing. Lorsque nous associons les autorisations attribuées au compte d'utilisateur d'Adam Carter avec les autorisations attribuées au groupe Marketing, Adam bénéficie à la fois des autorisations en lecture et en écriture pour le dossier Images marketing.

Règles importantes pour les autorisations NTFS

Il existe deux groupes importants d'autorisations NTFS :

- Autorisations explicites et héritées. Lorsque vous appliquez des autorisations NTFS, les autorisations qui sont appliquées explicitement à un fichier ou à un dossier ont priorité sur celles qui sont héritées d'un dossier parent.
- Autorisations Refuser et Autoriser. Une fois que les autorisations NTFS ont été divisées en autorisations explicites et héritées, toutes les autorisations Refuser existantes remplacent les autorisations Autoriser contradictoires au sein du groupe.

Par conséquent, en tenant compte de ces règles, les autorisations NTFS s'appliqueront dans l'ordre suivant :

1. Refus explicite
2. Autorisation explicite
3. Refus hérité
4. Autorisation héritée

Il est important de se souvenir que les autorisations NTFS sont cumulatives et que ces règles s'appliquent seulement lorsque deux paramètres d'autorisation NTFS sont en conflit mutuel.

Procédure de configuration des autorisations NTFS

Vous pouvez afficher et configurer des autorisations NTFS en procédant comme suit :

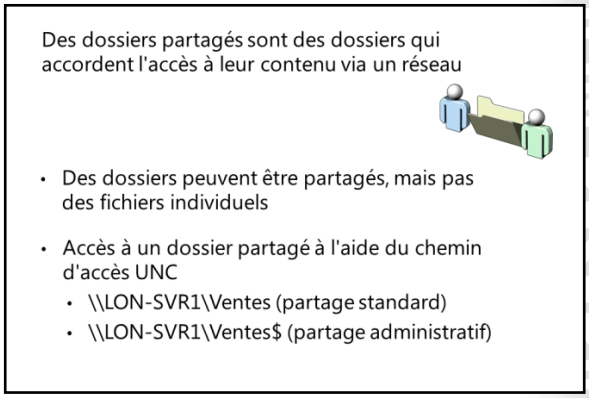
1. Cliquez avec le bouton droit sur le fichier ou le dossier pour lequel vous voulez attribuer des autorisations, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Sécurité**. Dans cet onglet, vous pouvez sélectionner les utilisateurs ou les groupes actuels dotés d'autorisations permettant d'afficher les autorisations spécifiques attribuées à chaque principal.
3. Pour ouvrir une boîte de dialogue d'autorisations modifiable afin de pouvoir modifier des autorisations existantes ou ajouter de nouveaux utilisateurs ou groupes, cliquez sur le bouton **Modifier**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les dossiers partagés ?

Les dossiers partagés constituent un composant clé pour accorder l'accès aux fichiers sur votre serveur à partir du réseau. Lorsque vous partagez un dossier, ce dossier et tout son contenu deviennent accessibles à plusieurs utilisateurs simultanément, via le réseau. Les dossiers partagés conservent un ensemble distinct d'autorisations par rapport aux autorisations NTFS, qui s'appliquent au contenu du dossier. Ces autorisations sont utilisées pour fournir un niveau de sécurité supplémentaire pour les fichiers et les dossiers mis à la disposition des utilisateurs dans le réseau.



La plupart des entreprises déploient des serveurs de fichiers dédiés pour héberger les dossiers partagés. Vous pouvez stocker des fichiers dans des dossiers partagés par catégorie ou par fonction. Par exemple, vous pouvez placer des fichiers partagés pour le service Ventes dans un dossier partagé et les fichiers partagés pour le service Marketing dans un autre.

Remarque : Le processus de partage s'applique seulement au niveau du dossier. Vous ne pouvez pas partager un fichier individuel ou un groupe de fichiers.

Accès à un dossier partagé

Les utilisateurs accèdent en général à un dossier partagé via le réseau en utilisant son adresse UNC (Universal Naming Convention). L'adresse UNC contient le nom du serveur qui héberge le dossier et le nom réel du dossier partagé, séparés par une barre oblique inverse (\) et précédés par deux barres obliques inverses (\\). Par exemple, le chemin d'accès UNC du dossier partagé Sales sur le serveur LON-SVR1 peut être \\LON-SVR1\Sales.

Partage d'un dossier dans le réseau

Windows Server 2012 fournit différentes manières de partager un dossier :

- Cliquez sur le lecteur approprié, puis dans la section Services de fichiers et de stockage dans le Gestionnaire de serveur, cliquez sur la tâche **Nouveau partage**.
- Utilisez l'Assistant Partage de fichiers, à partir du menu contextuel du dossier ou en cliquant sur le bouton **Partager** dans l'onglet **Partage** de la boîte de dialogue **Propriétés** du dossier.
- Utilisez le partage avancé en cliquant sur le bouton **Partage avancé** dans l'onglet **Partage** de la boîte de dialogue **Propriétés** du dossier.
- Utilisez l'outil en ligne de commande **Net use** dans une fenêtre de ligne de commande.
- Utilisez l'applet de commande **New-SMBShare** dans Windows PowerShell®.

Remarque : Lors du partage d'un dossier, vous êtes invité à donner un nom au dossier partagé. Ce nom ne doit pas nécessairement être le même que celui du dossier réel ; ce peut être un nom descriptif qui décrit mieux le contenu du dossier aux utilisateurs du réseau.

Partages administratifs

Vous pouvez créer des dossiers partagés administratifs (ou cachés) qui doivent être accessibles via le réseau mais cachés aux utilisateurs parcourant le réseau. Vous pouvez accéder à un dossier partagé administratif en entrant son chemin d'accès UNC, mais le dossier ne s'affichera pas si vous accédez au serveur en utilisant une fenêtre de l'Explorateur de fichiers. Les dossiers partagés administratifs disposent également en général d'un ensemble d'autorisations plus restrictif qui reflète la nature administrative du contenu de ces dossiers.

Pour masquer un dossier partagé, ajoutez le symbole dollar ($) au nom du dossier. Par exemple, vous pouvez transformer un dossier partagé sur LON-SVR1, nommé Sales, en dossier partagé caché en le nommant Sales$. Le dossier partagé est accessible via le réseau à l'aide du chemin d'accès UNC \\LON-SVR1\Sales$.

Remarque : Les autorisations d'un dossier partagé s'appliquent uniquement aux utilisateurs qui accèdent au dossier via le réseau. Elles n'affectent pas les utilisateurs qui accèdent au dossier localement sur l'ordinateur où le dossier est stocké.

Autorisations de dossier partagé

Tout comme les autorisations NTFS, vous pouvez attribuer des autorisations de dossier partagé à des utilisateurs, des groupes et des ordinateurs. Toutefois, à la différence des autorisations NTFS, les autorisations de dossier partagé ne sont pas configurables pour les fichiers ou les dossiers individuels figurant dans le dossier partagé. Les autorisations de dossier partagé sont définies une fois pour le dossier partagé lui-même et s'appliquent universellement au contenu entier du dossier partagé pour les utilisateurs qui accèdent au dossier via le réseau.

Lorsque vous créez un dossier partagé, l'autorisation partagée attribuée par défaut au groupe Tout le monde est définie sur Lecture.

Le tableau ci-dessous répertorie les autorisations que vous pouvez accorder à un dossier partagé.

Autorisation de dossier partagé	Description
Lecture	Les utilisateurs peuvent visualiser les noms des dossiers et des fichiers, visualiser les données et les attributs des fichiers, exécuter les fichiers programmes et les scripts, ainsi que parcourir l'arborescence au sein du dossier partagé.
Modification	Les utilisateurs peuvent créer des dossiers, ajouter des fichiers aux dossiers, modifier ou ajouter des données dans les fichiers, modifier les attributs des fichiers, supprimer des dossiers et des fichiers et effectuer toutes les tâches permises par l'autorisation Lecture.
Contrôle total	Les utilisateurs peuvent changer les autorisations des fichiers, prendre possession des fichiers et effectuer toutes les tâches permises par l'autorisation Modification.

Remarque : Quand vous attribuez des autorisations Contrôle total sur un dossier partagé à un utilisateur, ce dernier peut modifier les autorisations sur le dossier partagé, notamment supprimer tous les utilisateurs (y compris les administrateurs) de la liste des autorisations du dossier partagé. Dans la plupart des cas, vous devriez accorder l'autorisation Modification à la place de l'autorisation Contrôle total.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Héritage des autorisations

Par défaut, NTFS et les dossiers partagés utilisent l'héritage pour propager les autorisations dans l'ensemble d'une arborescence. Quand vous créez un fichier ou un dossier, vous lui attribuez automatiquement les autorisations définies sur les dossiers placés au-dessus de lui (dossiers parents) dans la hiérarchie de l'arborescence.

L'héritage est utilisé pour gérer l'accès aux ressources sans affecter d'autorisations explicites à chaque objet

Par défaut, les autorisations NTFS sont héritées dans une relation parent/enfant

Blocage de l'héritage

- Vous pouvez bloquer l'héritage des autorisations
- Vous pouvez appliquer le blocage au niveau du fichier ou du dossier
- Vous pouvez définir le blocage sur un dossier pour propager les nouvelles autorisations aux objets enfants

Application de l'héritage

Examinez l'exemple suivant. Adam Carter est membre du groupe Marketing et du groupe New York Editors. Le tableau suivant est un résumé des autorisations pour cet exemple :

Dossier ou fichier	Autorisations attribuées	Autorisations d'Adam
Marketing (dossier)	Lecture – Marketing	Lecture
Images marketing (dossier)	Aucune définie	Lecture (héritée)
New York (dossier)	Écriture – New York Editors	Lecture(h) + Écriture
Fall_Composite.jpg (fichier)	Aucune définie	Lecture(h) + Écriture(h)

Dans cet exemple, Adam est membre de deux groupes auxquels sont attribuées des autorisations pour des fichiers et des dossiers dans l'arborescence. Ces autorisations sont les suivantes :

- Le dossier de niveau supérieur, Marketing, possède une autorisation attribuée pour le groupe Marketing qui autorise l'accès en lecture.
- Au niveau suivant, le dossier Images marketing ne possède aucune autorisation explicite définie mais, en raison de l'héritage des autorisations, Adam a obtenu l'accès en lecture à ce dossier et à son contenu à partir des autorisations définies sur le dossier Marketing.
- Au troisième niveau, le dossier New York a l'autorisation Écriture attribuée à l'un des groupes d'Adam, New York Editors. Outre cette autorisation Écriture explicitement attribuée, le dossier New York hérite également de l'autorisation Lecture du dossier Marketing. Ces autorisations sont transmises vers le bas aux objets fichiers et dossiers et se cumulent aux autorisations de lecture et d'écriture explicites définies sur ces fichiers.
- Le quatrième et dernier niveau correspond au fichier Fall_Composite.jpg. Même si aucune autorisation explicite n'a été définie pour ce fichier, Adam dispose d'un accès en lecture et en écriture au fichier en raison des autorisations héritées des dossiers Marketing et New York.

Conflits entre autorisations

Parfois, des autorisations définies explicitement sur un fichier ou un dossier entrent en conflit avec des autorisations héritées d'un dossier parent. Dans ce cas, les autorisations attribuées explicitement remplacent toujours les autorisations héritées. Dans l'exemple donné, si l'accès en écriture au dossier parent Marketing a été refusé à Adam Carter, mais que l'accès en écriture au dossier New York lui a été ensuite accordé explicitement, l'autorisation d'accès en écriture accordée a priorité sur l'autorisation refusée d'accès en écriture héritée.

Blocage de l'héritage

Vous pouvez également désactiver le comportement d'héritage pour un fichier ou un dossier (et son contenu) sur un lecteur NTFS pour définir explicitement des autorisations pour un ensemble d'objets sans inclure les autorisations héritées à partir des dossiers parents. Windows Server 2012 propose une option permettant de bloquer l'héritage sur un fichier ou un dossier. Pour bloquer l'héritage sur un fichier ou un dossier, procédez comme suit :

- Cliquez avec le bouton droit sur le fichier ou le dossier où vous souhaitez bloquer l'héritage, puis cliquez sur **Propriétés**.
- Dans la fenêtre Propriétés, cliquez sur l'onglet **Sécurité**, puis sur le bouton **Avancé**.
- Dans la fenêtre Paramètres de sécurité avancés, cliquez sur le bouton **Modifier les autorisations**.
- Dans la fenêtre Paramètres de sécurité avancés suivante, cliquez sur le bouton **Désactiver l'héritage**.

À ce stade, vous êtes invité à convertir les autorisations héritées en autorisations explicites ou à supprimer toutes les autorisations héritées de l'objet pour repartir à zéro en matière d'autorisations.

Réinitialisation du comportement d'héritage par défaut

Après avoir bloqué l'héritage, les modifications apportées aux autorisations sur l'arborescence parente n'exercent plus aucun effet sur les autorisations pour l'objet enfant (et son contenu) dont l'héritage est bloqué, à moins que vous réinitialisiez ce comportement à partir d'un des dossiers parents en activant la case à cocher **Remplacer toutes les autorisations des objets enfants par des autorisations pouvant être héritées de cet objet**. Quand vous activez cette case à cocher, l'ensemble existant d'autorisations sur le dossier actif est propagé vers le bas à tous les objets enfants dans l'arborescence et remplace toutes les autorisations explicitement attribuées pour ces fichiers et dossiers. Cette case à cocher est située directement sous la case à cocher **Inclure les autorisations pouvant être héritées du parent de cet objet**.

Autorisations effectives

L'accès à un fichier ou dossier dans Windows Server 2012 est accordé sur la base d'une combinaison d'autorisations. Lorsqu'un utilisateur tente d'accéder à un fichier ou à un dossier, l'autorisation qui s'applique dépend de divers facteurs, incluant :

- les autorisations héritées et explicitement définies qui s'appliquent à l'utilisateur ;
- les autorisations héritées et explicitement définies qui s'appliquent aux groupes auxquels l'utilisateur appartient ;
- la façon dont l'utilisateur accède au fichier ou aux dossiers : localement ou via le réseau.

Lorsque des autorisations de dossier partagé et NTFS sont combinées, l'autorisation la plus restrictive est appliquée

Exemple : si un utilisateur ou un groupe dispose sur le dossier partagé de l'autorisation de partage Lecture et de l'autorisation NTFS Écriture, l'utilisateur ou le groupe pourra seulement lire le fichier, car c'est l'autorisation la plus restrictive

Les autorisations de partage comme les autorisations de fichiers et de dossiers NTFS doivent être correctes, sinon l'utilisateur ou le groupe se verra refuser l'accès à la ressource

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les autorisations NTFS effectives sont les autorisations cumulatives qui sont attribuées à un utilisateur pour un fichier ou un dossier en fonction des facteurs répertoriés ci-dessus. Les principes suivants déterminent les autorisations NTFS effectives :

- Les autorisations cumulatives sont la combinaison des plus hautes autorisations NTFS accordées à l'utilisateur et à tous les groupes dont l'utilisateur est membre. Par exemple, si un utilisateur est membre d'un groupe disposant de l'autorisation de lecture et membre d'un groupe disposant de l'autorisation de modification, l'autorisation de modification cumulative est attribuée à l'utilisateur.
- Les refus ont priorité sur les autorisations équivalentes. Toutefois, une autorisation explicite peut primer sur un refus hérité. Par exemple, si l'accès en écriture à un dossier est refusé à un utilisateur via un refus hérité, mais que l'accès en écriture à un sous-dossier ou à un fichier particulier lui est accordé explicitement, l'autorisation explicite prime sur le refus hérité pour le sous-dossier ou le fichier particulier.
- Vous pouvez appliquer des autorisations à un utilisateur ou à un groupe. Il est préférable d'attribuer des autorisations à des groupes, car elles sont plus efficaces que la gestion d'autorisations définies pour de nombreux individus.
- Les autorisations de fichiers NTFS ont la priorité sur les autorisations de dossiers NTFS. Par exemple, si un utilisateur a l'autorisation de lecture sur un dossier mais que l'autorisation de modification lui a été accordée sur certains fichiers dans ce dossier, l'autorisation effective pour ces fichiers est définie sur Modification.
- Chaque objet sur un lecteur NTFS ou dans les services de domaine Active Directory® (AD DS) a un propriétaire. Le propriétaire contrôle la manière dont les autorisations sont définies sur l'objet et qui en bénéficie. Par exemple, un utilisateur qui crée un fichier dans un dossier où il dispose de l'autorisation de modification peut modifier les autorisations sur le fichier en spécifiant Contrôle total.

Outil Autorisations effectives

Windows Server 2012 fournit un outil Autorisations effectives qui montre les autorisations NTFS effectives sur un fichier ou un dossier pour un utilisateur, en fonction des autorisations attribuées au compte d'utilisateur et aux groupes auxquels le compte d'utilisateur appartient. Vous pouvez accéder à l'outil Autorisations effectives en procédant comme suit :

1. Cliquez avec le bouton droit sur le fichier ou le dossier pour lequel vous voulez analyser les autorisations, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés**, cliquez sur le bouton **Avancé**.
3. Dans la fenêtre Paramètres de sécurité avancés, cliquez sur l'onglet **Autorisations effectives**.
4. Choisissez un utilisateur ou un groupe à évaluer à l'aide du bouton **Sélectionner**.

Combinaison d'autorisations NTFS et d'autorisations de dossier partagé

Les autorisations NTFS et les autorisations de dossier partagé fonctionnent ensemble pour contrôler l'accès aux ressources de fichiers et de dossiers via un réseau. Lorsque vous configurez l'accès aux ressources réseau sur un lecteur NTFS, utilisez les autorisations NFTS les plus restrictives pour contrôler l'accès aux dossiers et aux fichiers, et combinez-les avec les autorisations de dossier partagé les plus restrictives pour contrôler l'accès au réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement de la combinaison d'autorisations NTFS et d'autorisations de dossier partagé

Quand vous appliquez des autorisations NTFS et de dossier partagé, souvenez-vous que l'autorisation la plus restrictive des deux définit l'accès dont bénéficiera un utilisateur à un fichier ou à un dossier. Les deux exemples suivants expliquent cela plus en détail :

- Si vous définissez l'autorisation NTFS Contrôle total sur un dossier, mais définissez l'autorisation de dossier partagé Lecture, l'utilisateur dispose uniquement de l'autorisation Lecture lorsqu'il accède au dossier via le réseau. L'accès est restreint au niveau du dossier partagé et aucun accès supérieur au niveau des autorisations NTFS ne s'applique.
- De même, si vous définissez l'autorisation de dossier partagé sur Contrôle total et que vous définissez les autorisations NTFS sur Écriture, l'utilisateur n'aura aucune restriction au niveau du dossier partagé, mais les autorisations NTFS sur le dossier accorderont uniquement les autorisations Écriture sur ce dossier.

L'utilisateur doit avoir des autorisations appropriées sur le fichier ou le dossier NTFS et sur le dossier partagé. Si aucune autorisation n'existe pour l'utilisateur (en tant qu'individu ou en tant que membre d'un groupe) sur les deux ressources, l'accès est refusé.

Considérations liées aux autorisations NTFS et de dossier partagé combinées

Voici quelques considérations permettant de faciliter l'administration des autorisations :

- Accordez des autorisations aux groupes plutôt qu'aux utilisateurs. Des individus peuvent toujours être ajoutés ou supprimés dans les groupes, tandis que les autorisations au cas-par-cas sont difficiles à suivre et complexes à gérer.
- Refusez des autorisations uniquement en cas de nécessité. Les refus étant hérités, le fait de refuser des autorisations sur un dossier peut empêcher des utilisateurs d'avoir accès à des fichiers à un niveau inférieur de l'arborescence. Vous ne devez refuser des autorisations que dans les cas suivants :
  - pour exclure un sous-ensemble d'un groupe disposant d'une autorisation ;
  - pour exclure une autorisation spécifique lorsque vous avez accordé des autorisations de contrôle total à un utilisateur ou à un groupe.
- Ne refusez jamais l'accès à un objet au groupe Tout le monde. Si vous refusez l'accès à un objet au groupe Tout le monde, vous refusez l'accès aux administrateurs, y compris à vous-même. Supprimez plutôt le groupe Tout le monde de la liste des autorisations à condition d'accorder des autorisations sur l'objet à d'autres utilisateurs, groupes ou ordinateurs.
- Accordez des autorisations sur un objet situé le plus haut possible dans l'arborescence, pour que les paramètres de sécurité soient propagés dans toute l'arborescence. Par exemple, au lieu de rassembler des groupes qui représentent tous les services de la société dans un dossier « Lecture », attribuez le groupe Utilisateurs du domaine (qui est un groupe par défaut de tous les comptes d'utilisateurs du domaine) au partage. De cette manière, plus besoin de mettre à jour les groupes de services avant que les nouveaux utilisateurs ne reçoivent le dossier partagé.
- Utilisez des autorisations NTFS à la place d'autorisations de dossier partagé pour affiner l'accès. Configurer à la fois des autorisations de dossier partagé et NTFS peut s'avérer difficile. Envisagez d'affecter les autorisations les plus restrictives à un groupe qui contient de nombreux utilisateurs au niveau du dossier partagé, puis utilisez des autorisations NTFS pour attribuer des autorisations plus spécifiques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que l'énumération basée sur l'accès ?

Avec l'énumération basée sur l'accès, les utilisateurs voient seulement les fichiers et dossiers auxquels ils ont l'autorisation d'accéder. L'énumération basée sur l'accès fournit une meilleure expérience utilisateur, car elle permet d'afficher une vue moins complexe du contenu d'un dossier partagé, ce qui aide les utilisateurs à rechercher les fichiers dont ils ont besoin. Windows Server 2012 permet l'énumération basée sur l'accès des dossiers qu'un serveur partage via le réseau.

L'énumération basée sur l'accès permet à un administrateur de contrôler la visibilité des dossiers partagés en fonction des autorisations définies sur le dossier partagé

L'énumération basée sur l'accès est

- Générée dans Windows Server 2012
- Disponible pour les dossiers partagés
- Configurable sur la base d'un dossier partagé

Activation de l'énumération basée sur l'accès

Pour activer l'énumération basée sur l'accès pour un dossier partagé :

1. Ouvrez le Gestionnaire de serveur.
2. Dans le volet de navigation, cliquez sur **Services de fichiers et de stockage**.
3. Dans le volet de navigation, cliquez sur **Partages**.
4. Dans le volet Partages, cliquez avec le bouton droit sur le dossier partagé pour lequel vous souhaitez activer l'énumération basée sur l'accès, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés**, cliquez sur **Paramètres**, puis activez la case à cocher **Activer l'énumération basée sur l'accès**.

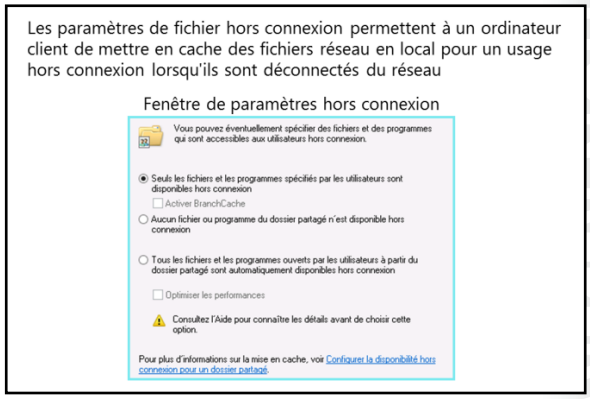
Quand la case à cocher **Activer l'énumération basée sur l'accès** est activée, l'énumération basée sur l'accès est activée sur le dossier partagé. Ce paramètre est unique pour chaque dossier partagé sur le serveur.

Remarque : La console Services de fichiers et de stockage est le seul emplacement de l'interface Windows Server 2012 où vous pouvez configurer l'énumération basée sur l'accès pour un dossier partagé. L'énumération basée sur l'accès est non disponible dans l'ensemble des boîtes de dialogue de propriétés accessibles en cliquant avec le bouton droit sur le dossier partagé dans l'Explorateur de fichiers.

Que sont les fichiers hors connexion ?

Un *fichier hors connexion* est une copie d'un fichier réseau qui est stockée sur un ordinateur client. Les fichiers hors connexion permettent aux utilisateurs d'accéder aux fichiers réseau lorsque leur ordinateur client est déconnecté du réseau.

Les fichiers et les dossiers hors connexion sont édités ou modifiés par le client, et les modifications sont synchronisées avec la copie réseau des fichiers la prochaine fois que le client se connecte au réseau. Le comportement et la planification de la synchronisation des fichiers hors connexion sont contrôlés par le système d'exploitation client Windows.



Les fichiers hors connexion sont disponibles avec les systèmes d'exploitation suivants :

- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2
- Windows Server 2008
- Windows Vista®
- Windows Server 2003
- Windows XP

Avec Windows Server 2012, vous visualisez la fenêtre Paramètres hors connexion pour un dossier partagé en cliquant sur le bouton **Mise en cache** dans la fenêtre Partage avancé. Les options suivantes sont disponibles dans la fenêtre Paramètres hors connexion :

- Seuls les fichiers et les programmes spécifiés par les utilisateurs sont disponibles hors connexion. Il s'agit de l'option par défaut lorsque vous configurez un dossier partagé. Quand vous utilisez cette option, aucun fichier ni programme n'est disponible hors connexion par défaut, et les utilisateurs contrôlent à quels fichiers et programmes ils souhaitent accéder lorsqu'ils ne sont pas connectés au réseau. Vous pouvez également choisir l'option **Activer BranchCache**. Cette option permet aux ordinateurs qui accèdent aux fichiers de mettre en cache les fichiers téléchargés à partir du dossier à l'aide de Windows BranchCache®. Vous devez installer et configurer BranchCache sur le serveur Windows Server 2012 pour pouvoir sélectionner cette option.
- Aucun fichier ou programme du dossier partagé n'est disponible hors connexion. Cette option empêche les ordinateurs clients d'effectuer des copies des fichiers et programmes dans le dossier partagé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Tous les fichiers et les programmes ouverts par les utilisateurs à partir du dossier partagé sont automatiquement disponibles hors connexion. Chaque fois qu'un utilisateur accède au lecteur ou dossier partagé et y ouvre un fichier ou un programme, ce fichier ou ce programme est automatiquement mis à la disposition de cet utilisateur hors connexion. Les fichiers et programmes automatiquement rendus disponibles hors connexion demeurent dans le cache des fichiers hors connexion et sont synchronisés avec la version sur le serveur jusqu'à ce que le cache soit plein ou que l'utilisateur supprime les fichiers. Les fichiers et programmes qui ne sont pas ouverts ne sont pas disponibles hors connexion.
- Optimisé pour les performances. Si vous activez la case à cocher **Optimisé pour les performances**, les fichiers exécutables (.exe, .dll) qui sont exécutés à partir du dossier partagé par un ordinateur client sont automatiquement mis en cache sur cet ordinateur client. La prochaine fois que l'ordinateur client exécutera les fichiers exécutables, il accédera à son cache local plutôt qu'au dossier partagé sur le serveur.

Remarque : La fonctionnalité Fichiers hors connexion doit être activée sur l'ordinateur client pour que les fichiers et les programmes soient automatiquement mis en cache. En outre, l'option **Optimisé pour les performances** n'a aucun effet sur les ordinateurs clients qui utilisent Windows Vista ou un système d'exploitation Windows antérieur, parce que ces systèmes d'exploitation effectuent automatiquement une mise en cache au niveau des programmes, telle que la spécifie cette option.

Configuration du paramètre Toujours disponible hors connexion

Vous pouvez configurer des ordinateurs exécutant Windows Server 2012 ou Windows 8 pour qu'ils utilisent le mode Toujours disponible hors connexion lorsqu'ils accèdent à des dossiers partagés. Lorsque vous configurez cette option, les ordinateurs clients utilisent toujours la version mise en cache localement des fichiers à partir d'un partage réseau, même s'ils sont connectés au serveur de fichiers via une connexion réseau haut-débit.

Cette configuration favorise en général un accès plus rapide aux fichiers pour les ordinateurs clients, notamment lorsque la connectivité ou la vitesse d'une connexion réseau est intermittente. La synchronisation avec les fichiers sur le serveur se produit selon la configuration des fichiers hors connexion de l'ordinateur client.

Procédure d'activation du mode Toujours disponible hors connexion

Pour activer le mode Toujours disponible hors connexion, vous pouvez utiliser la stratégie de groupe pour activer le paramètre **Configurer le mode de liaison lente** et définir la valeur de latence **1**. Le paramètre **Configurer le mode de liaison lente** est situé dans la stratégie de groupe sous le nœud Configuration ordinateur\Stratégies administratives\Réseau\Fichiers hors connexion.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Création et configuration d'un dossier partagé

La création et la configuration d'un dossier partagé sont en général effectuées dans l'Explorateur de fichiers, dans la boîte de dialogue **Propriétés** du fichier ou du dossier, dans l'onglet **Partage**. Lorsque vous créez un dossier partagé, assurez-vous toujours que vous définissez des autorisations appropriées pour tous les fichiers et dossiers dans le dossier partagé.

Dans cette démonstration, vous allez apprendre à :

- créer un dossier partagé ;
- attribuer des autorisations pour le dossier partagé ;
- configurer l'énumération basée sur l'accès ;
- configurer les fichiers hors connexion.

Procédure de démonstration

Créer un dossier partagé

1. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur le lecteur E:, créez un dossier nommé **Données**.
3. Partagez le dossier **Données**.

Attribuer des autorisations pour le dossier partagé

- Accordez aux utilisateurs authentifiés les autorisations de modification pour **\\LON-SVR1\Données**.

Configurer l'énumération basée sur l'accès

1. Ouvrez le **Gestionnaire de serveur**.
2. Naviguez jusqu'au volet Partager dans la console de gestion Services de fichiers et de stockage.
3. Ouvrez la boîte de dialogue **Propriétés de Données** pour **\\LON-SVR1\Données** et activez l'énumération basée sur l'accès.

Configurer les fichiers hors connexion

1. Ouvrez la boîte de dialogue **Propriétés de Données** pour **E:\Données**.
2. Accédez à l'onglet **Partage** et ouvrez les paramètres de **partage avancé**.
3. Ouvrez les paramètres **de mise en cache**, puis désactivez les fichiers hors connexion.

Remarque : Laissez tous les ordinateurs virtuels dans leur état actuel pour la démonstration suivante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Protection des fichiers et des dossiers partagés à l'aide de clichés instantanés

Vous utilisez des clichés instantanés pour restaurer des versions précédentes de fichiers et de dossiers. Il est nettement plus rapide de restaurer une version précédente d'un fichier à partir d'un cliché instantané qu'à partir d'une copie de sauvegarde traditionnelle qui pourrait être stockée hors site. Les fichiers et les dossiers peuvent être récupérés par les administrateurs, ou directement par les utilisateurs finaux.

Cette leçon présente aux stagiaires les clichés instantanés et leur montre comment configurer une planification de clichés instantanés dans Windows Server 2012.

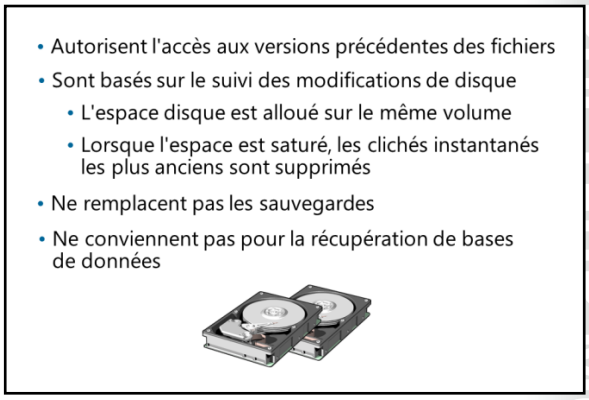
Objectifs de la leçon

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

- décrire les clichés instantanés ;
- décrire les considérations pour la planification de clichés instantanés ;
- identifier les méthodes de restauration des données à partir des clichés instantanés ;
- restaurer des données à partir d'un cliché instantané.

Que sont les clichés instantanés ?

Un *cliché instantané* est une image statique (ou une *capture instantanée*) d'un ensemble de données, tel qu'un fichier ou un dossier. Les clichés instantanés permettent de récupérer des fichiers et des dossiers en fonction des captures instantanées qui sont prises des lecteurs de stockage. Après une capture instantanée, vous pouvez visualiser et éventuellement restaurer les versions précédentes des fichiers et des dossiers qui existaient au moment où la capture instantanée a été effectuée.



Un cliché instantané n'effectue pas une copie complète de tous les fichiers pour chaque capture instantanée. Au lieu de cela, après une capture instantanée, Windows Server 2012 effectue le suivi des modifications sur le lecteur. Une quantité spécifique d'espace disque est allouée pour le suivi des blocs modifiés du disque. Quand vous accédez à une version précédente d'un fichier, une partie du contenu peut figurer dans la version actuelle du fichier et une autre dans la capture instantanée.

Par défaut, les blocs modifiés du disque sont stockés sur le même lecteur que le fichier original, mais vous pouvez modifier ce comportement. Vous pouvez également définir la quantité d'espace disque allouée pour les clichés instantanés. Plusieurs captures instantanées sont retenues jusqu'à ce que l'espace disque alloué soit saturé, après quoi, les captures instantanées les plus vieilles sont supprimées pour faire de la place pour de nouvelles captures instantanées. La quantité d'espace disque utilisée par une capture instantanée est basée sur la taille des modifications du disque entre les captures instantanées.

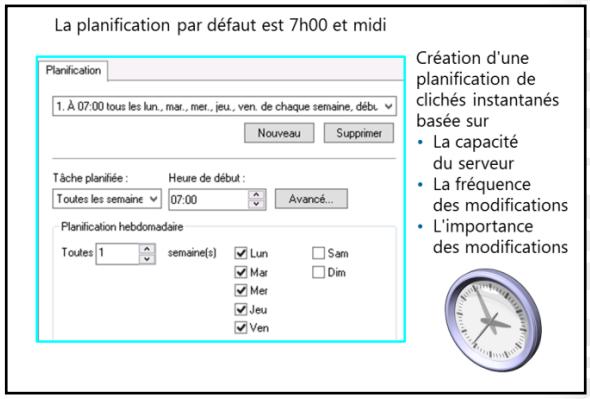
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Puisqu'une capture instantanée n'est pas une copie complète des fichiers, vous ne pouvez pas utiliser les clichés instantanés pour remplacer des sauvegardes traditionnelles. Si le disque contenant un lecteur est perdu ou endommagé, les captures instantanées de ce lecteur sont également perdues.

Les clichés instantanés conviennent pour la récupération des fichiers de données, mais pas pour des données plus complexes (telles que des bases de données), qui doivent être cohérentes logiquement avant qu'une sauvegarde soit effectuée. Une base de données restaurée à partir de versions précédentes est susceptible d'être endommagée et de requérir des réparations de base de données.

Éléments à prendre en compte pour la planification des clichés instantanés

La planification par défaut pour la création de clichés instantanés est du lundi au vendredi à 7h00 du matin, et de nouveau à midi. Vous pouvez modifier la planification par défaut comme vous le souhaitez pour votre organisation.

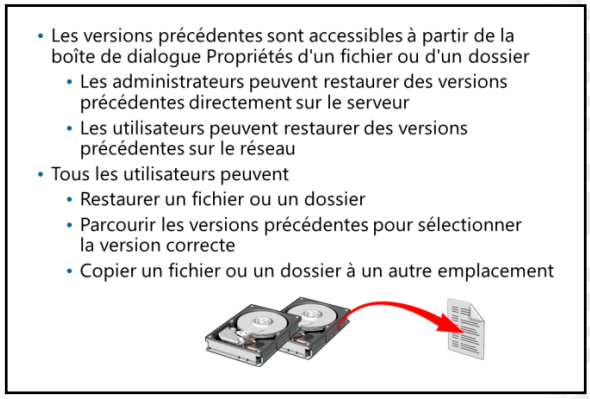


Lorsque vous planifiez des clichés instantanés :

- Considérez que l'augmentation de la fréquence des clichés instantanés augmente la charge qui pèse sur le serveur. Il est recommandé de ne pas planifier de clichés instantanés de lecteur plus d'une fois par heure.
- Augmentez la fréquence des clichés instantanés pour des données qui changent souvent. Ceci augmente la probabilité de capturer les modifications récentes des fichiers.
- Augmentez la fréquence des clichés instantanés pour les données importantes. Ceci augmente la probabilité de capturer les modifications récentes des fichiers.

Restauration de données à partir d'un cliché instantané

Les versions précédentes des fichiers peuvent être restaurées par les utilisateurs ou les administrateurs. La plupart des utilisateurs ignorent qu'ils peuvent faire ceci et ils auront besoin d'instructions sur la façon de restaurer une version précédente d'un fichier.



Les administrateurs peuvent accéder aux versions précédentes des fichiers directement sur le serveur qui stocke les fichiers. Les utilisateurs peuvent accéder aux versions précédentes des fichiers via le réseau à partir d'un partage de fichiers. Dans les deux cas, les versions précédentes sont accessibles à partir de la boîte de dialogue **Propriétés** du fichier ou du dossier. Les administrateurs peuvent restaurer des versions précédentes des fichiers directement sur le serveur, alors que les utilisateurs peuvent restaurer des versions précédentes pour les fichiers et les dossiers partagés auxquels ils peuvent accéder via le réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors de l'affichage de versions précédentes d'un dossier, vous pouvez parcourir les fichiers disponibles et sélectionner seulement le fichier dont vous avez besoin. Si plusieurs versions des fichiers sont disponibles, vous pouvez examiner chaque version avant de décider laquelle restaurer. Enfin, vous pouvez copier une version précédente d'un fichier dans un autre emplacement au lieu de la restaurer à son emplacement précédent. Ceci évite de remplacer la version actuelle du fichier.

Les systèmes d'exploitation clients Windows XP avec Service Pack 2 (SP2) ou ultérieurs, Windows Vista et Windows 7 sont capables d'accéder aux versions précédentes des fichiers sans qu'aucun logiciel supplémentaire ne soit installé. La capacité à accéder aux versions précédentes des fichiers n'est plus prise en charge dans les systèmes d'exploitation Windows antérieurs à Windows XP avec SP2.

Démonstration : Restauration de données à partir d'un cliché instantané

Vous pouvez créer des clichés instantanés en utilisant la planification par défaut ou vous pouvez modifier la planification pour fournir des captures instantanées plus fréquentes. Dans les deux cas, vous verrez uniquement les versions du fichier tel qu'il a changé. La réalisation d'un cliché instantané d'un fichier qui n'a pas changé n'exerce aucun effet réel sur le cliché instantané. Aucune version supplémentaire n'est disponible et aucun espace n'est utilisé dans la capture instantanée pour ce fichier particulier.

Dans cette démonstration, vous allez apprendre à :

- configurer des clichés instantanés ;
- créer un nouveau fichier ;
- créer un cliché instantané ;
- modifier le fichier ;
- restaurer la version précédente.

Procédure de démonstration

Configurer des clichés instantanés

1. Sur LON-SVR1, ouvrez l'**Explorateur de fichiers**.
2. Activez les clichés instantanés pour **Disque local (C:)**.

Créer un nouveau fichier

1. Ouvrez l'**Explorateur de fichiers**.
2. Créez un dossier sur le lecteur C:, nommé **Données**.
3. Créez un fichier texte nommé **TestFile.txt** dans le dossier Données.
4. Modifiez le contenu de **TestFile.txt** en ajoutant et en enregistrant le texte **Version 1**.

Créer un cliché instantané

1. Dans l'Explorateur de fichiers, cliquez avec le bouton droit sur **Disque local (C:)**, puis cliquez sur **Configurer les clichés instantanés**.
2. Dans la fenêtre Clichés instantanés, cliquez sur **Créer**.
3. Une fois le cliché instantané terminé, cliquez sur **OK**.

Modifier le fichier

1. Dans l'Explorateur de fichiers, double-cliquez sur **TestFile.txt** pour ouvrir le document.
2. Dans le Bloc-notes, tapez **Version 2**.
3. Fermez le Bloc-notes et cliquez sur **Enregistrer** pour enregistrer les modifications.

Restaurer la version précédente

1. Dans l'Explorateur de fichiers, cliquez avec le bouton droit sur **TestFile.txt**, puis cliquez sur **Restaurer les versions précédentes**.
2. Restaurez la version la plus récente.
3. Dans la fenêtre d'avertissement, cliquez sur **Restaurer**.
4. Ouvrez **TestFile.txt** pour ouvrir le document et vérifiez que la version précédente est restaurée.

Remarque : Laissez tous les ordinateurs virtuels dans leur état actuel pour la démonstration suivante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration de l'impression réseau

En utilisant le rôle Services d'impression et de numérisation de document dans Windows Server 2012, vous pouvez partager des imprimantes dans un réseau et centraliser la gestion des serveurs d'impression et des imprimantes réseau. La console de gestion de l'impression vous permet de surveiller les files d'attente d'impression et de recevoir des notifications importantes concernant l'activité des serveurs d'impression.

Windows Server 2012 présente de nouvelles fonctionnalités et modifications importantes au rôle Services d'impression et de numérisation de document que vous pouvez utiliser pour mieux gérer votre environnement d'impression réseau. Cette leçon explique les aspects importants de l'impression réseau et présente les nouvelles fonctionnalités d'impression réseau disponibles dans Windows Server 2012.

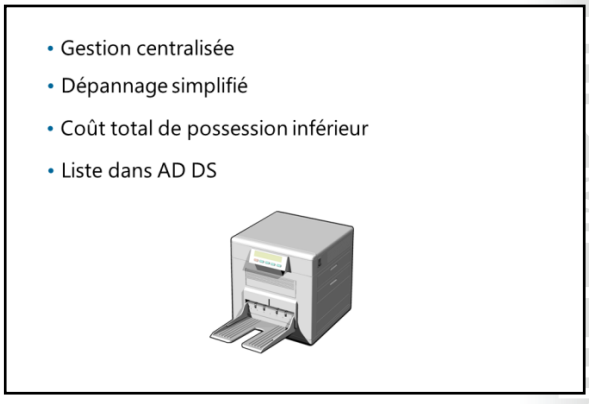
Objectifs de la leçon

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

- identifier les avantages de l'impression réseau ;
- décrire l'opération améliorée Pointer et imprimer ;
- identifier les options de sécurité pour l'impression réseau ;
- créer plusieurs configurations pour un périphérique d'impression ;
- décrire le pool d'imprimantes ;
- décrire l'impression directe pour les filiales ;
- identifier les méthodes pour déployer des imprimantes sur les clients.

Avantages de l'impression réseau

Vous pouvez configurer l'impression réseau en utilisant Windows Server 2012 en tant que serveur d'impression pour les utilisateurs. Dans cette configuration, les ordinateurs clients soumettent les travaux d'impression au serveur d'impression pour les remettre à une imprimante connectée au réseau.



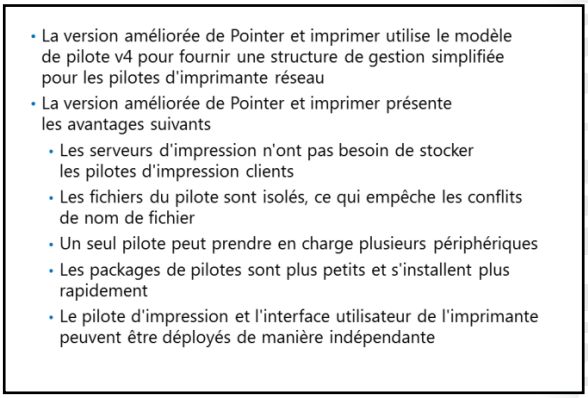
Avantages de l'impression réseau

- Gestion centralisée. Le plus grand avantage lié à l'utilisation de Windows Server 2012 en tant que serveur d'impression est la gestion centralisée de l'impression. Au lieu de gérer les connexions des clients à de nombreux périphériques individuels, vous gérez leur connexion au serveur. Vous installez des pilotes d'imprimante de manière centralisée sur le serveur et les distribuez aux stations de travail.
- Dépannage simplifié. En installant les pilotes d'imprimante de manière centralisée sur un serveur, vous simplifiez également la résolution des problèmes. Il est relativement facile de déterminer si des problèmes d'impression sont provoqués par l'imprimante, le serveur ou l'ordinateur client.

- Coûts réduits. Une imprimante réseau est plus chère que celles utilisées habituellement pour l'impression locale, mais elle présente également des coûts sensiblement inférieurs en matière de consommables et une impression de meilleure qualité. Par conséquent, le coût de l'impression est minimisé car le coût initial de l'imprimante est réparti entre tous les ordinateurs qui se connectent à cette imprimante. Par exemple, une imprimante réseau unique peut servir à 100 utilisateurs ou plus.
- Les utilisateurs peuvent aisément rechercher des imprimantes. Vous pouvez également publier des imprimantes réseau dans AD DS, ce qui permet aux utilisateurs de rechercher des imprimantes dans leur domaine.

Qu'est-ce que l'opération améliorée Pointer et imprimer ?

L'opération améliorée Pointer et imprimer est une nouvelle fonctionnalité de Windows Server 2012, qui facilite l'installation de pilotes pour les imprimantes réseau. L'opération améliorée Pointer et imprimer utilise le nouveau type de pilote de version 4 (v4) qui est introduit dans Windows Server 2012 et Windows 8.



Présentation des pilotes V3 et V4

Le standard de pilote d'imprimante Windows qui est utilisé dans les versions antérieures de Windows Server a existé sous une forme relativement identique depuis l'introduction des pilotes de version 3 (v3) dans les systèmes d'exploitation Microsoft Windows 2000. Avec les pilotes v3, les fabricants d'imprimantes créent des pilotes d'impression personnalisés pour chaque appareil spécifique qu'ils produisent, pour garantir que les applications Windows peuvent utiliser toutes leurs fonctionnalités d'impression. Avec le modèle v3, la gestion de l'infrastructure d'imprimante exige des administrateurs qu'ils conservent des pilotes pour chaque périphérique d'impression dans l'environnement, ainsi que des pilotes 32 bits et 64 bits distincts pour un périphérique d'impression unique, afin de prendre en charge les deux plateformes.

Présentation du pilote d'imprimante V4

Windows Server 2012 et Windows 8 incluent la prise en charge des pilotes d'impression v4, qui permet une gestion et une installation améliorées des pilotes de périphérique d'impression. Sous le modèle v4, les fabricants de périphériques d'impression peuvent créer des pilotes de classe d'impression qui prennent en charge un langage et des fonctionnalités d'impression similaires qui peuvent être communs à un grand ensemble de périphériques. Les langages d'impression communs peuvent inclure le langage PCL (Printer Control Language), .ps ou XPS (XML Paper Specification).

Les pilotes V4 sont en général délivrés à l'aide de Windows Update ou de Windows Software Update Services. À la différence des pilotes v3, les pilotes v4 ne sont pas délivrés à partir d'un magasin d'impression hébergé sur le serveur d'impression.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le modèle de pilote V4 offre les avantages suivants :

- Le partage d'une imprimante ne requiert pas la fourniture de pilotes correspondant à l'architecture cliente.
- Les fichiers de pilote sont isolés pilote par pilote, ce qui évite les conflits de noms de fichier de pilote.
- Un seul pilote peut prendre en charge plusieurs périphériques.
- Les packages de pilotes sont plus petits et plus simples que les pilotes v3, ce qui favorise des temps d'installation de pilote plus courts.
- Le pilote d'imprimante et l'interface utilisateur de l'imprimante peuvent être déployés de manière indépendante.

Utilisation de l'opération améliorée Pointer et imprimer pour l'installation des pilotes

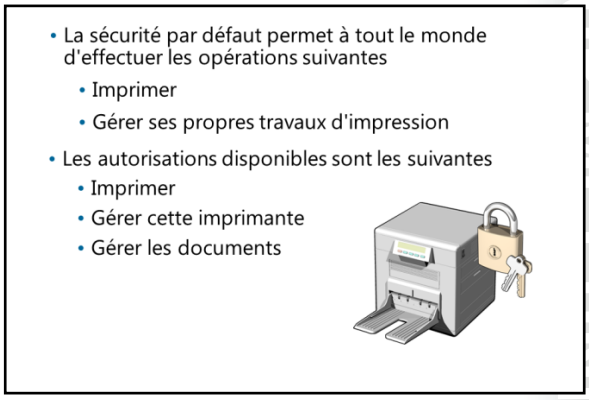
Sous le modèle v4, le partage d'imprimantes et l'installation de pilotes fonctionnent automatiquement sous l'opération améliorée Pointer et imprimer. Lorsqu'une imprimante réseau est installée sur un ordinateur client, le serveur et le client fonctionnent ensemble pour identifier le périphérique d'impression. Le pilote s'installe alors directement à partir du magasin de pilotes sur l'ordinateur client, ou à partir de Windows Update ou de Windows Software Update Services.

Avec l'opération améliorée Pointer et imprimer, les pilotes de périphérique d'impression n'ont plus besoin d'être conservés sur le serveur d'impression. L'installation de pilotes pour les périphériques d'impression réseau est accélérée parce que les pilotes d'imprimante n'ont plus besoin d'être transférés via le réseau du serveur au client.

Si le magasin de pilotes sur l'ordinateur client ne contient pas de pilote pour l'imprimante réseau en cours d'installation, et s'il est impossible d'obtenir un pilote approprié à partir de Windows Update ou de Windows Server Update Services, Windows utilise un mécanisme de rappel pour activer l'impression interplateforme à l'aide du pilote d'impression issu du serveur d'impression.

Options de sécurité pour l'impression réseau

Quand une imprimante est partagée via un réseau, aucune sécurité n'est requise dans de nombreux cas. L'imprimante est considérée d'accès libre, ce qui signifie que chacun est autorisé à l'utiliser pour imprimer. Ceci est la configuration par défaut pour une imprimante qui est partagée sur un serveur Windows.



Les autorisations disponibles pour l'impression partagée incluent les autorisations suivantes :

- Imprimer : cette autorisation permet aux utilisateurs d'imprimer des documents sur l'imprimante. Par défaut, le groupe Tout le monde dispose de cette autorisation.
- Gérer cette imprimante : cette autorisation permet aux utilisateurs de modifier les paramètres de l'imprimante, y compris de mettre à jour les pilotes. Par défaut, cette autorisation est accordée aux administrateurs, aux opérateurs de serveur et aux opérateurs d'impression.
- Gestion des documents : cette autorisation permet aux utilisateurs de modifier et de supprimer des travaux d'impression dans la file d'attente. Cette autorisation est attribuée au CRÉATEUR PROPRIÉTAIRE, ce qui signifie que l'utilisateur qui crée un travail d'impression gère ce travail. Les administrateurs, les opérateurs de serveur et les opérateurs d'impression disposent également de cette autorisation pour tous les travaux d'impression.

Démonstration : Création de plusieurs configurations pour un périphérique d'impression

La création de plusieurs configurations pour un périphérique d'impression vous permet d'attribuer des files d'attente d'impression à des utilisateurs ou des groupes spécifiques de sorte qu'ils puissent imprimer des travaux prioritaires sur une imprimante en cours d'utilisation par d'autres utilisateurs. Lorsqu'un travail d'impression est envoyé à la file d'attente d'impression prioritaire, le serveur d'impression traite ce travail avant tous les travaux provenant de la file d'attente de priorité normale.

Dans cette démonstration, vous allez apprendre à :

- créer une imprimante partagée ;
- créer une deuxième imprimante partagée utilisant le même port ;
- augmenter la priorité d'impression pour une file d'attente d'impression prioritaire.

Procédure de démonstration

Créer une imprimante partagée

1. Ouvrez la fenêtre Périphériques et imprimantes.
2. Ajoutez une imprimante utilisant le port local **LPT1** et le pilote de classe **Brother Color Leg Type1**.
3. Nommez l'imprimante **AllUsers**.
4. Partagez l'imprimante en utilisant les paramètres par défaut.

Créer une deuxième imprimante partagée utilisant le même port

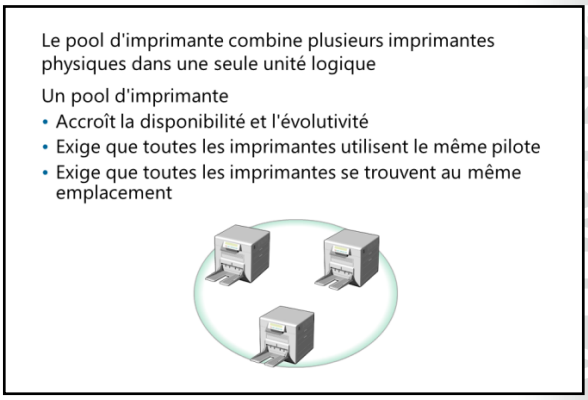
1. Ouvrez la fenêtre Périphériques et imprimantes.
2. Ajoutez une imprimante utilisant le port local **LPT1** et le pilote de classe **Brother Color Leg Type1**.
3. Nommez l'imprimante **Executives**.
4. Partagez l'imprimante en utilisant les paramètres par défaut.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Augmenter la priorité d'impression pour une file d'attente d'impression prioritaire

1. Ouvrez la fenêtre de propriétés Imprimante Executives.
2. Augmentez la priorité en spécifiant **10**.

Qu'est-ce que le pool d'imprimantes ?



Le *pool d'imprimantes* est une manière d'associer plusieurs imprimantes physiques en une seule unité logique. Pour les ordinateurs clients, le pool d'imprimantes apparaît comme une imprimante unique. Lorsque des travaux sont soumis au pool d'imprimantes, n'importe quelle imprimante disponible dans le pool d'imprimantes peut les traiter.

Le pool d'imprimantes augmente l'évolutivité et la disponibilité de l'impression réseau. Si une imprimante dans le pool est non disponible (par exemple, en raison d'un travail d'impression de grande envergure, d'un bourrage papier ou de son état hors connexion), tous les travaux sont distribués aux imprimantes restantes. Si un pool d'imprimantes n'a pas une capacité suffisante, vous pouvez ajouter une autre imprimante au pool d'imprimantes sans effectuer aucune configuration des clients.

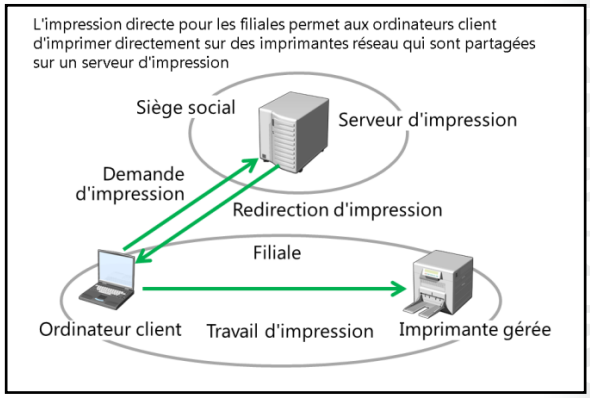
Un pool d'imprimantes est configuré sur un serveur en spécifiant plusieurs ports pour une imprimante. Chaque port correspond à l'emplacement d'une imprimante physique. Dans la plupart des cas, les ports correspondent à une adresse IP sur le réseau plutôt qu'à une connexion LPT ou USB.

Les conditions requises pour un pool d'imprimantes sont les suivantes :

- Les imprimantes doivent utiliser le même pilote : les clients utilisent un pilote d'imprimante unique pour générer les travaux d'impression. Toutes les imprimantes doivent accepter les travaux d'impression dans le même format. Dans de nombreux cas, ceci signifie qu'un modèle unique d'imprimante est utilisé.
- Les imprimantes doivent être dans le même emplacement : les imprimantes d'un pool d'imprimantes doivent être physiquement proches les unes des autres. Lorsque les utilisateurs récupèrent leurs travaux d'impression, ils doivent passer en revue toutes les imprimantes du pool d'imprimantes pour trouver leur document. Les utilisateurs n'ont aucun moyen de savoir quelle imprimante a imprimé leur document.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que l'impression directe pour les filiales ?



L'impression directe pour les filiales réduit les coûts du réseau pour les organisations qui ont centralisé leurs rôles Windows Server. Lorsque l'impression directe pour les filiales est activée, les clients Windows obtiennent les informations sur l'imprimante à partir du serveur d'impression, mais envoient les travaux d'impression directement à l'imprimante. Les données d'impression ne transitent plus par le serveur central avant de revenir à l'imprimante de la filiale. Cette configuration réduit le trafic entre l'ordinateur client, le serveur d'impression et l'imprimante de la filiale, et se traduit par une hausse de l'efficacité du réseau.

L'impression directe pour les filiales est transparente à l'utilisateur. En outre, l'utilisateur est en mesure d'imprimer même si le serveur d'impression est non disponible pour une raison quelconque (par exemple, si la liaison WAN [réseau étendu] au centre de données est interrompue). Ceci est dû au fait que les informations sur l'imprimante sont mises en cache sur l'ordinateur client dans la filiale.

Configuration de l'impression directe pour les filiales

L'impression directe pour les filiales est configurée par un administrateur à l'aide de la console de gestion de l'impression ou de l'interface de ligne de commande Windows PowerShell.

Pour configurer l'impression directe pour les filiales dans la console de gestion de l'impression, procédez comme suit :

1. Dans le Gestionnaire de serveur, ouvrez la console de **gestion de l'impression**.
2. Dans le volet de navigation, développez Serveurs d'impression, puis développez le serveur d'impression qui héberge l'imprimante réseau pour laquelle l'impression directe pour les filiales sera activée.
3. Cliquez sur le nœud **Imprimantes**, cliquez avec le bouton droit sur l'imprimante souhaitée, puis cliquez sur **Activer l'impression directe pour les filiales**.

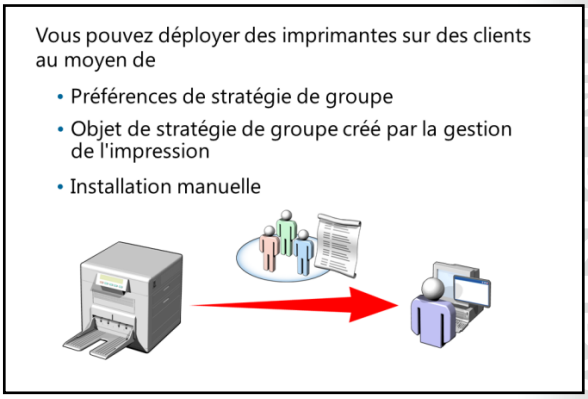
Pour configurer l'impression directe pour les filiales à l'aide de Windows PowerShell, tapez l'applet de commande suivante à une invite Windows PowerShell :

```
Set-Printer -name "<Nom de l'imprimante>" -ComputerName <Nom du serveur d'impression> -
RenderingMode BranchOffice
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Déploiement d'imprimantes sur des clients

Le déploiement d'imprimantes sur les clients est une partie essentielle de la gestion des services d'impression dans le réseau. Un système bien conçu pour déployer les imprimantes est évolutif et peut être utilisé pour gérer des centaines ou des milliers d'ordinateurs.



Les options de déploiement des imprimantes sont les suivantes :

- Préférences des stratégies de groupe. Vous pouvez utiliser les préférences des stratégies de groupe pour déployer des imprimantes partagées sur des clients Windows XP, Windows Vista, Windows 7 et Windows 8. L'imprimante peut être associée avec le compte d'utilisateur ou le compte d'ordinateur, et peut être ciblée par groupe. Pour les ordinateurs exécutant Windows XP, vous devez installer l'extension Stratégie de groupe Client de préférences.
- Objet de stratégie de groupe créé par la gestion de l'impression. L'outil d'administration de gestion de l'impression peut ajouter des imprimantes à un objet GPO pour leur distribution sur les ordinateurs clients sur la base d'un compte d'utilisateur ou d'un compte d'ordinateur. Les ordinateurs Windows XP doivent être configurés pour exécuter PushPrinterConnections.exe.
- Installation manuelle. Chaque utilisateur peut ajouter des imprimantes manuellement en parcourant le réseau ou en utilisant l'Assistant Ajout d'imprimante. Il est important de noter que les imprimantes réseau qui sont installées manuellement sont disponibles seulement pour l'utilisateur qui les a installées. Si plusieurs utilisateurs partagent un ordinateur, chacun d'eux doit installer l'imprimante manuellement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation des services de fichier et d'impression

Scénario

Votre responsable vous a récemment demandé de configurer les services de fichiers et d'impression pour la filiale. Ceci vous oblige à configurer un nouveau dossier partagé qui sera utilisé par plusieurs services, à configurer des clichés instantanés sur les serveurs de fichiers et à configurer un pool d'imprimantes.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- créer et configurer un partage de fichiers ;
- configurer des clichés instantanés ;
- créer et configurer un pool d'imprimantes.

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	22410B-LON-CL1 22410B-LON-DC1 22410B-LON-SVR1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur Gestionnaire Hyper-V®.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
5. Répétez les étapes 2 à 4 pour **22410B-LON-SVR1**. Répétez les étapes 2 et 3 pour **22410B-LON-CL1**. Ne vous connectez pas à LON-CL1 tant qu'il ne vous a pas été demandé de le faire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Création et configuration d'un partage de fichiers

Scénario

Votre responsable vous a demandé de créer un nouveau dossier partagé qui sera utilisé par tous les services. Il y aura un partage de fichiers unique avec des dossiers distincts pour chaque service. Pour garantir que les utilisateurs voient uniquement les fichiers auxquels ils ont accès, vous devez activer l'énumération basée sur l'accès sur le partage.

Des problèmes se sont produits dans d'autres filiales avec des conflits lorsque les fichiers hors connexion sont utilisés pour les structures de données partagées. Pour éviter les conflits, vous devez désactiver les fichiers hors connexion pour ce partage.

Les tâches principales de cet exercice sont les suivantes :

1. Créer l'arborescence du nouveau partage
2. Configurer des autorisations NTFS sur l'arborescence
3. Créer le dossier partagé
4. Tester l'accès au dossier partagé
5. Activer l'énumération basée sur l'accès
6. Tester l'accès au partage
7. Désactiver les fichiers hors connexion pour le partage

▶ Tâche 1 : Créer l'arborescence du nouveau partage

1. Sur LON-SVR1, ouvrez l'Explorateur de fichiers et créez les dossiers suivants :
   - **E:\Données**
   - **E:\Données\Development**
   - **E:\Données\Marketing**
   - **E:\Données\Research**
   - **E:\Données\Sales**

▶ Tâche 2 : Configurer des autorisations NTFS sur l'arborescence

1. Dans l'Explorateur de fichiers, bloquez l'héritage des autorisations NTFS pour **E:\Données** et, lorsque vous y êtes invité, convertissez les autorisations héritées en autorisations explicites.
2. Dans l'Explorateur de fichiers, supprimez les autorisations pour **LON-SVR1\Users** sur les sous-répertoires dans **E:\Données**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'Explorateur de fichiers, ajoutez les autorisations NTFS suivantes pour l'arborescence :

Dossier	Autorisations
E:\Données	Aucune modification
E:\Données\Development	Modification : ADATUM\Development
E:\Données\Marketing	Modification : ADATUM\Marketing
E:\Données\Research	Modification : ADATUM\Research
E:\Données\Sales	Modification : ADATUM\Sales

▶ Tâche 3 : Créer le dossier partagé

1. Dans l'Explorateur de fichiers, partagez le dossier **E:\Données**.
2. Attribuez les autorisations suivantes au dossier partagé :
   - Modification : **ADATUM\Utilisateurs authentifiés**

▶ Tâche 4 : Tester l'accès au dossier partagé

1. Connectez-vous à LON-CL1 en tant que **ADATUM\Bernard** avec le mot de passe **Pa$$w0rd**.

Remarque : Bernard est membre du groupe Development.

2. Ouvrez l'Explorateur de fichiers.
3. Accédez à **\\LON-SVR1\Données**.
4. Essayez d'ouvrir les dossiers **Development**, **Marketing**, **Research** et **Sales**.

Remarque : Bernard doit avoir accès au dossier Development. Toutefois, bien que Bernard puisse encore voir les autres dossiers, il n'a pas accès à leur contenu.

5. Déconnectez-vous de LON-CL1.

▶ Tâche 5 : Activer l'énumération basée sur l'accès

1. Basculez vers **LON-SVR1**.
2. Ouvrez le **Gestionnaire de serveur**.
3. Cliquez sur **Services de fichiers et de stockage**.
4. Cliquez sur **Partages**.
5. Ouvrez la fenêtre Propriétés pour le partage de **Données** et, dans la page **Paramètres**, activez l'option **Énumération basée sur l'accès**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 6 : Tester l'accès au partage

1. Connectez-vous à **LON-CL1** en tant que **ADATUM\Bernard** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez une fenêtre de l'Explorateur de fichiers et accédez à **\\LON-SVR1\Données**.

Remarque : Bernard peut à présent visualiser uniquement le dossier Development, le dossier pour lequel des autorisations lui ont été attribuées.

3. Ouvrez le dossier **Development** pour confirmer l'accès.
4. Déconnectez-vous de LON-CL1.

▶ Tâche 7 : Désactiver les fichiers hors connexion pour le partage

1. Basculez vers **LON-SVR1**.
2. Ouvrez l'**Explorateur de fichiers**.
3. Accédez au lecteur **Allfiles (E:)**.
4. Ouvrez la fenêtre Propriétés pour le dossier Données et désactivez la mise en cache des fichiers hors connexion.

Résultats : À la fin de cet exercice, vous aurez créé un nouveau dossier partagé à l'usage de plusieurs services.

Exercice 2 : Configuration de clichés instantanés

Scénario

La société A. Datum Corporation stocke des sauvegardes quotidiennes hors site pour permettre une récupération d'urgence. Chaque matin, la sauvegarde de la nuit précédente est placée hors site. La récupération d'un fichier de la sauvegarde exige le renvoi sur site des bandes de sauvegarde. La durée globale de récupération d'un fichier de la sauvegarde peut être d'une journée ou plus.

Votre responsable vous a demandé de garantir l'activation des clichés instantanés sur le serveur de fichiers afin que vous puissiez restaurer les fichiers récemment modifiés ou supprimés sans utiliser de bande de sauvegarde. Puisque les données propres à cette filiale changent fréquemment, il vous a été demandé de configurer la création d'un cliché instantané toutes les heures.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer des clichés instantanés pour le partage de fichiers
2. Créer plusieurs clichés instantanés d'un fichier
3. Récupérer un fichier supprimé à partir d'un cliché instantané

▶ Tâche 1 : Configurer des clichés instantanés pour le partage de fichiers

1. Basculez vers **LON-SVR1**.
2. Ouvrez l'**Explorateur de fichiers**.
3. Accédez au lecteur E, cliquez avec le bouton droit sur **Allfiles (E:)**, puis cliquez sur **Configurer les clichés instantanés**.
4. Activez les **clichés instantanés** pour le lecteur E.
5. Configurez les paramètres pour planifier un cliché instantané toutes les heures pour le lecteur E.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer plusieurs clichés instantanés d'un fichier

1. Sur LON-SVR1, basculez vers l'**Explorateur de fichiers** et accédez au dossier **E:\Données\Development**.
2. Créez un nouveau fichier texte nommé **Report.txt**.
3. Revenez à la boîte de dialogue **Propriétés de Allfiles (E:)** ; elle devrait être encore ouverte dans l'onglet Clichés instantanés. Cliquez sur **Créer**.

▶ Tâche 3 : Récupérer un fichier supprimé à partir d'un cliché instantané

1. Sur LON-SVR1, revenez à la fenêtre de l'Explorateur de fichiers.
2. Supprimez le fichier **Report.txt**.
3. Ouvrez la boîte de dialogue **Propriétés** pour **E:\Données\Development**, puis cliquez sur l'onglet **Versions précédentes**.
4. Ouvrez la version la plus récente du dossier **Development**, puis copiez le fichier **Report.txt**.
5. Collez le fichier dans le dossier **Development**.
6. Fermez l'Explorateur de fichiers et toutes les fenêtres ouvertes.

Résultats : À la fin de cet exercice, vous aurez activé des clichés instantanés sur le serveur de fichiers.

Exercice 3 : Création et configuration d'un pool d'imprimantes

Scénario

Votre responsable vous a demandé de créer une nouvelle imprimante partagée pour votre filiale. Toutefois, au lieu de créer l'imprimante partagée sur le serveur local dans la filiale, il vous a demandé de créer l'imprimante partagée dans le siège social et d'utiliser l'impression directe pour les filiales. Ceci permet de gérer l'imprimante dans le siège social, mais empêche les travaux d'impression d'être transmis via les liaisons WAN.

Pour garantir la haute disponibilité de cette imprimante, vous devez formater cette dernière en tant qu'imprimante mise en pool. Deux périphériques d'impression physiques du même modèle ont été installés dans la filiale à cet effet.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le rôle serveur Services d'impression et de numérisation de document
2. Installer une imprimante
3. Configurer le pool d'imprimantes
4. Installer une imprimante sur un ordinateur client
5. Pour préparer le module suivant

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Installer le rôle serveur Services d'impression et de numérisation de document

1. Sur LON-SVR1, ouvrez le **Gestionnaire de serveur**.
2. Installez le rôle Services de document et d'impression et acceptez les paramètres par défaut.

▶ Tâche 2 : Installer une imprimante

1. Sur LON-SVR1, utilisez la console de gestion de l'impression pour installer une imprimante avec les paramètres suivants :
   - Adresse IP : **172.16.0.200**
   - Pilote : **Microsoft XPS Class Driver**
   - Nom : **Imprimante de filiale**
2. Partagez l'imprimante.
3. Répertoriez l'imprimante dans AD DS.
4. Activez l'impression directe pour les filiales.

▶ Tâche 3 : Configurer le pool d'imprimantes

1. Sur LON-SVR1, dans la console de gestion de l'impression, créez un nouveau port avec la configuration suivante :
   - Type : **Port TCP/IP standard**
   - Adresse IP : **172.16.0.201**
   - Connexion : **Generic Network Card**
2. Ouvrez la page **Propriétés de Imprimante de filiale**, et, dans l'onglet **Ports**, activez le pool d'imprimantes.
3. Sélectionnez le port **172.16.0.201** comme deuxième port.

▶ Tâche 4 : Installer une imprimante sur un ordinateur client

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ajoutez une imprimante, en sélectionnant **Imprimante de filiale sur LON-SVR1**.

▶ Tâche 5 : 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 **22410B-LON-SVR1**, puis cliquez sur **Rétablir**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22410B-LON-CL1** et **22410B-LON-DC1**.

Résultats : À la fin de cet exercice, vous aurez installé le rôle serveur Services de documents et d'impression et installé une imprimante avec le pool d'imprimantes.

Question : Comment l'implémentation de l'énumération basée sur l'accès bénéficie-t-elle aux utilisateurs du dossier partagé Données dans cet atelier pratique ?

Question : Existe-t-il une autre manière de récupérer le fichier dans l'exercice relatif aux clichés instantanés ? Quel avantage les clichés instantanés offrent-ils en comparaison ?

Question : Dans l'exercice 3, comment pourriez-vous configurer l'impression directe pour les filiales si vous étiez dans un emplacement distant et n'aviez pas accès à l'interface graphique utilisateur de Windows Server 2012 pour le serveur d'impression ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Comment l'héritage affecte-t-il les autorisations explicitement attribuées sur un fichier ?

Question : Pourquoi ne devriez-vous pas utiliser les clichés instantanés comme moyen de sauvegarde des données ?

Question : Dans quels scénarios l'impression directe pour les filiales peut-elle être avantageuse ?

Outils

Nom de l'outil	Utilisé pour	Emplacement
Outil Autorisations effectives	Évaluation des autorisations combinées pour un fichier, un dossier ou un dossier partagé.	Sous **Avancé**, dans l'onglet **Sécurité** de la boîte de dialogue **Propriétés** d'un fichier, d'un dossier ou d'un dossier partagé.
Outil en ligne de commande **Net use**	Configuration des composants réseau de Windows Server 2012.	Invite de commandes.
Console de gestion de l'impression	Gestion de l'environnement d'impression dans Windows Server 2012.	Menu Outils dans le Gestionnaire de serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11

Implémentation d'une stratégie de groupe

Table des matières :

Vue d'ensemble du module **11-1**

Leçon 1 : Vue d'ensemble d'une stratégie de groupe **11-2**

Leçon 2 : Traitement d'une stratégie de groupe **11-11**

Leçon 3 : Implémentation d'un magasin central pour les modèles d'administration **11-18**

Atelier pratique : Implémentation d'une stratégie de groupe **11-23**

Contrôle des acquis et éléments à retenir **11-27**

Vue d'ensemble du module

Assurer la maintenance d'un environnement informatique cohérent au sein d'une organisation représente un véritable défi. Les administrateurs ont besoin d'un mécanisme pour configurer et appliquer les paramètres et les restrictions des ordinateurs et des utilisateurs. La stratégie de groupe peut fournir cette cohérence en permettant aux administrateurs de gérer et d'appliquer les paramètres de configuration de manière centralisée.

Ce module fournit une vue d'ensemble d'une stratégie de groupe et fournit des informations détaillées sur la procédure d'implémentation des objets de stratégie de groupe.

Objectifs

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

- créer et gérer des objets de stratégie de groupe ;
- décrire le traitement de stratégie de groupe ;
- implémenter un magasin central pour les modèles d'administration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble d'une stratégie de groupe

La stratégie de groupe vous permet de contrôler l'environnement informatique. Afin de pouvoir l'appliquer correctement, il est important de comprendre comment la stratégie de groupe fonctionne. Cette leçon fournit une vue d'ensemble de la structure d'une stratégie de groupe, et définit les objets de stratégie de groupe locale et basée sur un domaine. Elle décrit également les types de paramètre disponibles pour les utilisateurs et les groupes.

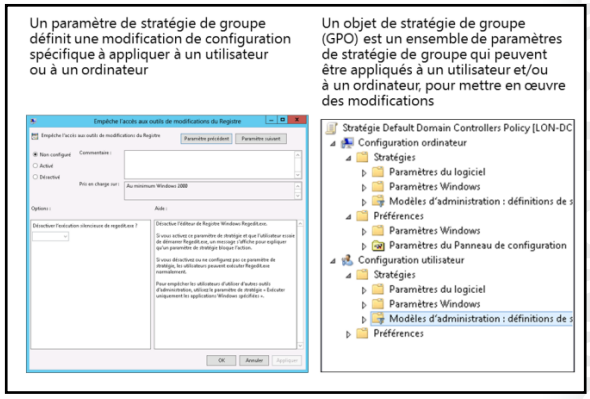
Objectifs de la leçon

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

- décrire les composants de la stratégie de groupe ;
- décrire les objets de stratégie de groupe locale multiple ;
- décrire les options de stockage des objets de stratégie de groupe de domaine ;
- décrire les préférences et les stratégies d'objet de stratégie de groupe ;
- décrire les objets de stratégie de groupe Starter ;
- décrire le processus de délégation de la gestion des objets de stratégie de groupe ;
- décrire le processus de création et de gestion des objets de stratégie de groupe.

Composants de la stratégie de groupe

Les paramètres de stratégie de groupe sont des paramètres de configuration qui permettent aux administrateurs d'appliquer des paramètres en modifiant les paramètres du Registre spécifiques à l'utilisateur et spécifiques à l'ordinateur sur les ordinateurs basés sur un domaine. Vous pouvez regrouper des paramètres de stratégie de groupe pour créer des objets de stratégie de groupe, que vous pouvez ensuite appliquer aux utilisateurs ou aux ordinateurs.



Objets de stratégie de groupe

Un *objet de stratégie de groupe* est un objet qui contient un ou plusieurs paramètres de stratégie qui appliquent un paramètre de configuration pour les utilisateurs, les ordinateurs ou les deux. Les modèles d'objets de stratégie de groupe sont stockés dans SYSVOL tandis que les objets des conteneurs d'objets de stratégie de groupe sont stockés dans AD DS. Les objets de stratégie de groupe peuvent être gérés à l'aide de la console Gestion des stratégies de groupe (GPMC). Dans cette console, vous pouvez ouvrir et modifier un objet de stratégie de groupe à l'aide de l'Éditeur de gestion des stratégies de groupe. Les objets de stratégie de groupe sont liés logiquement à des conteneurs Active Directory® pour appliquer des paramètres aux objets contenus dans ces conteneurs. Les objets de stratégie de groupe ne peuvent pas être reliés aux conteneurs Utilisateurs et Ordinateurs. Ils peuvent être reliés à des sites, des domaines et des unités d'organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Paramètres de stratégie de groupe

Un paramètre de stratégie de groupe est le composant le plus précis de la stratégie de groupe. Il définit une modification de configuration spécifique à appliquer à un objet (un ordinateur, un utilisateur, ou les deux) au sein des services de domaine Active Directory (AD DS). Une stratégie de groupe a des milliers de paramètres configurables. Ces paramètres peuvent affecter presque chaque zone de l'environnement informatique. Les paramètres ne peuvent pas tous être appliqués à toutes les versions antérieures des systèmes d'exploitation Windows Server® et Windows®. Chaque nouvelle version introduit de nouveaux paramètres et de nouvelles fonctions qui s'appliquent uniquement à cette version spécifique. Si un paramètre de stratégie de groupe est appliqué à un ordinateur qui ne peut pas le traiter, celui-ci l'ignore simplement.

La plupart des paramètres de stratégie ont trois états :

- Non configuré. L'objet de stratégie de groupe ne modifiera pas la configuration existante de ce paramètre particulier pour l'utilisateur ou l'ordinateur.
- Activé. Le paramètre de stratégie sera appliqué.
- Désactivé. Le paramètre de stratégie est spécifiquement inversé.

Par défaut, l'état Non configuré est affecté à la plupart des paramètres.

Remarque : Il existe quelques paramètres à valeurs multiples ou dont les valeurs sont de type chaîne de texte. Ceux-ci sont généralement utilisés pour fournir des détails de configuration spécifiques aux applications ou aux composants du système d'exploitation. Par exemple, un paramètre pourrait fournir l'URL de la page d'accueil de Windows Internet Explorer® ou de certaines applications bloquées.

Les effets de la modification de configuration varient selon le paramètre de stratégie. Par exemple, si vous activez le paramètre de stratégie **Empêcher l'accès au Panneau de configuration**, les utilisateurs ne pourront plus ouvrir le Panneau de configuration. Si vous désactivez ce paramètre de stratégie, vous permettez aux utilisateurs d'ouvrir le Panneau de configuration. Remarquez le double négatif de ce paramètre de stratégie : vous désactivez une stratégie qui empêche une action, ce qui autorise ainsi cette action.

Structure des paramètres de stratégie de groupe

Il y a deux groupes distincts de paramètres de stratégie de groupe :

- Paramètres de l'utilisateur. Il s'agit des paramètres qui modifient la ruche HKey de l'utilisateur actuel dans le Registre.
- Paramètres de l'ordinateur. Il s'agit des paramètres qui modifient la ruche HKEY de l'ordinateur local dans le Registre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les paramètres de l'utilisateur et de l'ordinateur ont chacun trois domaines de configuration, qui sont décrits dans le tableau suivant.

Section	Description
Paramètres logiciels	Comprennent les paramètres logiciels qui peuvent être déployés pour l'utilisateur ou l'ordinateur. Les logiciels qui sont déployés pour un utilisateur sont spécifiques à cet utilisateur. Les logiciels qui sont déployés pour l'ordinateur sont à la disposition de tous les utilisateurs de cet ordinateur.
Paramètres du système d'exploitation Windows	Comprennent les paramètres de script et les paramètres de sécurité pour l'utilisateur et l'ordinateur, et la maintenance Internet Explorer pour la configuration utilisateur.
Modèles d'administration	Comprennent des centaines de paramètres qui modifient le Registre afin de contrôler les divers aspects de l'environnement de l'utilisateur et de l'ordinateur. De nouveaux modèles d'administration peuvent être créés par Microsoft ou d'autres fournisseurs. Vous pouvez ajouter ces nouveaux modèles à la Console de gestion des stratégies de groupe. Par exemple, Microsoft met à disposition le téléchargement des modèles Office 2010 et vous pouvez les ajouter à la Console de gestion des stratégies de groupe.

Éditeur de gestion des stratégies de groupe

L'Éditeur de gestion des stratégies de groupe affiche les différents paramètres de stratégie de groupe qui sont disponibles dans un objet de stratégie de groupe. Ceux-ci sont affichés dans une hiérarchie organisée qui commence par la division entre les paramètres de l'ordinateur et les paramètres de l'utilisateur, puis qui se développe pour afficher le nœud Configuration de l'ordinateur et le nœud Configuration de l'utilisateur. L'Éditeur de gestion des stratégies de groupe est l'endroit où tous les paramètres et les préférences de stratégie de groupe sont configurés.

Préférences de stratégie de groupe

En plus des sections de la stratégie de groupe présentées dans le tableau précédent, un nœud Préférences est présent sous les nœuds Configuration de l'ordinateur et Configuration de l'utilisateur dans l'Éditeur de gestion des stratégies de groupe. Les préférences fournissent encore plus de fonctions avec lesquelles configurer l'environnement et seront présentées ultérieurement dans ce module.

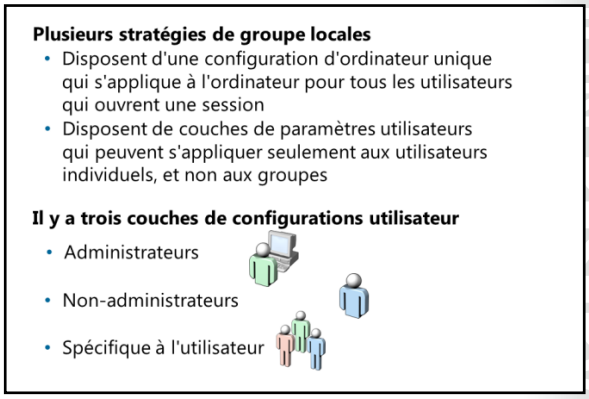
Stratégie de groupe locale

Tous les systèmes qui exécutent les systèmes d'exploitation client ou serveur Microsoft® Windows 2000 ou version plus récente disposent également d'objets de stratégie de groupe locale. Les paramètres de stratégie locale s'appliquent uniquement à l'ordinateur local, mais vous pouvez les exporter et les importer sur d'autres ordinateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les objets de stratégie de groupe locale multiple ?



Dans les systèmes d'exploitation Windows antérieurs à Windows Vista®, il n'y avait qu'une seule configuration utilisateur disponible dans la stratégie de groupe locale. Cette configuration était appliquée à tous les utilisateurs qui se connectaient depuis cet ordinateur local. C'est encore vrai, mais Windows Vista® et les systèmes d'exploitation client Windows plus récents, ainsi que Windows Server 2008 et les systèmes d'exploitation Windows Server plus récents sont dotés d'une fonctionnalité supplémentaire : les objets de stratégie de groupe locale multiple. Dans Windows 8 et Windows Server 2012, vous pouvez désormais également avoir différents paramètres utilisateur pour différents utilisateurs locaux, mais cette option est uniquement disponible pour les configurations des utilisateurs qui figurent dans la stratégie de groupe. En fait, il y a un seul ensemble de configurations d'ordinateur disponible dans Windows 8 et Windows Server 2012, qui affecte tous les utilisateurs de l'ordinateur.

Windows 8 et Windows Server 2012 fournissent cette fonctionnalité avec les trois couches d'objets de stratégie de groupe locale suivantes :

- Stratégie de groupe locale (contient les paramètres de configuration de l'ordinateur)
- Stratégie de groupe Administrateurs et Non-administrateurs
- Stratégie de groupe locale spécifique à l'utilisateur

Remarque : Il existe une exception à cette fonctionnalité : les contrôleurs de domaine. En raison de la nature de leur rôle, les contrôleurs de domaine ne peuvent pas avoir d'objets de stratégie de groupe locale.

Mode de traitement des couches

Les couches d'objets de stratégie de groupe locale sont traitées dans l'ordre suivant :

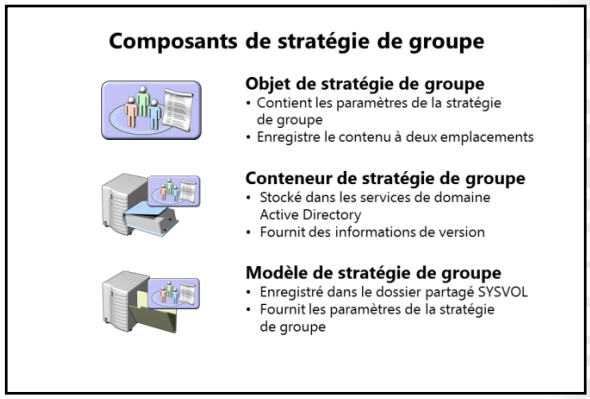
1. Stratégie de groupe locale
2. Stratégie de groupe Administrateurs et Non-administrateurs
3. Stratégie de groupe locale spécifique à l'utilisateur

À l'exception des catégories Administrateur ou Non-administrateur, il n'est pas possible d'appliquer des objets de stratégie de groupe locale à des groupes, mais uniquement à différents comptes d'utilisateurs locaux. Les utilisateurs du domaine sont soumis à la stratégie de groupe locale, ou aux paramètres Administrateur ou Non-administrateur, selon les besoins.

Remarque : Les administrateurs de domaine peuvent désactiver le traitement des objets de stratégie de groupe locale sur les clients qui exécutent des systèmes d'exploitation Windows ou Windows Server en activant le paramètre de stratégie **Désactiver le traitement des objets de stratégie de groupe locaux** dans un objet de stratégie de groupe du domaine.

Stockage des objets de stratégie de groupe de domaine

Les paramètres de stratégie de groupe sont présentés sous forme d'objets de stratégie de groupe dans la console de gestion des stratégies de groupe (GPMC), mais un objet de stratégie de groupe représente en réalité deux composants : un modèle de stratégie de groupe et un conteneur de stratégie de groupe.



Modèle de stratégie de groupe

Les modèles de stratégie de groupe correspondent à la collection réelle de paramètres que vous pouvez modifier. Le modèle de stratégie de groupe est une collection de fichiers stockée dans le dossier SYSVOL de chaque contrôleur de domaine. SYSVOL se trouve dans le chemin %SystemRoot% \SYSVOL\Domain\Policies\GPOGUID, où GPOGUID est le GUID du conteneur de stratégie de groupe. Lorsque vous créez un objet de stratégie de groupe, un nouveau modèle de stratégie de groupe est créé dans le dossier SYSVOL et un nouveau conteneur de stratégie de groupe est créé dans AD DS.

Conteneur de stratégie de groupe

Le conteneur de stratégie de groupe est un objet Active Directory qui est stocké dans la base de données Active Directory. Chaque conteneur de stratégie de groupe comprend un attribut d'identificateur unique universel (GUID) qui identifie l'objet de façon unique dans AD DS. Le conteneur de stratégie de groupe définit les attributs de base de l'objet de stratégie de groupe, tels que les liens et les numéros de version, mais il ne contient aucun paramètre.

Par défaut, lors de l'actualisation de la stratégie de groupe, les extensions côté client (CSE) de la stratégie de groupe appliquent les paramètres d'un objet de stratégie de groupe uniquement si celui-ci a été mis à jour.

Le client de stratégie de groupe peut identifier un objet de stratégie de groupe mis à jour par son numéro de version. Chaque objet de stratégie de groupe a un numéro de version qui est incrémenté chaque fois qu'une modification est faite. Le numéro de version est enregistré en tant qu'attribut de conteneur de stratégie de groupe et dans un fichier texte, GPT.ini, dans le dossier Modèle de stratégie de groupe. Le client de stratégie de groupe connaît le numéro de version de chaque objet de stratégie de groupe qu'il a précédemment appliqué. Si, pendant l'actualisation de la stratégie de groupe, le client de stratégie de groupe découvre que le numéro de version du conteneur de stratégie de groupe a été modifié, les extensions CSE sont informées que l'objet de stratégie de groupe est mis à jour.

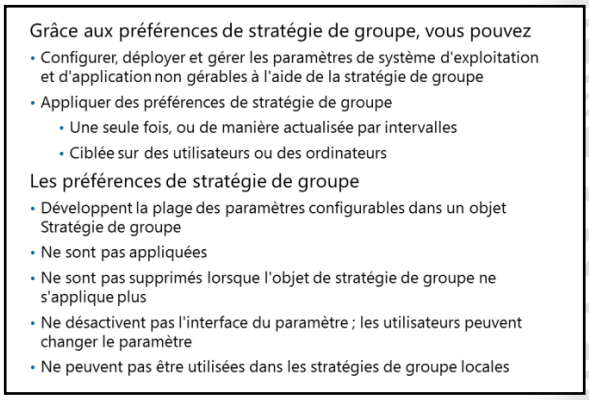
Lors de la modification d'une stratégie de groupe, c'est la version située sur l'ordinateur qui dispose du rôle d'opérations à maître unique flottant (FSMO) d'émulateur de contrôleur de domaine principal (PDC) qui est modifiée. Quel que soit l'ordinateur utilisé pour effectuer la modification, la console de gestion des stratégies de groupe est axée sur l'émulateur PDC par défaut. Il est possible de modifier le focus de la console de gestion des stratégies de groupe pour modifier une version sur un autre contrôleur de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les préférences de stratégie de groupe ?

Les *préférences de stratégie de groupe* sont une fonctionnalité du système d'exploitation Windows Server 2012. Les préférences comprennent plus de 20 extensions de stratégie de groupe qui développent la plage des paramètres configurables dans un objet de stratégie de groupe. Les préférences contribuent à réduire le besoin de scripts d'ouverture de session.



Remarque : Les extensions côté client de la stratégie de groupe doivent être installées sur les systèmes d'exploitation Windows XP pour leur permettre de traiter les préférences de stratégie de groupe. Elles peuvent être téléchargées à partir du site de téléchargement de Microsoft.

Caractéristiques des préférences

Les préférences présentent les caractéristiques suivantes :

- Les préférences existent pour les ordinateurs et les utilisateurs.
- À la différence des paramètres de stratégie de groupe, les préférences ne sont pas appliquées, et les utilisateurs peuvent modifier les configurations qui sont établies par des préférences.
- Les préférences peuvent être gérées à l'aide des Outils d'administration de serveur distant (RSAT).
- Les préférences peuvent être appliquées une seule fois au démarrage ou à l'ouverture de session, ou être actualisées à intervalles réguliers.
- À la différence des paramètres de stratégie de groupe, les préférences ne sont pas supprimées quand l'objet de stratégie de groupe n'est plus appliqué, mais vous pouvez modifier ce comportement.
- Les préférences peuvent facilement être ciblées vers certains utilisateurs ou ordinateurs de différentes manières, par exemple l'appartenance au groupe de sécurité ou la version du système d'exploitation.
- Les préférences ne sont pas disponibles pour les objets de stratégie de groupe locale.
- À la différence de la stratégie de groupe, l'interface utilisateur du paramètre n'est pas désactivée.

Utilisations courantes des préférences de stratégie de groupe

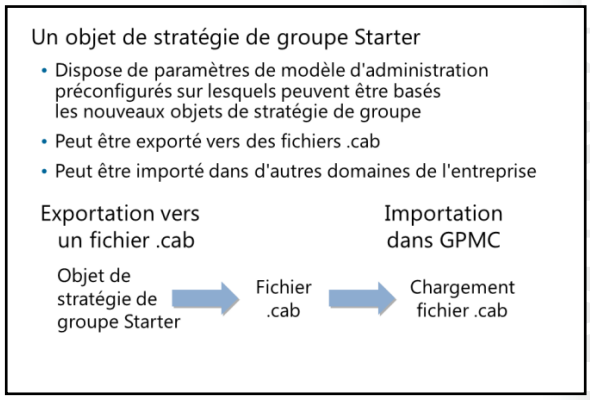
Bien que vous puissiez configurer de nombreux paramètres via les préférences de stratégie de groupe, voici certaines de leurs utilisations les plus courantes :

- Mapper des lecteurs réseau pour des utilisateurs
- Configurer des raccourcis Bureau pour des utilisateurs ou des ordinateurs
- Définir les variables d'environnement
- Mapper des imprimantes
- Définir les options d'alimentation

- Configurer les menus de démarrage
- Configurer les sources de données
- Configurer les options Internet
- Planifier les tâches

Que sont les objets de stratégie de groupe Starter ?

Les *objets de stratégie de groupe Starter* sont des modèles qui facilitent la création des objets de stratégie de groupe. Lorsque vous créez des objets de stratégie de groupe, vous pouvez choisir d'utiliser un objet de stratégie de groupe Starter comme source. Cela simplifie et accélère la création de plusieurs objets de stratégie de groupe avec la même configuration de base.



Paramètres disponibles

Les objets de stratégie de groupe Starter peuvent uniquement contenir des paramètres du nœud Modèles d'administration de la section Configuration de l'utilisateur ou Configuration de l'ordinateur. Les nœuds Paramètres du logiciel et Paramètres Windows de la stratégie de groupe ne sont pas disponibles, car ces nœuds impliquent l'interaction des services et sont plus complexes et dépendants du domaine.

Exportation des objets de stratégie de groupe Starter

Vous pouvez exporter des objets de stratégie de groupe Starter vers un fichier CAB (.cab) puis charger ce fichier .cab dans un autre environnement totalement indépendant de la forêt ou du domaine source. L'exportation d'un objet de stratégie de groupe Starter vous permet d'envoyer le fichier .cab à d'autres administrateurs, qui peuvent ensuite l'utiliser dans d'autres zones. Par exemple, vous pouvez créer un objet de stratégie de groupe qui définit les paramètres de sécurité d'Internet Explorer. Si vous souhaitez que tous les sites et les domaines utilisent les mêmes paramètres, vous pouvez exporter l'objet de stratégie de groupe Starter vers un fichier .cab, puis le distribuer.

Quand utiliser des objets de stratégie de groupe Starter ?

La situation la plus courante dans laquelle vous pouvez utiliser un objet de stratégie de groupe Starter est lorsque vous souhaitez un groupe de paramètres pour un type de rôle d'ordinateur. Par exemple, vous pourriez souhaiter que tous les portables de l'entreprise aient les mêmes restrictions de bureau, ou que tous les serveurs de fichiers aient les mêmes paramètres de stratégie de groupe de base, mais permettre certaines variations pour les différents services.

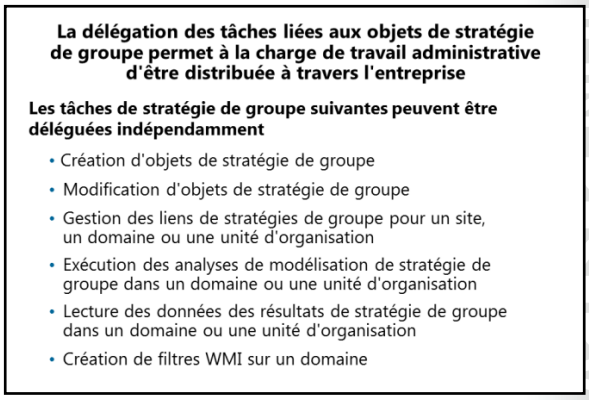
Objets de stratégie de groupe Starter inclus

La console de gestion des stratégies de groupe comprend un lien permettant de créer un dossier Objet de stratégie de groupe Starter, qui contient un certain nombre d'objets de stratégie de groupe Starter prédéfinis. Ces stratégies fournissent des paramètres préconfigurés et orientés sécurité pour les clients Client Entreprise (EC) et Sécurité spécialisée - Fonctionnalité limitée (SSLF) pour les paramètres de l'utilisateur et de l'ordinateur sur les systèmes d'exploitation Windows Vista et Windows XP avec Service Pack 2 (SP2). Vous pouvez utiliser ces stratégies comme point de départ quand vous concevez des stratégies de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Délégation de la gestion des objets de stratégie de groupe



Les administrateurs peuvent déléguer certaines des tâches d'administration de stratégie de groupe à d'autres utilisateurs. Ces utilisateurs n'ont pas besoin d'être des administrateurs de domaine ; ils peuvent être des utilisateurs auxquels certains droits sur les objets de stratégie de groupe sont accordés. Par exemple, un utilisateur qui gère une unité d'organisation particulière pourrait être chargé d'effectuer des tâches de création de rapports et d'analyse, tandis que le groupe d'assistance technique est autorisé à modifier les objets de stratégie de groupe pour cette unité d'organisation. Un troisième groupe de développeurs pourrait être chargé de créer des filtres Windows Management Instrumentation (WMI).

Les tâches de stratégie de groupe suivantes peuvent être déléguées de manière indépendante :

- Création d'objets de stratégie de groupe, y compris d'objets de stratégie de groupe Starter
- Modification d'objets de stratégie de groupe
- Gestion des liens de stratégies de groupe pour un site, un domaine ou une unité d'organisation
- Exécution de l'analyse de modélisation de stratégie de groupe
- Lecture des données des résultats de stratégie de groupe
- Création de filtres WMI

Le groupe Propriétaires créateurs de la stratégie de groupe laisse ses membres créer de nouveaux objets de stratégie de groupe, et modifier ou supprimer les objets de stratégie de groupe qu'ils ont créés.

Autorisations de stratégie de groupe par défaut

Par défaut, les utilisateurs et les groupes suivants disposent de l'accès complet pour gérer la stratégie de groupe :

- Administrateurs de domaine
- Administrateurs de l'entreprise
- Propriétaire créateur
- Système local

Le groupe Utilisateur authentifié dispose des autorisations Lire et Appliquer la stratégie de groupe uniquement.

Autorisations de création d'objets de stratégie de groupe

Par défaut, seuls les administrateurs du domaine, les administrateurs de l'entreprise et les propriétaires créateurs de la stratégie de groupe peuvent créer de nouveaux objets de stratégie de groupe. Vous pouvez utiliser deux méthodes pour accorder ce droit à un groupe ou à un utilisateur :

- Ajouter le groupe ou l'utilisateur au groupe Propriétaires créateurs de la stratégie de groupe
- Accorder explicitement au groupe ou à l'utilisateur l'autorisation de créer des objets de stratégie de groupe à l'aide de la console de gestion des stratégies de groupe (GPMC)

Autorisations de modification d'objets de stratégie de groupe

Pour modifier un objet de stratégie de groupe, l'utilisateur doit y avoir accès aussi bien en lecture qu'en écriture. Vous pouvez accorder cette autorisation à l'aide de la console GPMC.

Gestion des liaisons des objets de stratégie de groupe

La capacité de lier des objets de stratégie de groupe à un conteneur est une autorisation qui est spécifique à ce conteneur. Dans la console GPMC, vous pouvez gérer cette autorisation à l'aide de l'onglet **Délégation** du conteneur. Vous pouvez également la déléguer via l'Assistant Délégation de contrôle dans Utilisateurs et ordinateurs Active Directory.

Modélisation et résultats de stratégie de groupe

Vous pouvez déléguer la capacité d'utiliser les outils de création de rapports via la console GPMC ou à l'aide de l'Assistant Délégation de contrôle dans Utilisateurs et ordinateurs Active Directory.

Création de filtres WMI

Vous pouvez déléguer la capacité de créer et de gérer les filtres WMI via la console GPMC ou à l'aide de l'Assistant Délégation de contrôle dans Utilisateurs et ordinateurs Active Directory.

Démonstration : Création et gestion d'objets de stratégie de groupe

Dans cette démonstration, vous allez apprendre à :

- créer un objet de stratégie de groupe à l'aide de la console de gestion des stratégies de groupe ;
- modifier un objet de stratégie de groupe à l'aide de l'Éditeur de gestion des stratégies de groupe ;
- utiliser Windows PowerShell pour créer un objet de stratégie de groupe.

Procédure de démonstration

Créer un objet de stratégie de groupe à l'aide de la console de gestion des stratégies de groupe

- Connectez-vous à **LON-DC1** en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd** et créez une stratégie nommée **Interdire Windows Messenger**.

Modifier un objet de stratégie de groupe à l'aide de l'Éditeur de gestion des stratégies de groupe

1. Modifiez la stratégie pour interdire l'utilisation de Windows Messenger.
2. Liez l'objet de stratégie de groupe Interdire Windows Messenger au domaine.

Utiliser Windows PowerShell pour créer un objet de stratégie de groupe nommé Verrouillage de l'ordinateur

- Dans Windows PowerShell, importez le module **grouppolicy** et utilisez l'applet de commande **New-GPO** comme suit :

```
New-GPO –Name "Verrouillage de l'ordinateur"
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Traitement d'une stratégie de groupe

Il est essentiel de bien comprendre comment une stratégie de groupe est appliquée pour pouvoir développer une stratégie de groupe. Cette leçon vous montre comment la stratégie de groupe est associée à des objets Active Directory, comment elle est traitée et comment contrôler son application. Après avoir créé les objets de stratégie de groupe et configuré les paramètres que vous souhaitez appliquer, vous devez les lier à des conteneurs. Les objets de stratégie de groupe sont appliqués dans un ordre spécifique. Cet ordre peut déterminer quels paramètres sont appliqués aux objets. Il y a deux stratégies par défaut qui sont automatiquement créées. Ces stratégies sont utilisées pour fournir le mot de passe et les paramètres de sécurité pour le domaine et les contrôleurs de domaine. L'application des stratégies peut également être contrôlée par le filtrage de sécurité.

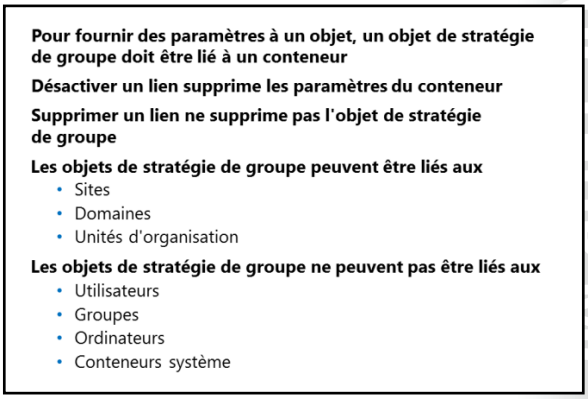
Objectifs de la leçon

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

- décrire une liaison d'objet de stratégie de groupe ;
- expliquer comment appliquer des objets de stratégie de groupe à des conteneurs et des objets ;
- décrire l'ordre de traitement des stratégies de groupe ;
- décrire les objets de stratégie de groupe par défaut ;
- décrire le filtrage de sécurité des objets de stratégie de groupe.

Liaisons d'objet de stratégie de groupe

Une fois que vous avez créé un objet de stratégie de groupe et défini tous les paramètres que vous souhaitez qu'il fournisse, l'étape suivante consiste à lier la stratégie à un conteneur Active Directory. Une liaison d'objet de stratégie de groupe est la connexion logique de la stratégie à un conteneur. Vous pouvez lier un objet de stratégie de groupe unique à plusieurs conteneurs à l'aide de la console GPMC. Vous pouvez lier des objets de stratégie de groupe aux types de conteneur suivants :



- Sites
- Domaines
- Unités d'organisation

Une fois qu'un objet de stratégie de groupe est lié à un conteneur, par défaut, la stratégie est appliquée à tous les objets de ce conteneur, et ensuite, à tous les conteneurs enfants sous cet objet parent. C'est dû au fait que les autorisations par défaut de l'objet de stratégie de groupe sont telles que les utilisateurs authentifiés disposent des autorisations Lire et Appliquer la stratégie de groupe. Vous pouvez modifier ce comportement en gérant les autorisations sur l'objet de stratégie de groupe.

Vous pouvez désactiver les liens aux conteneurs, ce qui supprime les paramètres de configuration. Vous pouvez également supprimer des liens. La suppression de liens ne supprime pas l'objet de stratégie de groupe réel, mais uniquement la connexion logique au conteneur.

Les objets de stratégie de groupe ne peuvent pas être liés directement à des utilisateurs, des groupes ou des ordinateurs. En outre, les objets de stratégie de groupe ne peuvent pas être liés aux conteneurs système dans AD DS, notamment aux conteneurs Intégré, Ordinateurs, Utilisateurs ou Comptes de services administrés. Les conteneurs système AD DS reçoivent les paramètres de stratégie de groupe des objets de stratégie de groupe qui sont liés au niveau du domaine uniquement.

Application des objets de stratégie de groupe

Les paramètres de configuration de l'ordinateur sont appliqués au démarrage, puis actualisés à intervalles réguliers. Tous les scripts de démarrage sont exécutés au démarrage de l'ordinateur. L'intervalle par défaut est de 90 minutes, mais il est configurable. L'exception à l'intervalle défini concerne les contrôleurs de domaine, dont les paramètres sont actualisés toutes les cinq minutes.

- **Quand vous appliquez des objets de stratégie de groupe, souvenez-vous de ce qui suit**
  - Les paramètres de l'ordinateur s'appliquent au démarrage
  - Les paramètres de l'utilisateur s'appliquent à la connexion
  - Les stratégies sont actualisées à intervalles réguliers et configurables
  - Les paramètres de sécurité sont actualisés au moins toutes les 16 heures
  - Les stratégies sont actualisées manuellement en utilisant
    - La commande **Gpupdate**
    - L'applet de commande Windows PowerShell **Invoke-Gpupdate**
  - Avec la nouvelle fonctionnalité d'actualisation des stratégies à distance dans Windows Server 2012, vous pouvez actualiser les stratégies à distance

Les paramètres utilisateur sont appliqués à l'ouverture de session et actualisés à intervalles réguliers et configurables ; la valeur par défaut est également de 90 minutes. Tous les scripts d'ouverture de session sont exécutés à l'ouverture de la session.

Remarque : Divers paramètres utilisateur requièrent deux ouvertures de session avant que l'utilisateur perçoive l'effet de l'objet de stratégie de groupe. Cela est dû au fait que les utilisateurs ouvrant une session sur le même ordinateur utilisent des informations d'identification mises en cache pour accélérer les ouvertures de session. Cela signifie que, bien que les paramètres de stratégie soient fournis à l'ordinateur, l'utilisateur est déjà connecté et les paramètres n'entreront donc pas en vigueur avant l'ouverture de session suivante. Le paramètre de redirection de dossier en est un exemple.

Vous pouvez modifier l'intervalle d'actualisation en configurant un paramètre de stratégie de groupe. Pour les paramètres de l'ordinateur, le paramètre d'intervalle d'actualisation se trouve dans le nœud Configuration de l'ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe. Pour les paramètres utilisateur, l'intervalle d'actualisation se trouve dans les paramètres correspondants sous Configuration de l'utilisateur. Les paramètres de sécurité constituent une exception à l'intervalle d'actualisation. La section paramètres de sécurité de la stratégie de groupe est actualisée au moins toutes les 16 heures, indépendamment de l'intervalle défini pour l'intervalle d'actualisation.

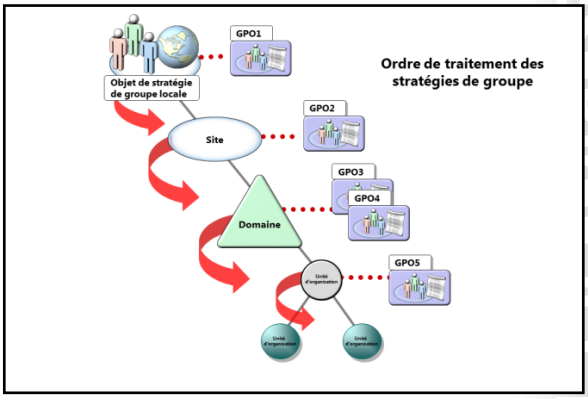
Vous pouvez également actualiser la stratégie de groupe manuellement. L'utilitaire de ligne de commande **Gpupdate** actualise et fournit toutes les nouvelles configurations de stratégie de groupe. La commande **Gpupdate /force** actualise tous les paramètres de stratégie de groupe. Il existe également une nouvelle applet de commande Windows PowerShell **Invoke-Gpupdate**, qui remplit la même fonction.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'Actualisation des stratégies à distance est une nouvelle fonctionnalité de Windows Server 2012. Cette fonctionnalité permet aux administrateurs d'utiliser la console GPMC pour cibler une unité d'organisation et forcer l'actualisation de la stratégie de groupe sur tous ses ordinateurs et utilisateurs actuellement connectés. Pour ce faire, cliquez avec le bouton droit sur n'importe quelle unité d'organisation, puis cliquez sur **Mise à jour de la stratégie de groupe**. La mise à jour se produit dans un délai de 10 minutes.

Ordre de traitement des stratégies de groupe

Les objets de stratégie de groupe ne sont pas appliqués simultanément, mais dans un ordre logique. Les objets de stratégie de groupe qui sont appliqués plus tard dans le processus d'application des objets de stratégie de groupe remplacent les éventuels paramètres de stratégie conflictuels qui ont été appliqués plus tôt.



Les objets de stratégie de groupe sont appliqués dans l'ordre suivant :

1. Objets de stratégie de groupe locale. Chaque système d'exploitation qui exécute Windows 2000 ou version plus récente dispose potentiellement déjà d'une stratégie de groupe locale configurée.
2. Objets de stratégie de groupe du site. Les stratégies qui sont liées à des sites sont traitées ensuite.
3. Objets de stratégie de groupe du domaine. Les stratégies qui sont liées au domaine sont traitées ensuite. Il y a souvent plusieurs stratégies au niveau du domaine. Ces stratégies sont traitées par ordre de préférence.
4. Objets de stratégie de groupe de l'unité d'organisation. Les stratégies liées aux unités d'organisation sont traitées ensuite. Ces stratégies contiennent les paramètres qui sont spécifiques aux objets de cette unité d'organisation. Par exemple, les utilisateurs du groupe Ventes peuvent nécessiter des paramètres spéciaux. Vous pouvez lier une stratégie à l'unité d'organisation Ventes pour fournir ces paramètres.
5. Stratégies d'unité d'organisation enfant. Les stratégies qui sont liées à des unités d'organisation enfant sont traitées en dernier.

Les objets contenus dans les conteneurs reçoivent l'effet cumulé de toutes les stratégies dans l'ordre de traitement. En cas de conflit entre les paramètres, c'est la dernière stratégie appliquée qui entre en vigueur. Par exemple, une stratégie au niveau du domaine peut restreindre l'accès aux outils de modification du Registre, mais vous pouvez configurer une stratégie au niveau de l'unité d'organisation et la lier à l'unité d'organisation Service informatique pour inverser cette stratégie. Étant donné que la stratégie au niveau de l'unité d'organisation est appliquée plus tard dans le processus, l'accès aux outils de modification du Registre sera disponible.

Remarque : D'autres méthodes, telles que l'application et le blocage de l'héritage, peuvent modifier l'effet des stratégies sur les conteneurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si plusieurs stratégies sont appliquées au même niveau, l'administrateur peut leur attribuer une valeur de préférence pour contrôler leur ordre de traitement. L'ordre de préférence par défaut est l'ordre dans lequel les stratégies ont été liées.

Vous pouvez également désactiver la configuration d'utilisateur ou d'ordinateur d'un objet de stratégie de groupe particulier. Si vous savez qu'une section d'une stratégie est vide, vous devez désactiver la section vide pour accélérer le traitement de la stratégie. Par exemple, si vous avez une stratégie qui fournit uniquement la configuration du bureau utilisateur, vous pouvez désactiver la section ordinateur de la stratégie.

Que sont les objets de stratégie de groupe par défaut ?

Lors de l'installation du rôle AD DS, deux objets de stratégie de groupe par défaut sont créés : la stratégie de domaine par défaut et la stratégie par défaut des contrôleurs de domaine.

Il existe par défaut deux objets de stratégie de groupe (GPO)

- **Stratégie de domaine par défaut**
  - Utilisée pour définir les stratégies de compte pour le domaine
    - Mot de passe
    - Verrouillage de compte
    - Protocole Kerberos
- **Stratégie par défaut des contrôleurs de domaine**
  - Utilisée pour définir des stratégies d'audit
  - Définit des droits d'utilisateur sur les contrôleurs de domaine

Stratégie de domaine par défaut

La stratégie de domaine par défaut est liée au domaine et affecte tous les principes de sécurité du domaine. Elle contient les paramètres de stratégie de mot de passe, les paramètres de verrouillage de compte et le protocole Kerberos. Il est recommandé de ne configurer aucun autre paramètre dans cette stratégie. Si vous devez configurer d'autres paramètres à appliquer au domaine entier, vous devez créer de nouvelles stratégies pour fournir ces paramètres, puis lier ces stratégies au domaine.

Stratégie par défaut des contrôleurs de domaine

La stratégie par défaut des contrôleurs de domaine est liée à l'unité d'organisation des contrôleurs de domaine et devrait seulement affecter des contrôleurs de domaine. Cette stratégie est conçue pour fournir des paramètres d'audit et des droits d'utilisateur, et ne devrait pas être utilisée à d'autres fins.

Filtrage de sécurité des objets de stratégie de groupe

Par nature, un objet de stratégie de groupe s'applique à tous les principes de sécurité du conteneur et à tous les conteneurs enfant situés au-dessous du parent. Cependant, vous souhaiterez peut-être modifier ce comportement et faire s'appliquer certains objets de stratégie de groupe à certains principes de sécurité particuliers uniquement. Par exemple, vous pourriez souhaiter exempter certains utilisateurs d'une unité d'organisation d'une stratégie de bureau restrictive. Vous pouvez le faire grâce au filtrage de sécurité.

Appliquer des autorisations de stratégie de groupe

- L'objet de stratégie de groupe a une liste de contrôle d'accès (onglet de délégation, cliquez sur Avancé)
- Par défaut : Autoriser Appliquer la stratégie de groupe pour les utilisateurs authentifiés

Portée limitée aux utilisateurs de certains groupes globaux ou universels

- Supprimer les utilisateurs authentifiés
- Ajouter les groupes globaux ou universels appropriés (la portée des objets de stratégie de groupe GPO n'est pas limitée aux groupes locaux de domaine)

Portée limitée aux utilisateurs, à l'exception de ceux appartenant à certains groupes

- Sous l'onglet Délégation, cliquez sur Avancé
- Ajouter des groupes globaux appropriés
- Refuser l'autorisation d'appliquer la stratégie de groupe

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Chaque objet de stratégie de groupe dispose d'une liste de contrôle d'accès (ACL) qui définit les autorisations sur cet objet de stratégie de groupe. Par défaut, les utilisateurs authentifiés sont autorisés à appliquer les autorisations Lire et Appliquer la stratégie de groupe. En réglant les autorisations dans la liste de contrôle d'accès, vous pouvez contrôler les principes de sécurité qui reçoivent l'autorisation d'appliquer les paramètres de l'objet de stratégie de groupe. Pour ce faire, deux approches sont possibles : refuser l'accès à la stratégie de groupe ou limiter les autorisations sur la stratégie de groupe.

Remarque : Le groupe Utilisateurs authentifiés inclut tous les comptes d'utilisateurs et d'ordinateurs qui ont été authentifiés dans AD DS.

Refuser l'accès à la stratégie de groupe

Si la plupart des principes de sécurité du conteneur doivent recevoir les paramètres de la stratégie, mais pas certains, vous pouvez exempter des principes de sécurité particuliers en leur refusant l'accès à la stratégie de groupe. Par exemple, vous pourriez avoir une stratégie de groupe que tous les utilisateurs de l'unité d'organisation Ventes doivent recevoir, à l'exception du groupe Responsables des ventes. Vous pouvez exempter ce groupe (ou cet utilisateur) en l'ajoutant à la liste de contrôle d'accès de l'objet de stratégie de groupe, puis en affectant la valeur Refuser à l'autorisation.

Limiter les autorisations sur la stratégie de groupe

Sinon, si vous avez créé un objet de stratégie de groupe qui ne doit être appliqué qu'à quelques principes de sécurité d'un conteneur, vous pouvez supprimer le groupe Utilisateurs authentifiés de la liste de contrôle d'accès, ajouter les principes de sécurité qui doivent recevoir les paramètres de l'objet de stratégie de groupe, puis leur accorder les autorisations Lire et Appliquer la stratégie de groupe. Par exemple, vous pourriez avoir un objet de stratégie de groupe contenant des paramètres de configuration de l'ordinateur qui ne doivent s'appliquer qu'aux ordinateurs portables. Vous pourriez supprimer le groupe Utilisateurs authentifiés de la liste de contrôle d'accès, ajouter les comptes d'ordinateurs des portables, puis leur accorder les autorisations Lire et Appliquer la stratégie de groupe.

Remarque : Il est recommandé de ne jamais refuser l'accès au groupe Utilisateurs authentifiés. Si vous le faites, les principes de sécurité ne recevront jamais les paramètres de l'objet de stratégie de groupe.

Vous pouvez accéder à la liste de contrôle d'accès d'un objet de stratégie de groupe dans la console GPMC en sélectionnant l'objet de stratégie de groupe dans le dossier Objet de stratégie de groupe, puis en cliquant sur l'onglet **Délégation>Avancé**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Discussion : Identification de l'application de la stratégie de groupe

Pour cette discussion, examinez la structure AD DS dans le graphique, lisez le scénario, puis répondez aux questions de la diapositive.

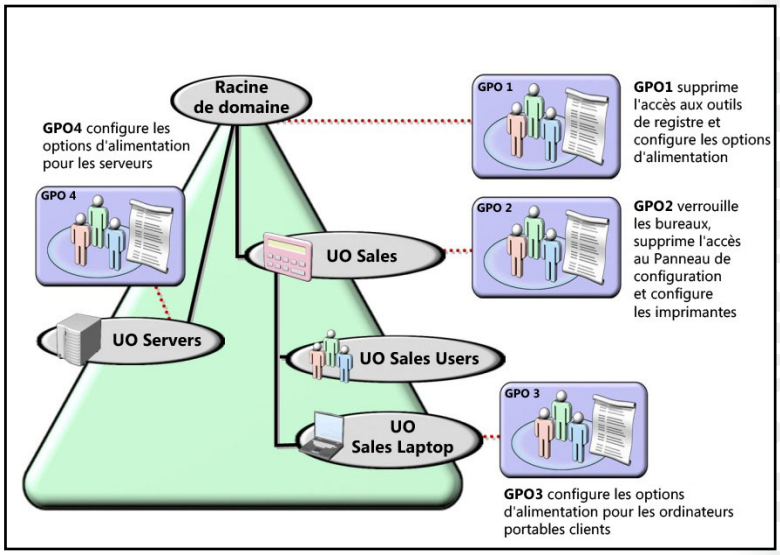
Examinez le scénario et le graphique de structure des services de domaine Active Directory dans le manuel pour répondre aux questions suivantes

- Quelles options d'alimentation recevront les serveurs de l'unité d'organisation Serveurs ?
- Quelles options d'alimentation recevront les ordinateurs portables de l'unité d'organisation Ordinateurs portables du service des ventes ?
- Quelles options d'alimentation recevront tous les autres ordinateurs du domaine ?
- Les utilisateurs de l'unité d'organisation Commerciaux, qui ont créé les stratégies locales pour accorder l'accès au Panneau de configuration, pourront-ils accéder au Panneau de configuration ?
- Si vous deviez accorder l'accès au Panneau de configuration à certains utilisateurs, comment procéderiez-vous ?
- L'objet GPO2 peut-il être appliqué à d'autres unités d'organisation du service ?

20 minutes

Scenario

L'illustration suivante représente une partie de la structure AD DS d'A. Datum Corporation, qui contient l'unité d'organisation Ventes avec ses unités d'organisation enfants et l'unité d'organisation Serveurs.



- GPO1 est lié au conteneur du domaine Adatum. Cet objet de stratégie de groupe configure les options d'alimentation qui éteignent les écrans et les disques après 30 minutes d'inactivité, et restreint l'accès aux outils de modification du Registre.
- GPO2 contient des paramètres pour verrouiller les postes de travail de l'unité d'organisation Commerciaux et configurer les imprimantes pour les commerciaux.
- GPO3 configure les options d'alimentation pour les ordinateurs portables de l'unité d'organisation Ordinateurs portables du service des ventes.
- GPO4 configure un autre ensemble d'options d'alimentation pour garantir que les serveurs ne passent jamais en mode d'économie d'énergie.

Certains utilisateurs de l'unité d'organisation Ventes disposent des droits d'administration sur leurs ordinateurs et ont créé des stratégies locales pour accorder spécifiquement l'accès au Panneau de configuration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Questions de discussion

Sur la base de ce scénario, répondez aux questions suivantes :

Question : Quelles options d'alimentation recevront les serveurs de l'unité d'organisation Serveurs ?

Question : Quelles options d'alimentation recevront les ordinateurs portables de l'unité d'organisation Ordinateurs portables du service des ventes ?

Question : Quelles options d'alimentation recevront tous les autres ordinateurs du domaine ?

Question : Les utilisateurs de l'unité d'organisation Commerciaux, qui ont créé les stratégies locales pour accorder l'accès au Panneau de configuration, pourront-ils accéder au Panneau de configuration ?

Question : Si vous deviez accorder l'accès au Panneau de configuration à certains utilisateurs, comment procèderiez-vous ?

Question : L'objet GPO2 peut-il être appliqué à d'autres unités d'organisation du service ?

Démonstration : Utilisation des outils de diagnostic de stratégie de groupe

Dans cette démonstration, vous allez apprendre à :

- utiliser Gpupdate pour actualiser la stratégie de groupe ;
- utiliser l'applet de commande **Gpresult** pour produire les résultats dans un fichier HTML ;
- utiliser l'Assistant Modélisation de stratégie de groupe pour tester la stratégie.

Procédure de démonstration

Utiliser Gpupdate pour actualiser la stratégie de groupe

- Sur LON-DC1, utilisez **Gpupdate** pour actualiser les objets de stratégie de groupe.

Utiliser l'applet de commande Gpresult pour produire les résultats dans un fichier HTML

1. Utilisez **Gpresult /H** pour créer un fichier HTML qui affiche les paramètres des objets de stratégie de groupe actuels.
2. Ouvrez le rapport HTML et consultez les résultats.

Utiliser l'Assistant Modélisation de stratégie de groupe pour tester la stratégie

- Utilisez l'Assistant Modélisation de stratégie de groupe pour simuler l'application d'une stratégie pour les utilisateurs de l'unité d'organisation Responsables qui se connectent à n'importe quel ordinateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Implémentation d'un magasin central pour les modèles d'administration

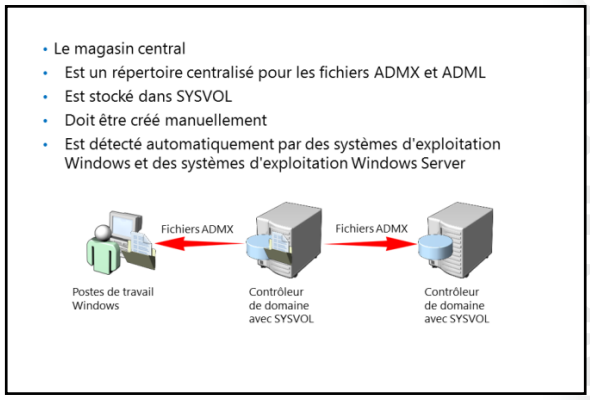
Les grandes organisations peuvent avoir de nombreux objets de stratégie de groupe gérés par plusieurs administrateurs. Lorsqu'un administrateur modifie un objet de stratégie de groupe, les fichiers de modèle sont extraits du poste de travail local. Le magasin central fournit un dossier unique dans SYSVOL qui contient tous les modèles requis pour créer et modifier des objets de stratégie de groupe. Cette leçon présente les fichiers qui constituent les modèles, et explique comment créer un emplacement de magasin central pour assurer la cohérence des modèles que les administrateurs utilisent.

Objectifs de la leçon

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

- décrire le magasin central ;
- décrire les modèles d'administration ;
- décrire le mode de fonctionnement des modèles d'administration ;
- décrire les paramètres de stratégie gérés et non gérés.

Qu'est-ce que le magasin central ?



Si votre organisation dispose de plusieurs postes de travail d'administration, des problèmes sont susceptibles de survenir lors de la modification des objets de stratégie de groupe. Si vous n'avez pas de magasin central pour contenir les fichiers de modèles, le poste de travail à partir duquel vous effectuez les modifications va utiliser les fichiers .admx (ADMX) et .adml (ADML) qui sont stockés dans le dossier PolicyDefinitions local. Si les différents postes de travail d'administration ont différents systèmes d'exploitation ou différents niveaux de Service Pack, les fichiers ADMX et ADML peuvent présenter certaines différences. Par exemple, les fichiers ADMX et ADML qui sont stockés sur un poste de travail Windows 7 sans Service Pack peuvent ne pas être identiques aux fichiers qui sont stockés sur un contrôleur de domaine Windows Server 2012.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

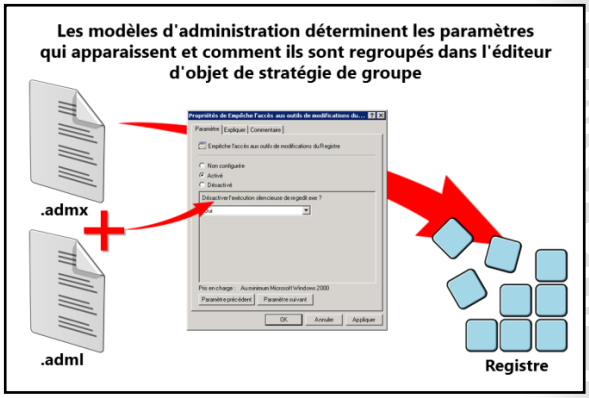
Le magasin central traite ce problème. Il fournit un point unique à partir duquel les postes de travail d'administration peuvent télécharger les mêmes fichiers ADMX et ADML lors de la modification d'un objet de stratégie de groupe. Le magasin central est détecté automatiquement par les systèmes d'exploitation Windows Vista ou version plus récente, et par les systèmes d'exploitation Windows Server 2008. Le poste de travail local que l'administrateur utilise pour effectuer l'administration vérifie donc toujours s'il existe un magasin central avant de charger les fichiers ADMX et ADML locaux dans l'Éditeur d'objets de stratégie de groupe. Lorsque le poste de travail local détecte un magasin central, il télécharge les fichiers de modèle à partir de celui-ci. De cette façon, l'expérience d'administration est cohérente entre les divers postes de travail.

Vous devez créer et configurer manuellement le magasin central. Vous devez tout d'abord créer un dossier sur un contrôleur de domaine, nommer ce dossier **PolicyDefinitions** et l'enregistrer sous C:\Windows\SYSVOL\sysvol\{Nom de domaine}\Policies\. Ce dossier sera maintenant votre magasin central. Vous devez ensuite copier tout le contenu du dossier C:\Windows\PolicyDefinitions dans le magasin central. Les fichiers ADML de ce dossier se trouvent également dans un dossier spécifique à la langue (tel que **fr-FR**).

Que sont les modèles d'administration ?

Un modèle d'administration se compose de deux types de fichier XML :

- Les fichiers ADMX spécifient le paramètre du Registre à modifier. Ils sont indépendants de la langue.
- Les fichiers ADML génèrent l'interface utilisateur pour configurer les paramètres de stratégie des modèles d'administration dans l'Éditeur de gestion des stratégies de groupe. Ils sont spécifiques à la langue.



Les fichiers ADMX et ADML sont stockés dans le dossier %SystemRoot%\PolicyDefinitions. Vous pouvez également créer vos propres modèles d'administration personnalisés au format XML. Les modèles d'administration qui contrôlent les produits Microsoft Office (par exemple, Office Word, Office Excel® et Office PowerPoint®) sont également disponibles à partir du site Web de téléchargement de Microsoft.

Les modèles d'administration présentent les caractéristiques suivantes :

- Ils sont organisés en sous-dossiers qui hébergent les options de configuration des zones spécifiques de l'environnement, telles que le réseau, le système et les composants Windows.
- Les paramètres de la section Ordinateur modifient la ruche HKEY_LOCAL_MACHINE du Registre, et les paramètres de la section Utilisateur modifient la ruche HKEY_CURRENT_USER du Registre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

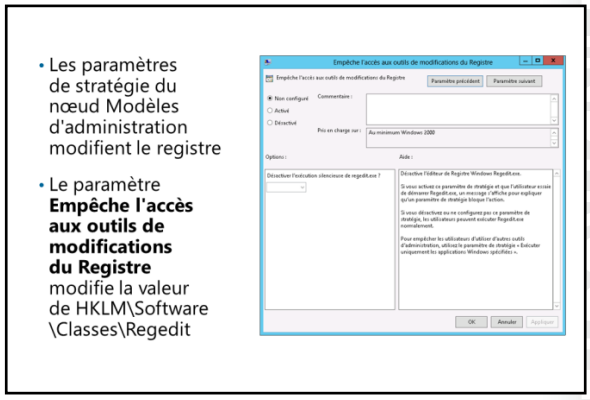
- Certains paramètres existent à la fois pour l'utilisateur et l'ordinateur. Par exemple, il existe un paramètre empêchant l'exécution de Windows Messenger à la fois dans le modèle Utilisateur et dans le modèle Ordinateur. En cas de paramètres conflictuels, le paramètre de la section Ordinateur est prioritaire.
- Certains paramètres sont disponibles uniquement pour certaines versions des systèmes d'exploitation Windows, comme plusieurs nouveaux paramètres qui ne peuvent être appliqués qu'à Windows 7 et aux versions plus récentes du système d'exploitation. Double-cliquer sur un paramètre permet d'afficher les versions prises en charge pour ce paramètre. Tout paramètre qui ne peut pas être traité par un système d'exploitation Windows plus ancien est simplement ignoré par ce système.

Fichiers ADM

Avant Windows Vista, les modèles d'administration avaient l'extension de fichier .adm (ADM). Les fichiers ADM étaient spécifiques à la langue et difficiles à personnaliser. Les fichiers ADM sont enregistrés dans SYSVOL dans le cadre du modèle de stratégie de groupe. Si un fichier ADM est utilisé dans plusieurs objets de stratégie de groupe, ce fichier est enregistré plusieurs fois. Cela augmente la taille de SYSVOL et augmente donc la taille du trafic de réplication Active Directory.

Mode de fonctionnement des modèles d'administration

Les modèles d'administration ont des paramètres pour presque tous les aspects de l'environnement informatique. Chaque paramètre du modèle correspond à un paramètre du Registre qui contrôle un aspect de l'environnement informatique. Par exemple, quand vous activez le paramètre qui empêche l'accès au Panneau de configuration, cela change la valeur de la clé de Registre qui contrôle cet aspect.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le nœud Modèles d'administration est organisé comme indiqué dans le tableau suivant.

Section	Nœuds
Paramètres de l'ordinateur	• Panneau de configuration • Réseau • Imprimantes • Système • Composants Windows • Tous les paramètres
Paramètres de l'utilisateur	• Panneau de configuration • Bureau • Réseau • Dossiers partagés • Menu Accueil et barre des tâches • Système • Composants Windows • Tous les paramètres

La plupart des nœuds contiennent plusieurs sous-dossiers pour mieux organiser les paramètres en groupes logiques. Même avec cette organisation, la recherche du paramètre dont vous avez besoin pourrait être une tâche décourageante. Pour vous aider à localiser les paramètres, dans le dossier Tous les paramètres, vous pouvez filtrer la liste de paramètres complète dans la section Ordinateur ou Utilisateur. Les options de filtre suivantes sont disponibles :

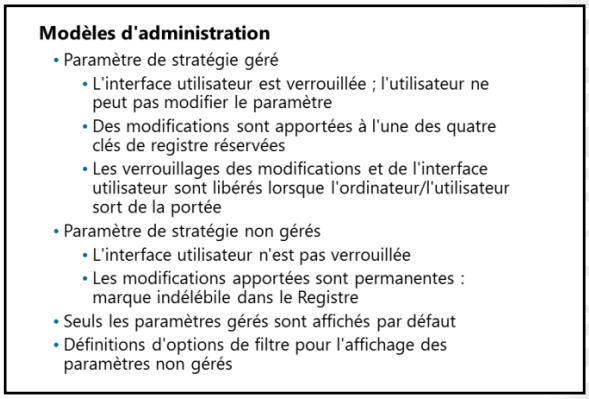
- Géré ou non géré
- Configuré ou non configuré
- Commenté
- Par mot clé
- Par plateforme

Vous pouvez également combiner plusieurs critères. Par exemple, vous pourriez filtrer les paramètres pour rechercher tous les paramètres configurés qui s'appliquent à Internet Explorer 10 à l'aide du mot clé **ActiveX**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Paramètres de stratégie gérés et non gérés

Il existe deux types de paramètres de stratégie : gérés et non gérés. Tous les paramètres de stratégie inclus dans les modèles d'administration d'un objet de stratégie de groupe sont des stratégies gérées. Le service Stratégie de groupe contrôle les paramètres de stratégie gérés et supprime un paramètre de stratégie lorsqu'il n'est plus dans l'étendue de l'utilisateur ou de l'ordinateur. Le service Stratégie de groupe ne contrôle pas les paramètres de stratégie non gérés. Ces paramètres de stratégie sont persistants. Le service Stratégie de groupe ne supprime pas les paramètres de stratégie non gérés.



Paramètres de stratégie gérés

Un paramètre de stratégie géré présente les caractéristiques suivantes :

- L'interface utilisateur est verrouillée de sorte qu'un utilisateur ne puisse pas modifier le paramètre. Avec les paramètres de stratégie gérés, l'interface utilisateur appropriée est désactivée. Par exemple, si vous configurez le papier peint du Bureau via un paramètre de stratégie de groupe, l'utilisateur verra ce paramètre grisé dans son interface utilisateur locale.
- Les modifications sont effectuées dans des zones restreintes du Registre, auxquelles seuls les administrateurs ont accès. Ces clés de Registre réservées sont les suivantes :
  - HKLM\Software\Policies (paramètres de l'ordinateur)
  - HKCU\Software\Policies (paramètres de l'utilisateur)
  - HKLM\Software\Microsoft\Windows\Current Version\Policies (paramètres de l'ordinateur)
  - HKCU\Software\Microsoft\Windows\Current Version\Policies (paramètres de l'utilisateur)
- Les modifications apportées par un paramètre de stratégie de groupe et le verrouillage de l'interface utilisateur sont annulés si l'utilisateur ou l'ordinateur passe hors de l'étendue de l'objet de stratégie de groupe. Par exemple, si vous supprimez un objet de stratégie de groupe, les paramètres de stratégie gérés qui avaient été appliqués à un utilisateur seront annulés. Cela signifie que, généralement, le paramètre est réinitialisé à son état précédent. En outre, l'interface utilisateur correspondant à ce paramètre est réactivée.

Paramètres de stratégie non gérés

En revanche, un paramètre de stratégie non géré apporte une modification persistante au Registre. Si l'objet de stratégie de groupe ne s'applique plus, le paramètre reste actif. On parle souvent de *marquage* du Registre, ce qui signifie lui apporter une modification permanente. Pour inverser l'effet du paramètre de stratégie, vous devez déployer une modification qui rétablit la configuration à l'état souhaité. En outre, un paramètre de stratégie non géré ne verrouille pas l'interface utilisateur correspondant à ce paramètre.

Par défaut, l'Éditeur de gestion des stratégies de groupe masque les paramètres de stratégie non gérés pour vous décourager d'implémenter une configuration difficile à rétablir. Bon nombre des paramètres qui sont disponibles dans les préférences de stratégie de groupe sont des paramètres non gérés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation d'une stratégie de groupe

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

En tant que membre de l'équipe de techniciens responsables des serveurs, votre rôle consiste à aider à déployer et configurer de nouveaux serveurs et services dans l'infrastructure existante, conformément aux instructions fournies par votre responsable informatique.

Votre responsable vous a demandé de créer un magasin central pour les fichiers ADMX afin de garantir que tout le monde puisse modifier les objets de stratégie de groupe qui ont été créés avec des fichiers ADMX personnalisés. Vous devez également créer un objet de stratégie de groupe Starter qui comprend des paramètres Internet Explorer, puis configurer un objet de stratégie de groupe qui applique des paramètres d'objet de stratégie de groupe pour les services Marketing et Informatique.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer un magasin central ;
- créer des objets de stratégie de groupe.

Configuration de l'atelier pratique

Durée approximative : 40 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-CL1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Instructions de configuration de l'atelier pratique

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 **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur Gestionnaire Hyper-V®.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 22410B-LON-CL1. Ne vous connectez pas tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Configuration d'un magasin central

Scénario

A. Datum a récemment implémenté un modèle ADMX personnalisé pour configurer une application. Un collègue a obtenu les fichiers ADMX du fournisseur avant de créer l'objet de stratégie de groupe avec les paramètres de configuration. Les paramètres ont été appliqués à l'application comme prévu.

Après l'implémentation, vous avez remarqué que vous ne pouvez pas modifier les paramètres de l'application dans l'objet de stratégie de groupe à partir de tout autre emplacement que le poste de travail qui a été initialement utilisé par votre collègue. Afin de résoudre ce problème, votre responsable vous a demandé de créer un magasin central pour les modèles d'administration. Une fois que vous aurez créé le magasin central, votre collègue copiera le modèle ADMX du fournisseur du poste de travail vers le magasin central.

Les tâches principales de cet exercice sont les suivantes :

1. Afficher l'emplacement des modèles d'administration dans un objet de stratégie de groupe
2. Créer un magasin central
3. Copier les modèles d'administration dans le magasin central
4. Vérifier l'emplacement des modèles d'administration dans la console GPMC

▶ Tâche 1 : Afficher l'emplacement des modèles d'administration dans un objet de stratégie de groupe

1. Connectez-vous à LON-DC1 en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Démarrez l'**Assistant GPMC**.
3. Dans le dossier Objet de stratégie de groupe, ouvrez **Default Domain Policy** et affichez l'emplacement des modèles d'administration.

▶ Tâche 2 : Créer un magasin central

1. Ouvrez l'**Explorateur de fichiers** et accédez à **C:\Windows\SYSVOL\sysvol\Adatum.com\Policies**.
2. Créez un dossier nommé **PolicyDefinitions**, qui sera utilisé pour le magasin central.

▶ Tâche 3 : Copier les modèles d'administration dans le magasin central

- Copiez le contenu du dossier **PolicyDefinitions** par défaut situé dans **C:\Windows\PolicyDefinitions** vers le nouveau dossier PolicyDefinitions situé dans **C:\Windows\SYSVOL\sysvol\Adatum.com\Policies**.

▶ Tâche 4 : Vérifier l'emplacement des modèles d'administration dans la console GPMC

- Vérifiez que l'Éditeur d'objets de stratégie de groupe utilise les fichiers ADMX du dossier **PolicyDefinitions** central en affichant le texte des informations sur l'emplacement du dossier des modèles d'administration.

Résultats : À la fin de cet exercice, vous devez avoir configuré un magasin central.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Création d'objets de stratégie de groupe

Scénario

Après une récente réunion du comité de stratégie informatique, la direction a décidé qu'A. Datum va utiliser la stratégie de groupe pour restreindre l'accès utilisateur à l'onglet **Général** d'Internet Explorer.

Votre responsable vous a demandé de créer un objet de stratégie de groupe Starter qui peut être utilisé pour tous les services avec les paramètres de restriction par défaut pour Internet Explorer. Vous devez ensuite créer les objets de stratégie de groupe qui fourniront les paramètres pour les membres de tous les services à l'exception du service informatique.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un objet de stratégie de groupe Starter par défaut Restrictions de Windows Internet Explorer
2. Configurer l'objet de stratégie de groupe Starter Restrictions d'Internet Explorer
3. Créer un objet de stratégie de groupe Restrictions d'Internet Explorer à partir de l'objet de stratégie de groupe Starter Restrictions d'Internet Explorer
4. Tester l'objet de stratégie de groupe pour les utilisateurs du domaine
5. Utiliser le filtrage de sécurité pour exempter le service informatique de la stratégie Restrictions d'Internet Explorer
6. Tester l'application de l'objet de stratégie de groupe pour les utilisateurs du service informatique
7. Tester l'application de l'objet de stratégie de groupe pour les autres utilisateurs du domaine
8. Pour préparer le module suivant

▶ Tâche 1 : Créer un objet de stratégie de groupe Starter par défaut Restrictions de Windows Internet Explorer®

1. Ouvrez la console **GPMC** et créez un objet de stratégie de groupe Starter nommé **Restrictions d'Internet Explorer**.
2. Tapez un commentaire stipulant que **Cet objet de stratégie de groupe désactive l'onglet Général des Options Internet**.

▶ Tâche 2 : Configurer l'objet de stratégie de groupe Starter Restrictions d'Internet Explorer

- Configurez l'objet de stratégie de groupe Starter nommé **Restrictions d'Internet Explorer** pour désactiver l'onglet **Général** des Options Internet.

Assistant de lecture : sélectionnez **Tous les paramètres** dans les modèles d'administration et recherchez une concordance exacte en filtrant par les mots clés **onglet Général**.

▶ Tâche 3 : Créer un objet de stratégie de groupe Restrictions d'Internet Explorer à partir de l'objet de stratégie de groupe Starter Restrictions d'Internet Explorer

- Créez un objet de stratégie de groupe nommé **Restrictions d'IE** basé sur l'objet de stratégie de groupe Starter Restrictions d'Internet Explorer et liez-le au domaine **Adatum.com**.

▶ Tâche 4 : Tester l'objet de stratégie de groupe pour les utilisateurs du domaine

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Brad** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Panneau de configuration**.
3. Essayez de modifier votre page d'accueil.
4. Ouvrez **Options Internet** pour vérifier que l'onglet **Général** a été restreint.
5. Déconnectez-vous de LON-CL1.

▶ Tâche 5 : Utiliser le filtrage de sécurité pour exempter le service informatique de la stratégie Restrictions d'Internet Explorer

1. Sur LON-DC1, ouvrez la console **GPMC**.
2. Configurez le filtrage de sécurité sur la stratégie Restrictions d'Internet Explorer pour refuser l'accès au service informatique.

▶ Tâche 6 : Tester l'application de l'objet de stratégie de groupe pour les utilisateurs du service informatique

1. Connectez-vous à **LON-CL1** en tant que **Brad** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Panneau de configuration**.
3. Essayez de modifier votre page d'accueil. Vérifiez que la boîte de dialogue **Propriétés Internet** affiche l'onglet **Général** et que tous les paramètres sont disponibles.
4. Déconnectez-vous de LON-CL1.

▶ Tâche 7 : Tester l'application de l'objet de stratégie de groupe pour les autres utilisateurs du domaine

1. Connectez-vous à **LON-CL1** en tant que **Boris** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Panneau de configuration**.
3. Essayez de modifier votre page d'accueil.
4. Ouvrez **Options Internet** pour vérifier que l'onglet **Général** a été restreint.
5. Déconnectez-vous de LON-CL1.

Résultats : À la fin de cet atelier pratique, vous devez avoir créé un objet de stratégie de groupe.

▶ 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 des **ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-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 **22410B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quels sont certains des avantages et des inconvénients liés à l'utilisation d'objets de stratégie de groupe au niveau du site ?

Question : Vous avez un certain nombre de scripts d'ouverture de session qui mappent des lecteurs réseau pour des utilisateurs. Les utilisateurs n'ont pas tous besoin de ces mappages de lecteurs. Vous devez donc vous assurer que seuls les utilisateurs souhaités reçoivent les mappages. Vous souhaitez arrêter d'utiliser des scripts. Quel est le meilleur moyen de mapper des lecteurs réseau sans utiliser de scripts pour les utilisateurs sélectionnés ?

Outils

Outil	Utilisation	Emplacement
Console de gestion des stratégies de groupe (GPMC)	Contrôle tous les aspects des stratégies de groupe	Dans le Gestionnaire de serveur, dans le menu **Outils**
Éditeur d'objets de stratégie de groupe	Configure les paramètres des objets de stratégie de groupe	Accessible en modifiant tout objet de stratégie de groupe
Jeu de stratégie résultant (RSoP)	Détermine quels paramètres s'appliquent à un utilisateur ou à un ordinateur	Dans la console GPMC
Assistant Modélisation de stratégie de groupe	Teste ce qui se produirait si des paramètres étaient appliqués aux utilisateurs ou aux ordinateurs, avant d'appliquer réellement ces paramètres	Dans la console GPMC
Éditeur de stratégie de groupe locale	Configure les paramètres de stratégie de groupe qui s'appliquent seulement à l'ordinateur local	Accessible en créant une console MMC (Microsoft Management Console) sur l'ordinateur local et en ajoutant le composant logiciel enfichable Éditeur d'objet de stratégie de groupe

Méthode conseillée

Voici les meilleures pratiques recommandées :

- N'utilisez pas la stratégie de domaine par défaut ni la stratégie par défaut des contrôleurs de domaine à d'autres fins. Créez plutôt de nouvelles stratégies.
- Limitez l'utilisation du filtrage de sécurité et des autres mécanismes qui rendent les diagnostics plus complexes.
- Désactivez les sections Utilisateur ou Ordinateur des stratégies si elles ne contiennent aucun paramètre configuré.
- Si vous avez plusieurs postes de travail d'administration, créez un magasin central.
- Ajoutez des commentaires à vos objets de stratégie de groupe pour expliquer ce que font les stratégies.
- Concevez votre structure d'unités d'organisation de façon à prendre en charge l'application de stratégies de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Un utilisateur constate un comportement anormal sur son poste de travail.	
Tous les utilisateurs d'une unité d'organisation spécifique rencontrent des problèmes, et plusieurs objets de stratégie de groupe sont appliqués à cette unité d'organisation.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12

Sécurisation des serveurs Windows à l'aide d'objets de stratégie de groupe

Table des matières :

Vue d'ensemble du module **12-1**

Leçon 1 : Vue d'ensemble de la sécurité des systèmes d'exploitation Windows **12-2**

Leçon 2 : Configuration des paramètres de sécurité **12-7**

Atelier pratique A : Renforcement de la sécurité des ressources de serveur **12-18**

Leçon 3 : Restriction de l'accès aux logiciels **12-26**

Leçon 4 : Configuration du Pare-feu Windows avec fonctions avancées de sécurité **12-31**

Atelier pratique B : Configuration d'AppLocker et du Pare-feu Windows **12-36**

Contrôle des acquis et éléments à retenir **12-43**

Vue d'ensemble du module

La protection de l'infrastructure informatique a toujours été une priorité pour les organisations. De nombreux risques de sécurité menacent les sociétés et leurs données critiques. Lorsqu'une société n'a pas des stratégies de sécurité adéquates, elle peut perdre des données, subir des indisponibilités de serveur et connaître une perte de crédibilité.

Pour assurer une protection face aux menaces contre la sécurité, les sociétés doivent avoir des stratégies de sécurité bien conçues qui comprennent de nombreux composants organisationnels et informatiques. Les stratégies de sécurité doivent être évaluées régulièrement car les menaces contre la sécurité évoluent et l'informatique doit suivre cette évolution.

Avant de commencer à concevoir des stratégies de sécurité pour favoriser la protection des données, des services et de l'infrastructure informatique de votre organisation, vous devez apprendre à identifier les menaces contre la sécurité, à planifier votre stratégie pour atténuer ces menaces et à sécuriser votre infrastructure Windows Server® 2012.

Objectifs

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

- décrire la sécurité du système d'exploitation Windows Server ;
- configurer les paramètres de sécurité à l'aide d'une stratégie de groupe ;
- empêcher l'exécution de logiciels non autorisés sur les serveurs et les clients ;
- configurer le Pare-feu Windows avec fonctions avancées de sécurité.

Leçon 1
Vue d'ensemble de la sécurité des systèmes d'exploitation Windows

Plus les organisations étendent la disponibilité de leurs données réseau, applications et systèmes, plus il est difficile de garantir la sécurité de l'infrastructure réseau. Les technologies de sécurité intégrées dans Windows Server 2012 permettent aux organisations d'assurer une meilleure protection de leurs ressources réseau et d'entreprise dans des environnements et des scénarios d'entreprise toujours plus complexes. Cette leçon passe en revue les outils et les concepts disponibles pour implémenter la sécurité dans une infrastructure Windows 8 et Windows Server 2012.

Windows Server 2012 comprend de nombreuses fonctionnalités qui fournissent différentes méthodes d'implémentation de la sécurité. Ces fonctionnalités sont combinées pour former le noyau des fonctionnalités de sécurité de Windows Server 2012. Pour maintenir un environnement sécurisé, il est essentiel de comprendre ces fonctionnalités et les concepts associés et de bien connaître leur implémentation élémentaire.

Objectifs de la leçon

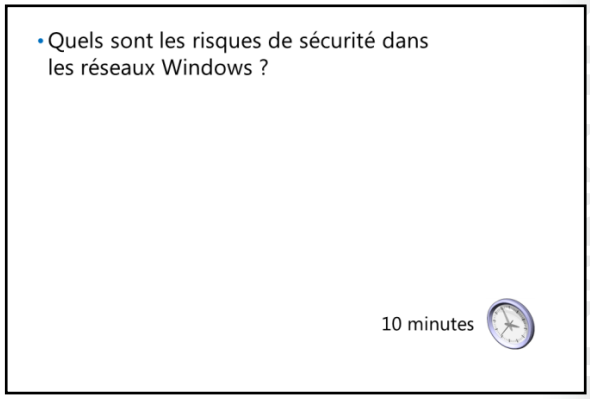
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- identifier les risques de sécurité pour Windows Server 2012 et les coûts qui leur sont associés ;
- appliquer le modèle de défense en profondeur pour améliorer la sécurité ;
- décrire les meilleures pratiques pour améliorer la sécurité de Windows Server 2012.

Discussion : identification des risques de sécurité et des coûts associés

La première étape dans le cadre de la défense de vos systèmes consiste à identifier les risques de sécurité potentiels et leurs coûts associés. Après cela, vous pouvez commencer à prendre des décisions éclairées au sujet de la façon d'allouer les ressources pour atténuer ces risques.

Examinez la question indiquée sur la diapositive et participez à la discussion pour identifier certains risques de sécurité dans les réseaux Windows et les coûts qui y sont associés.

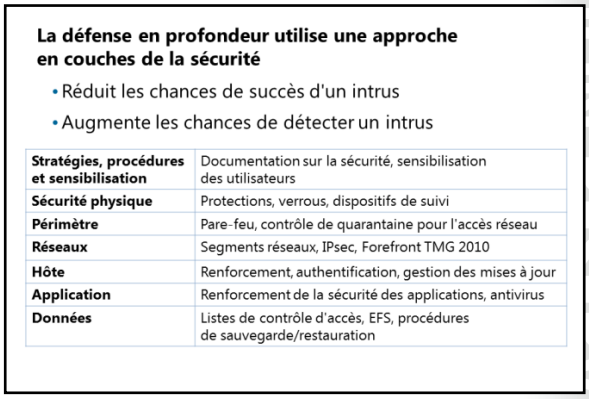


UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Application d'une défense en profondeur pour améliorer la sécurité

Vous pouvez atténuer les risques pesant sur le réseau informatique de votre organisation en sécurisant diverses couches de l'infrastructure. Le terme *défense en profondeur* est souvent utilisé pour décrire l'utilisation de plusieurs technologies de sécurité à des points différents de votre organisation.

Les technologies de défense en profondeur incluent les couches de sécurité qui s'étendent des stratégies utilisateur jusqu'à l'application et jusqu'aux données elles-mêmes.



Stratégies, procédures et sensibilisation

Les mesures relatives aux stratégies de sécurité doivent fonctionner dans le contexte des stratégies de l'organisation concernant les meilleures pratiques de sécurité. Par exemple, la mise en place d'une stratégie de mot de passe utilisateur rigoureuse n'est pas utile si les utilisateurs notent leurs mots de passe à côté de leur écran d'ordinateur ; les utilisateurs doivent être éduqués sur la façon de protéger leurs mots de passe. Un autre exemple de meilleure pratique de sécurité consiste à garantir que les utilisateurs ne s'éloignent pas de leur ordinateur de bureau sans avoir verrouillé au préalable l'ordinateur ou s'être déconnecté de l'ordinateur. Lorsque vous établissez les fondations de la sécurité du réseau de votre organisation, il est plus judicieux de commencer en créant des stratégies et des procédures appropriées et en les communiquant aux utilisateurs. Vous pouvez alors passer aux autres aspects du modèle de défense en profondeur.

Sécurité physique

Si n'importe quelle personne non autorisée peut accéder physiquement à un ordinateur connecté au réseau, la plupart des autres mesures de sécurité sont inutiles. Vous devez vous assurer que les ordinateurs contenant les données les plus sensibles (tels que les serveurs) sont physiquement sécurisés et que l'accès est accordé uniquement au personnel autorisé.

Périmètre

De nos jours, aucune organisation n'est isolée. Les organisations fonctionnent dans la sphère Internet et de nombreuses ressources réseau d'organisation sont disponibles à partir d'Internet. Cela peut inclure un site Web décrivant les services de votre organisation, ou des services internes que vous rendez disponibles en externe (comme les conférences Web et la messagerie électronique) afin que les utilisateurs puissent travailler de leur domicile ou de filiales.

Les réseaux de périmètre marquent la limite entre les réseaux publics et privés. En fournissant des serveurs proxy inverses dans le réseau de périmètre, vous pouvez proposer des services d'entreprise plus sécurisés dans le réseau public.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

De nombreuses organisations implémentent le contrôle de quarantaine pour l'accès réseau, dans le cadre duquel les ordinateurs qui se connectent au réseau d'entreprise font l'objet d'une vérification de divers critères de sécurité, par exemple si l'ordinateur possède les dernières mises à jour de sécurité, les mises à jour d'antivirus, ainsi que d'autres paramètres de sécurité recommandés par la société. Si ces critères sont remplis, l'ordinateur est autorisé à se connecter au réseau d'entreprise. Dans le cas contraire, l'ordinateur est placé dans un réseau isolé, appelé réseau de *quarantaine*, sans accès aux ressources de l'entreprise. Une fois que l'ordinateur a résolu les problèmes liés à ses paramètres de sécurité, il est retiré du réseau de quarantaine et est autorisé à se connecter aux ressources de l'entreprise.

Remarque : Un proxy inverse, tel que Microsoft® Forefront® Threat Management Gateway 2010 (Forefront TMG), vous permet de publier des services tels que la messagerie électronique et les services Web, à partir de l'intranet d'entreprise sans placer les serveurs de messagerie et Web dans le périmètre ni les exposer aux utilisateurs externes. Forefront TMG agit à la fois en tant que proxy inverse et solution de pare-feu.

Réseaux

Une fois que vous avez connecté vos ordinateurs à un réseau (interne ou public), ils sont exposés à différentes menaces, y compris l'écoute clandestine, l'usurpation d'identité, le déni de service et les attaques par relecture. En implémentant IPsec (Internet Protocol Security), vous pouvez chiffrer le trafic réseau et protéger les données lors de leur transfert entre ordinateurs.

Lorsque la communication a lieu via des réseaux publics, par exemple pour des employés travaillant à leur domicile ou dans des bureaux distants, il est recommandé que ces employés se connectent à une solution de pare-feu telle que Forefront TMG 2010 pour assurer une protection contre différents types de menaces liées au réseau.

Renforcement de la sécurité de l'ordinateur hôte

La couche suivante de défense est la couche utilisée pour l'ordinateur hôte. Ensemble, les étapes suivantes forment un processus appelé *renforcement de la sécurité de l'ordinateur hôte*. Sur votre ordinateur hôte, vous devez :

- maintenir sécurisés les ordinateurs à l'aide des dernières mises à jour de sécurité ;
- configurer des stratégies de sécurité, telles que la complexité des mots de passe ;
- configurer le pare-feu de l'hôte ;
- installer un logiciel antivirus.

Renforcement de la sécurité des applications

Les applications ne sont sécurisées que si les dernières mises à jour de sécurité ont été installées. Ensemble, les étapes suivantes forment un processus appelé *renforcement de la sécurité des applications :*

- Utilisez uniformément la fonctionnalité Windows Update des systèmes d'exploitation Windows pour maintenir à jour les applications.
- Testez les applications pour déterminer si elles présentent des failles de sécurité susceptibles de permettre à une personne malveillante externe de compromettre des applications ou d'autres composants réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sécurité des données

La dernière couche de sécurité concerne les données. Pour assurer la protection de votre réseau, vous devez :

- garantir l'utilisation appropriée des droits des utilisateurs de fichiers à l'aide des listes de contrôle d'accès (ACL) ;
- implémenter le chiffrement des données confidentielles à l'aide du système de fichiers EFS (Encrypting File System) ;
- effectuer des sauvegardes régulières des données.

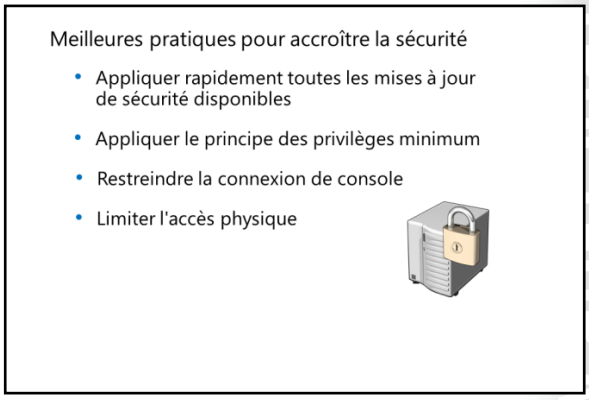
Documentation supplémentaire :

- Pour obtenir les derniers conseils en matière de sécurité et le dernier bulletin de sécurité Microsoft, reportez-vous au site relatif à la sécurité pour les professionnels de l'informatique, à l'adresse http://go.microsoft.com/fwlink/?LinkID=266741.
- Pour plus d'informations sur les types courants d'attaques réseau, reportez-vous à la page http://go.microsoft.com/fwlink/?LinkID=266742.

Question : Combien de couches du modèle de défense en profondeur devez-vous implémenter dans votre organisation ?

Meilleures pratiques pour améliorer la sécurité

Considérez les meilleures pratiques suivantes permettant d'améliorer la sécurité :



- Appliquez toutes les mises à jour de sécurité disponibles aussi rapidement que possible après leur diffusion. Vous devez vous efforcer d'implémenter les mises à jour de sécurité dès que possible pour garantir la protection de vos systèmes contre les vulnérabilités connues. Microsoft diffuse publiquement les détails de toutes les vulnérabilités connues après la publication d'une mise à jour, ce qui peut entraîner une augmentation des programmes malveillants tentant d'exploiter la vulnérabilité. Toutefois, veillez encore à tester convenablement les mises à jour avant de les appliquer à grande échelle dans votre organisation.
- Appliquez le principe des privilèges minimum. Fournissez aux utilisateurs et aux comptes de service les niveaux d'autorisation les plus bas qui sont requis pour effectuer les tâches requises. Ceci garantit que les programmes malveillants qui utilisent ces informations d'identification ont un impact limité. Cela garantit également que les utilisateurs sont limités dans leur capacité à supprimer par erreur des données ou à modifier des paramètres critiques du système d'exploitation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Restreignez l'ouverture de session dans la console d'administrateur. L'ouverture d'une session localement dans une console représente un plus grand risque pour un serveur que l'accès à distance à des données. Cela est dû au fait que certains programmes malveillants peuvent infecter un ordinateur uniquement en utilisant une session utilisateur sur cet ordinateur. Si vous autorisez les administrateurs à utiliser une connexion Bureau à distance pour l'administration du serveur, assurez-vous que des fonctionnalités de sécurité avancées sont activées, telles que le contrôle de compte d'utilisateur.
- Limitez l'accès physique. Si quelqu'un a physiquement accès à votre serveur, cette personne dispose pratiquement d'un accès illimité aux données sur ce serveur. Une personne non autorisée peut utiliser une grande variété d'outils pour réinitialiser rapidement le mot de passe sur des comptes administrateur local et obtenir un accès local, ou utiliser un lecteur USB pour introduire un programme malveillant.

Documentation supplémentaire : Pour plus d'informations sur les meilleures pratiques en matière de sécurité d'entreprise, reportez-vous à la page http://go.microsoft.com/fwlink/?LinkID=266743.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration des paramètres de sécurité

Une fois que vous êtes informé des menaces et des risques de sécurité, ainsi que des meilleures pratiques pour améliorer la sécurité, vous pouvez commencer à configurer la sécurité pour votre environnement Windows 8 et Windows Server 2012. Cette leçon explique comment configurer les paramètres de sécurité.

Pour appliquer ces paramètres de sécurité à plusieurs utilisateurs et ordinateurs dans votre organisation, vous pouvez utiliser les stratégies de groupe. Par exemple, vous pouvez configurer des paramètres de stratégie de mot de passe à l'aide des stratégies de groupe, puis les déployer pour plusieurs utilisateurs.

Une stratégie de groupe possède un composant de sécurité important qui vous permet de configurer la sécurité pour des utilisateurs et des ordinateurs. Vous pouvez appliquer uniformément la sécurité dans toute l'organisation dans les services de domaine Active Directory® (AD DS) en définissant des paramètres de sécurité dans un objet de stratégie de groupe (GPO) qui est associé à un site, à un domaine ou à une unité d'organisation (OU).

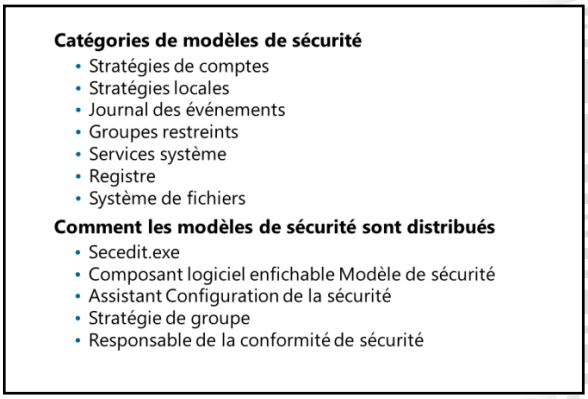
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire comment configurer des modèles de sécurité ;
- expliquer ce que sont les droits des utilisateurs et comment les configurer ;
- expliquer comment configurer les options de sécurité ;
- expliquer comment configurer le contrôle de compte d'utilisateur ;
- expliquer comment configurer l'audit de sécurité ;
- expliquer comment configurer des groupes restreints ;
- expliquer comment configurer les paramètres de stratégie de compte.

Documentation supplémentaire : Pour rechercher une liste détaillée des paramètres de stratégie de groupe, cliquez sur le lien suivant : http://go.microsoft.com/fwlink/?LinkID=266744 (page en anglais).

Configuration de modèles de sécurité

Les modèles de sécurité sont des fichiers que vous pouvez utiliser pour gérer et configurer les paramètres de sécurité sur des ordinateurs exécutant Windows. Selon les diverses catégories de paramètres de sécurité, les modèles de sécurité sont divisés en sections logiques. Vous pouvez configurer chacune des sections suivantes selon les besoins et les demandes d'une société :



- Stratégies de comptes. Stratégie de mot de passe, stratégie de verrouillage de compte et stratégie Kerberos
- Stratégies locales. Stratégie d'audit, attribution des droits utilisateur et options de sécurité

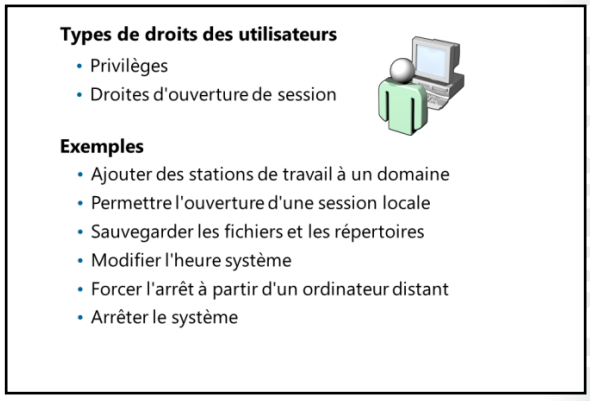
- Journal des événements. Paramètres des journaux d'événements Applications, Système et Sécurité
- Groupes restreints. Appartenance à des groupes dotés de droits et autorisations spéciaux
- Services système. Démarrage et autorisations pour les services système
- Registre. Autorisations pour les clés du Registre
- Système de fichiers. Autorisations pour les dossiers et les fichiers

Lorsque vous configurez un modèle de sécurité, vous pouvez l'utiliser pour configurer un ordinateur unique ou plusieurs ordinateurs dans le réseau. Voici quelques méthodes permettant de configurer et distribuer des modèles de sécurité :

- Secedit.exe. L'outil en ligne de commande secedit.exe configure et analyse la sécurité des systèmes en comparant la configuration actuelle d'un ordinateur exécutant Windows Server 2012 aux modèles de sécurité spécifiés.
- Composant logiciel enfichable Modèles de sécurité. Le composant logiciel enfichable Modèles de sécurité vous permet de créer une stratégie de sécurité à l'aide de modèles de sécurité.
- Assistant Configuration et analyse de la sécurité. Cet Assistant est un outil qui permet d'analyser et configurer la sécurité de l'ordinateur.
- Stratégie de groupe. La stratégie de groupe est une technologie permettant d'analyser et configurer les paramètres de l'ordinateur, y compris la distribution de paramètres de sécurité spécifiques.
- Responsable de la conformité de sécurité. Le responsable de la conformité de sécurité est un outil qui fournit des fonctionnalités de gestion de base de sécurité et des fonctionnalités d'exportation de base de sécurité centralisées.

Configuration des droits des utilisateurs

L'*attribution des droits utilisateur* se rapporte à la capacité d'exécuter des actions sur le système d'exploitation. Chaque ordinateur possède son propre ensemble de droits utilisateur, tels que le droit de modifier l'heure système. La plupart des droits sont accordés au système local ou à l'administrateur.



Les privilèges et les droits de connexion sont deux types de droits utilisateur :

- Les *privilèges* définissent l'accès aux ressources de l'ordinateur et du domaine. Les droits de sauvegarder des fichiers et des répertoires en sont un exemple.
- Les *droits de connexion* définissent les personnes autorisées à se connecter à un ordinateur et la manière dont elles peuvent se connecter. Par exemple, les droits de connexion peuvent définir le droit de se connecter localement à un système.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez configurer des droits via une stratégie de groupe. Initialement, la stratégie de domaine par défaut ne définit aucun droit utilisateur.

Vous pouvez configurer des paramètres pour les droits utilisateur en accédant à Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Attribution des droits utilisateurs dans la console de gestion des stratégies de groupe (GPMC).

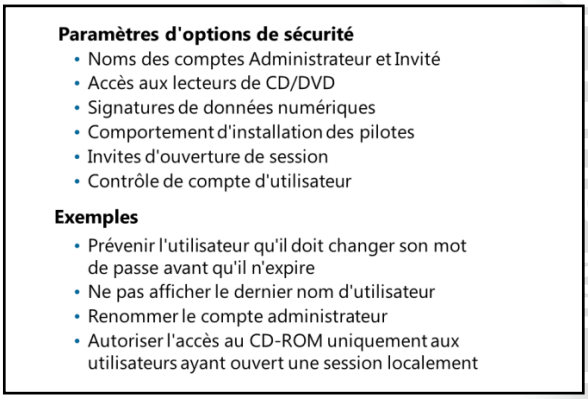
Voici quelques exemples de droits utilisateur couramment utilisés (et des stratégies qu'ils configurent) :

- **Ajouter des stations de travail au domaine**. Détermine quels utilisateurs ou groupes peuvent ajouter des stations de travail au domaine.
- **Permettre l'ouverture d'une session locale**. Détermine quels utilisateurs peuvent se connecter à l'ordinateur.
- **Autoriser l'ouverture de session par les services Bureau à distance**. Détermine quels utilisateurs ou groupes ont l'autorisation de se connecter en tant que client des services Bureau à distance.
- **Sauvegarder les fichiers et les répertoires**. Détermine quels utilisateurs ont les autorisations permettant de sauvegarder les fichiers et les dossiers sur un ordinateur.
- **Modifier l'heure système**. Détermine quels utilisateurs ou groupes possèdent les droits de modifier la date et l'heure sur l'horloge interne de l'ordinateur.
- **Forcer l'arrêt à partir d'un système distant**. Détermine quels utilisateurs sont autorisés à arrêter un ordinateur à partir d'un emplacement distant dans le réseau.
- **Arrêter le système**. Détermine quels utilisateurs parmi ceux connectés localement à un ordinateur sont autorisés à arrêter l'ordinateur.

Configuration des options de sécurité

Vous pouvez également utiliser les stratégies de groupe pour accéder aux options de sécurité et les configurer. Les paramètres de sécurité de l'ordinateur que vous pouvez configurer dans Options de sécurité comprennent les paramètres suivants :

- Noms des comptes Administrateur et Invité
- Accès aux lecteurs de CD/DVD
- Signatures de données numériques.
- Comportement d'installation des pilotes
- Invites d'ouverture de session
- Contrôle de compte d'utilisateur



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

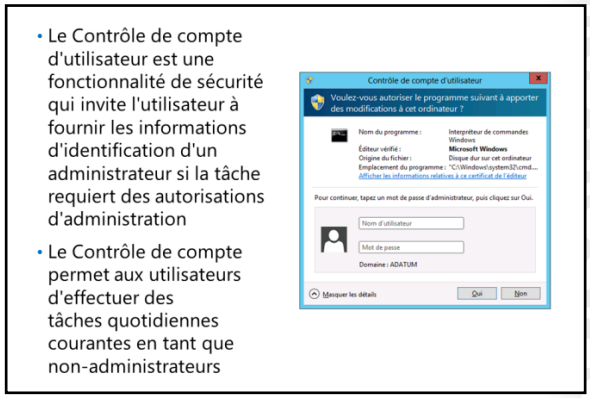
Vous pouvez également configurer les paramètres des options de sécurité en accédant à l'emplacement suivant dans la console de gestion des stratégies de groupe : **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité**.

Voici des exemples d'options de sécurité couramment utilisées :

- **Prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire**. Détermine combien de jours avant l'expiration d'un mot de passe de l'utilisateur, le système d'exploitation doit fournir un avertissement.
- **Ouverture de session interactive : ne pas afficher le dernier nom d'utilisateur**. Détermine si le nom du dernier utilisateur à s'être connecté à l'ordinateur doit s'afficher dans la fenêtre d'ouverture de session de Windows.
- **Comptes : renommer le compte administrateur**. Détermine si un nom de compte différent est associé à l'identificateur de sécurité (SID) pour le compte Administrateur.
- **Périphériques : autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session localement**. Détermine si un CD-ROM est accessible simultanément aux utilisateurs locaux et distants.

Configuration du contrôle de compte d'utilisateur

Les comptes administrateur comportent des risques de sécurité plus élevés. Lorsqu'un compte administrateur est connecté, ses privilèges autorisent l'accès au système d'exploitation Windows tout entier, y compris au Registre, aux fichiers système et aux paramètres de configuration. Tant qu'un compte administrateur est connecté, le système est vulnérable à une attaque et susceptible d'être compromis.



Le *contrôle de compte d'utilisateur* (UAC) est une fonctionnalité de sécurité qui contribue à empêcher toute modification non autorisée d'un ordinateur. Pour cela, il demande l'autorisation de l'utilisateur ou des informations d'identification d'administrateur avant d'exécuter des actions susceptibles d'affecter le fonctionnement de l'ordinateur ou de modifier des paramètres affectant plusieurs utilisateurs.

Par défaut, les utilisateurs standard et les administrateurs exécutent des applications et accèdent à des ressources dans le contexte de sécurité d'un utilisateur standard. Le contrôle de compte d'utilisateur permet à un utilisateur d'élever son statut de compte d'utilisateur standard en compte administrateur sans avoir à se déconnecter, à basculer vers un autre utilisateur ni à utiliser l'option **Exécuter en tant que**. Pour cette raison, le contrôle de compte d'utilisateur crée un environnement plus sécurisé pour l'exécution et l'installation d'applications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Quand une application requiert une autorisation de niveau administrateur, le contrôle de compte d'utilisateur en avertit l'utilisateur, comme suit :

- Si l'utilisateur est un administrateur, l'utilisateur confirme son choix d'élever son niveau d'autorisation et de continuer. Ce processus de demande d'approbation est appelé *mode d'approbation Administrateur*.

Remarque : Dans Windows Server 2012, le compte Administrateur intégré ne s'exécute pas en mode d'approbation Administrateur. En conséquence, aucune invite de contrôle de compte d'utilisateur ne s'affiche lors de l'utilisation du compte administrateur local.

- Si l'utilisateur n'est pas un administrateur, il convient d'entrer un nom d'utilisateur et un mot de passe pour un compte doté d'autorisations administratives. La saisie d'informations d'identification d'administration fournit temporairement à l'utilisateur des privilèges d'administrateur, mais seulement pour effectuer la tâche actuelle. Une fois la tâche terminée, les autorisations redeviennent celles d'un utilisateur standard.

Lorsque vous utilisez ce processus de notification et d'élévation vers des privilèges de compte administrateur, aucune modification ne peut être apportée à l'ordinateur sans que l'utilisateur le sache, car une invite demande à l'utilisateur l'autorisation ou des informations d'identification d'administrateur. Cela peut permettre d'empêcher qu'un logiciel malveillant ou un logiciel espion soit installé sur un ordinateur ou y apporte des modifications.

Le contrôle de compte d'utilisateur permet d'effectuer les modifications au niveau système suivantes sans invite, même lorsqu'un utilisateur est connecté en tant qu'utilisateur local :

- installer des mises à jour à partir de Windows Update ;
- installer des pilotes à partir de Windows Update ou ceux qui sont fournis avec le système d'exploitation ;
- afficher les paramètres du système d'exploitation Windows ;
- coupler des périphériques Bluetooth avec l'ordinateur ;
- réinitialiser la carte réseau et exécuter d'autres tâches de diagnostic et de réparation du réseau.

Modification du comportement du contrôle de compte d'utilisateur

Vous pouvez modifier l'expérience de notification du contrôle de compte d'utilisateur pour régler la fréquence et le comportement des invites UAC. Pour modifier le comportement du contrôle de compte d'utilisateur sur un ordinateur unique, accédez au Panneau de configuration de Windows Server 2012, puis à Système et sécurité.

Vous pouvez également configurer les paramètres de contrôle de compte d'utilisateur en accédant à l'emplacement suivant dans la console de gestion des stratégies de groupe : **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\ Options de sécurité**.

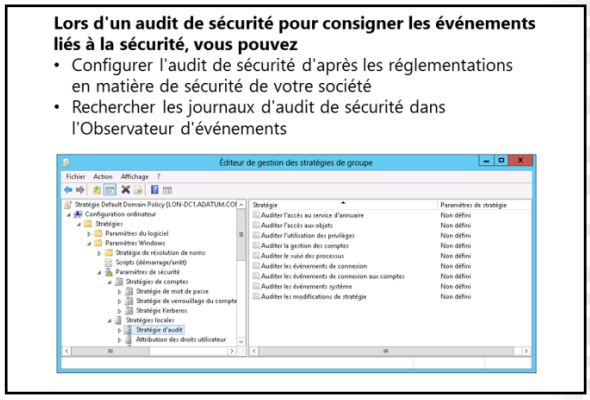
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous trouverez ci-après des exemples de paramètres d'objet de stratégie de groupe que vous pouvez configurer pour le contrôle de compte d'utilisateur :

- **Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur**. Contrôle le comportement de tous les paramètres de stratégie de contrôle de compte d'utilisateur pour l'ordinateur. Si ce paramètre est désactivé, le contrôle de compte d'utilisateur ne s'exécutera pas sur cet ordinateur.
- **Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré**. Lorsque vous activez ce paramètre, le compte Administrateur intégré utilise le mode d'approbation Administrateur.
- **Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation**. Ce paramètre contrôle le comportement de détection des installations d'applications pour l'ordinateur.
- **Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés**. Quand vous activez ce paramètre, une vérification d'infrastructure à clé publique est effectuée sur le fichier exécutable pour vérifier qu'il provient d'une source approuvée. Si le fichier est vérifié, il est autorisé à s'exécuter.

Remarque : Par défaut, le contrôle de compte d'utilisateur n'est pas configuré ni activé dans les installations minimales de Windows Server 2012.

Configuration de l'audit de sécurité



En général, un des composants de la stratégie de sécurité d'une organisation est l'enregistrement du comportement des activités des utilisateurs. Ce comportement peut inclure les tentatives réussies ou infructueuses d'accès aux données essentielles de l'entreprise stockées dans différents dossiers, ou les tentatives réussies ou infructueuses de connexion sur les différents serveurs. L'enregistrement de ces événements liés à la sécurité est appelé *audit de sécurité*. L'audit de sécurité génère des journaux d'événements de sécurité que les administrateurs peuvent consulter a posteriori dans l'observateur d'événements, dans le journal des événements de sécurité.

Après la configuration de l'audit, les informations présentes dans les journaux des événements de sécurité peuvent aider votre organisation à analyser sa conformité aux données d'entreprise et de sécurité importantes grâce au suivi précis d'activités définies, telles que :

- un administrateur de groupe qui a modifié des paramètres ou des données sur des serveurs contenant des informations hautement confidentielles ;
- un employé appartenant à un groupe donné qui a accédé à un dossier important contenant des données provenant de différents services ;
- un utilisateur qui essaie de se connecter à son compte à plusieurs reprises, sans succès, à partir d'un ordinateur interne à la société. Vous pouvez constater que l'employé qui possède ce compte d'utilisateur était en congés la semaine en question, ce qui signifie qu'un autre employé essayait de se connecter avec un compte d'utilisateur différent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez configurer les paramètres d'audit de sécurité en accédant à l'emplacement suivant dans la console de gestion des stratégies de groupe : **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Stratégie d'audit**.

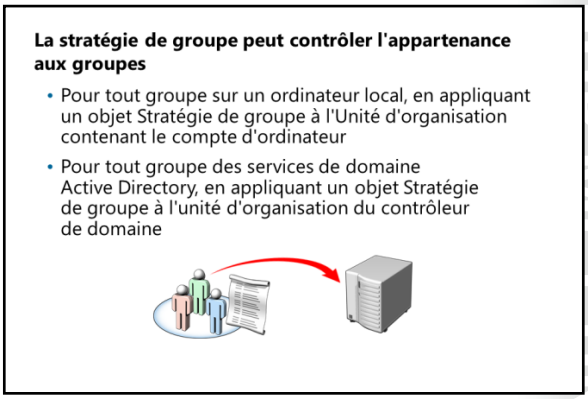
Vous trouverez ci-après des exemples de paramètres d'objet de stratégie de groupe que vous pouvez configurer pour l'audit :

- **Auditer les événements de connexion aux comptes**. Détermine si l'audit du système d'exploitation se produit chaque fois que l'ordinateur valide les informations d'identification d'un compte.
- **Auditer la gestion des comptes**. Détermine s'il convient d'auditer chaque événement de gestion des comptes, tel que la création, la modification, le changement de nom ou la suppression d'un compte d'utilisateur, la modification d'un mot de passe, ou l'activation et la désactivation d'un compte d'utilisateur.
- **Auditer l'accès aux objets**. Détermine si les audits du système d'exploitation ont accès aux objets non-Active Directory, tels que les dossiers et les fichiers. Avant de configurer les paramètres d'audit via une stratégie de groupe, vous devez configurer des listes de contrôle d'accès système (SACL) sur les dossiers ou les fichiers pour autoriser l'audit pour un type spécifique d'action, tel que l'écriture, la lecture ou la modification.
- **Auditer les événements système**. Détermine si le système d'exploitation effectue l'audit d'événements liés au système, tels que les tentatives de modification de l'heure système, les tentatives de démarrage ou d'arrêt du système, ou la taille du journal de sécurité dépassant un niveau de seuil d'avertissement configurable.

Documentation supplémentaire : Pour plus d'informations sur l'audit de sécurité, consultez l'article sur les nouveautés en matière d'audit de sécurité, à l'adresse http://go.microsoft.com/fwlink/?LinkID=266747.

Configuration des groupes restreints

Dans certains cas, vous pouvez souhaiter contrôler l'appartenance à certains groupes dans un domaine, tels que le groupe des administrateurs locaux, pour empêcher l'ajout d'autres comptes d'utilisateur à ces groupes.



Vous pouvez utiliser la stratégie Groupes restreints pour contrôler l'appartenance aux groupes en spécifiant les membres qui sont placés dans un groupe. Si vous définissez une stratégie de groupes restreints puis actualisez la stratégie de groupe, tout membre actuel d'un groupe qui ne figure pas dans la liste des membres de la stratégie de groupes restreints sera supprimé, y compris les membres par défaut tels que les administrateurs de domaine.

Bien que vous puissiez contrôler les groupes de domaine en attribuant des stratégies de groupes restreints aux contrôleurs de domaine, vous devez principalement utiliser ce paramètre pour configurer l'appartenance aux groupes essentiels, tels que les groupes Administrateurs de l'entreprise et Administrateurs du schéma. Vous pouvez également utiliser ce paramètre pour contrôler l'appartenance aux groupes locaux intégrés sur les stations de travail et les serveurs membres. Par exemple, vous pouvez placer le groupe Support technique dans le groupe Administrateurs local sur toutes les stations de travail.

Vous ne pouvez pas spécifier d'utilisateurs locaux dans un objet de stratégie de groupe de domaine. Les utilisateurs locaux qui se trouvent actuellement dans le groupe local contrôlé par la stratégie de groupes restreints seront supprimés. La seule exception à cela concerne le compte Administrateurs local qui figure toujours dans le groupe Administrateurs local.

Vous pouvez configurer les paramètres de groupes restreints en accédant à l'emplacement suivant dans la console de gestion des stratégies de groupe : **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Groupes restreints**.

Configuration des paramètres de stratégie de compte

Les stratégies de comptes protègent les comptes et les données de votre organisation en atténuant la menace que représentent les attaques qui essaient de deviner le nom d'utilisateur et le mot de passe d'un compte (elles sont parfois appelées *attaques en force brute*). La sécurisation de votre environnement réseau exige que tous les utilisateurs utilisent des mots de passe forts. Vous utilisez les paramètres de stratégie de mot de passe pour contrôler la complexité et la durée de vie des mots de passe utilisateur. Vous configurez les paramètres de stratégie de mot de passe via unes stratégies de groupe.

Les stratégies de compte atténuent la menace des attaques en force pour deviner les mots de passe de compte

Stratégies	Paramètres par défaut
Mot de passe	• Complexité des contrôles et durée de vie des mots de passé • Durée de vie maximale des mots de passe : 42 jours • Durée de vie minimale des mots de passe : 1 jour • Longueur minimale des mots de passe : 7 caractères • Mot de passe complexe : active • Enregistrer les mots de passe en utilisant un cryptage réversible : désactivé
Verrouillage de compte	• Contrôle le nombre de tentatives incorrectes qui peuvent être effectuées • Durée de verrouillage non défini • Seuil de verrouillage : 0 tentatives d'ouvertures de session non valides • Réinitialiser le verrouillages du compte après : non défini
Kerberos	• Sous-ensemble des attributs de la stratégie de sécurité de domaine • Peut uniquement être appliqué au niveau du domaine

Stratégies de comptes

Les composants des stratégies de comptes incluent les stratégies de mot de passe, les stratégies de verrouillage de compte et la stratégie Kerberos.

Les paramètres de stratégie sous Stratégies de comptes sont implémentés au niveau du domaine. Un domaine Windows Server 2012 peut avoir plusieurs stratégies de mot de passe et de verrouillage de compte, appelées *stratégies de mot de passe affinées*. Vous pouvez appliquer ces différentes stratégies à un utilisateur ou à un groupe de sécurité global dans un domaine, mais pas à une unité d'organisation.

Remarque : Si vous devez appliquer une stratégie de mot de passe affinée aux utilisateurs d'une unité d'organisation, vous pouvez utiliser un *groupe de clichés instantanés*, qui est un groupe de sécurité global qui est logiquement mappé à une unité d'organisation.

Vous pouvez configurer les paramètres des stratégies de comptes en accédant à l'emplacement suivant dans la console de gestion des stratégies de groupe : **Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de comptes**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégie de mot de passe

Les stratégies de mot de passe que vous pouvez configurer sont répertoriées dans le tableau ci-dessous.

Stratégie	Fonction	Meilleure pratique
Le mot de passe doit respecter des exigences de complexité	• Exige que les mots de passe : o doit être au moins égal à la longueur minimale du mot de passe spécifiée, avec au moins 3 caractères si la longueur minimale du mot de passe est définie sur 0.; o contiennent une combinaison d'au moins trois des types de caractères suivants : lettres majuscules, lettres minuscules, chiffres et symboles (signes de ponctuation) ; o ne contiennent ni le nom d'utilisateur ni le nom d'écran de l'utilisateur.	Activez ce paramètre. Ces exigences de complexité contribuent à garantir un mot de passe fort. Il est plus difficile de déchiffrer les mots de passe forts que ceux contenant des lettres et des chiffres simples. Indiquez aux utilisateurs d'utiliser des expressions comme mots de passe afin de créer de longs mots de passe faciles à mémoriser.
Appliquer l'historique des mots de passe	Empêche les utilisateurs de créer un nouveau mot de passe identique à leur mot de passe actuel ou à un mot de passe utilisé récemment. Pour spécifier le nombre de mots de passe mémorisés, fournissez une valeur. Par exemple, la valeur 1 signifie que seul le dernier mot de passe sera mémorisé, tandis que la valeur 5 signifie que les cinq mots de passe précédents seront mémorisés.	Plus le nombre est élevé, plus la sécurité est renforcée. La valeur par défaut est 24. L'application de l'historique des mots de passe garantit que des mots de passe ayant été compromis ne sont pas réutilisés.
Durée de vie maximale du mot de passe	Définit le nombre maximal de jours pendant lesquels un mot de passe est valide. Après ce nombre de jours, l'utilisateur doit modifier le mot de passe.	La valeur par défaut est 42 jours, mais il est recommandé de paramétrer 90 jours. Le paramétrage d'un nombre de jours trop élevé fournit aux pirates informatiques une plus grande fenêtre de temps pour déterminer le mot de passe. Le paramétrage d'un nombre de jours trop bas génère une frustration chez les utilisateurs qui doivent modifier leurs mots de passe trop fréquemment, et peut entraîner des appels plus fréquents au support technique.

(suite)

Stratégie	Fonction	Meilleure pratique
Durée de vie minimale du mot de passe	Définit le nombre minimal de jours qui doivent s'écouler avant qu'un mot de passe puisse être modifié.	Définissez la durée de vie minimale du mot de passe sur au moins 1 jour. En procédant ainsi, vous permettez à l'utilisateur de changer son mot de passe une fois par jour seulement. Ceci permet d'appliquer d'autres paramètres. Par exemple, si les cinq derniers mots de passe sont mémorisés, ceci garantit qu'au moins cinq jours s'écoulent avant que l'utilisateur puisse réutiliser le mot de passe d'origine. Si la durée de vie minimale du mot de passe est définie sur 0, l'utilisateur peut modifier son mot de passe six fois le même jour et commencer à réutiliser le mot de passe d'origine le même jour.
Longueur minimale du mot de passe	Spécifie le nombre minimal de caractères qu'un mot de passe peut comporter.	Définissez comme longueur une valeur comprise entre 8 et 12 caractères (à condition qu'ils répondent également aux exigences de complexité). Il est plus difficile de pirater un mot de passe plus long qu'un mot de passe plus court, à condition que le mot de passe ne soit pas un mot ou une expression courante.
Enregistrer les mots de passe en utilisant un chiffrement réversible	Fournit une prise en charge pour les applications qui exigent la connaissance d'un mot de passe utilisateur pour l'authentification.	N'utilisez ce paramètre que si vous utilisez un programme qui le requiert. L'activation de ce paramètre diminue la sécurité des mots de passe stockés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégie de verrouillage du compte

Les stratégies de verrouillage de compte que vous pouvez configurer sont répertoriées dans le tableau ci-dessous.

Stratégie	Fonction	Meilleure pratique
Seuil de verrouillage de comptes	Spécifie le nombre d'échecs de connexion autorisés avant que le compte soit verrouillé. Par exemple, si le seuil a pour valeur 3, le compte est verrouillé lorsqu'un utilisateur entre trois fois des informations de connexion incorrectes.	Un paramètre de 5 tient compte d'une erreur utilisateur raisonnable et limite les tentatives de connexion répétées à des fins malveillantes.
Durée de verrouillage des comptes	Permet de spécifier un délai, en minutes, après lequel le compte est déverrouillé et reprend automatiquement un fonctionnement normal. Si vous spécifiez 0, le compte sera verrouillé indéfiniment jusqu'à ce qu'un administrateur le déverrouille manuellement.	Une fois que le seuil a été atteint et que le compte est verrouillé, le compte doit rester verrouillé assez longtemps pour bloquer ou décourager toute attaque potentielle, mais pas trop longtemps pour ne pas gêner la productivité des utilisateurs légitimes. Une durée de 30 à 90 minutes est adaptée à la plupart des situations.
Réinitialiser le compteur de verrouillages du compte après	Définit un délai pour compter les tentatives de connexion incorrectes. Si la stratégie est définie pour une heure et que le seuil de verrouillage de compte est défini pour trois tentatives, un utilisateur peut entrer des informations de connexion incorrectes trois fois en une heure. Si l'utilisateur entre deux fois des informations incorrectes, mais entre les informations correctes la troisième fois, le compteur est réinitialisé après une heure (après la première entrée incorrecte) de sorte que le compte de tentatives infructueuses reprendra à un.	L'utilisation d'un délai compris entre 30 et 60 minutes est habituellement suffisant pour décourager les attaques automatisées et les tentatives manuelles d'un intrus de deviner un mot de passe.

Stratégie Kerberos

Cette stratégie est destinée aux comptes d'utilisateur de domaine et détermine les paramètres liés à Kerberos tels que l'application et la durée de vie des tickets. Les stratégies Kerberos n'existent pas dans la stratégie Ordinateur Local.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique A : Renforcement de la sécurité des ressources de serveur

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

Vous avez travaillé pour A. Datum pendant plusieurs années en tant que spécialiste du support technique. Votre fonction consistait à examiner les ordinateurs de bureau pour résoudre les problèmes d'application et les problèmes réseau. Vous avez récemment accepté une promotion au sein de l'équipe d'assistance technique des serveurs. En tant que nouveau membre de l'équipe, votre rôle consiste à aider à déployer et configurer de nouveaux serveurs et services dans l'infrastructure existante, conformément aux instructions fournies par votre responsable informatique.

Votre responsable vous a donné quelques paramètres relatifs à la sécurité qui doivent être implémentés sur tous les serveurs membres. Vous devez également implémenter l'audit du système de fichiers pour un partage de fichiers utilisé par le service Marketing. Enfin, vous devez implémenter l'audit pour les connexions au domaine.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- utiliser les stratégies de groupe pour sécuriser les serveurs membres ;
- effectuer l'audit de l'accès au système de fichiers ;
- effectuer l'audit des connexions au domaine.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-SVR1 22410B-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 **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22410B-LON-DC1** puis, dans le volet Actions, cliquez sur **Démarrer**.
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 **22410B-LON-SVR1** et les étapes 2 et 3 pour **22410B-LON-CL1**. Ne vous connectez pas à LON-CL1 tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Utilisation des stratégies de groupe pour sécuriser les serveurs membres

Scénario

A. Datum utilise le groupe Administrateurs d'ordinateur pour fournir aux administrateurs les autorisations permettant d'administrer les serveurs membres. Dans le cadre de la procédure d'installation d'un nouveau serveur, le groupe Administrateurs d'ordinateur du domaine est ajouté au groupe Administrateurs local sur le nouveau serveur. Récemment, cette étape importante manquait lors de la configuration de plusieurs nouveaux serveurs membres.

Pour s'assurer que le groupe Administrateurs d'ordinateur bénéficie toujours de l'autorisation permettant de gérer les serveurs membres, votre responsable vous a demandé de créer un objet de stratégie de groupe qui définisse l'appartenance au groupe Administrateurs local sur les serveurs membres pour inclure les administrateurs d'ordinateur serveur. Cet objet de stratégie de groupe doit également activer le mode d'approbation Administrateur pour le contrôle de compte d'utilisateur.

Les tâches principales de cet exercice sont les suivantes :

1. Créer une unité d'organisation de serveurs membres et y placer les serveurs
2. Créer un groupe Administrateurs de serveur
3. Créer un objet de stratégie de groupe des paramètres de sécurité des serveurs membres et le lier à l'unité d'organisation Serveurs membres
4. Configurer l'appartenance aux groupes pour les administrateurs locaux afin d'inclure les groupes Administrateurs de serveur et Administrateurs de domaine
5. Vérifier que les administrateurs d'ordinateur ont été ajoutés au groupe Administrateurs local
6. Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour supprimer des utilisateurs de l'autorisation Permettre l'ouverture d'une session locale
7. Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré
8. Vérifier qu'un utilisateur ne disposant pas de droits d'administration ne peut pas se connecter à un serveur membre

▶ Tâche 1 : Créer une unité d'organisation de serveurs membres et y placer les serveurs

1. Sur LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Créez une nouvelle unité d'organisation appelée **Unité d'organisation Serveurs membres**.
3. Placez les serveurs **LON-SVR1** et **LON-SVR2** dans **Unité d'organisation Serveurs membres**.

▶ Tâche 2 : Créer un groupe Administrateurs de serveur

- Sur LON-DC1, dans **Unité d'organisation Serveurs membres**, créez un nouveau groupe de sécurité global appelé **Administrateurs de serveur**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Créer un objet de stratégie de groupe des paramètres de sécurité des serveurs membres et le lier à l'unité d'organisation Serveurs membres

1. Sur LON-DC1, ouvrez la **console de gestion des stratégies de groupe**.
2. Dans la console de gestion des stratégies de groupe (GPMC), dans le conteneur Objets de stratégie de groupe, créez un nouvel **objet de stratégie de groupe** avec un nom **Paramètres de sécurité des serveurs membres**.
3. Dans la console de gestion des stratégies de groupe, liez l'objet **Paramètres de sécurité des serveurs membres** à l'**unité d'organisation Serveurs membres**.

▶ Tâche 4 : Configurer l'appartenance aux groupes pour les administrateurs locaux afin d'inclure les groupes Administrateurs de serveur et Administrateurs de domaine

1. Sur LON-DC1, ouvrez la **console de gestion des stratégies de groupe**.
2. Modifiez **Default Domain Policy**.
3. Accédez à **Configuration ordinateur**, cliquez sur **Stratégies**, sur **Paramètres Windows**, sur **Paramètres de sécurité**, puis sur **Groupes restreints**.
4. Ajoutez les groupes **Administrateurs de serveur** et **ADATUM\Admins du domaine** au groupe **Administrateurs**.
5. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 5 : Vérifier que les administrateurs d'ordinateur ont été ajoutés au groupe Administrateurs local

1. Basculez vers **LON-SVR1**, puis connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez une fenêtre Windows PowerShell®, et à l'invite de commande Windows PowerShell, tapez la commande suivante :

```
Gpupdate /force
```

3. Ouvrez le **Gestionnaire de serveur**, ouvrez la console **Gestion de l'ordinateur**, puis développez **Utilisateurs et groupes locaux**.
4. Confirmez que le groupe **Administrateurs** contient à la fois **ADATUM\Admins du domaine** et **ADATUM\Administrateurs de serveur** comme membres.
5. Fermez la console **Gestion de l'ordinateur**.

▶ Tâche 6 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour supprimer des utilisateurs de l'autorisation Permettre l'ouverture d'une session locale

1. Basculez vers **LON-DC1**.
2. Sur LON-DC1, dans GPMC, modifiez l'objet GPO **Paramètres de sécurité des serveurs membres**.
3. Dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Attribution des droits utilisateur** et configurez **Permettre l'ouverture d'une session locale** pour les groupes de sécurité **Admins du domaine** et **Administrateurs**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 7 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

1. Sur LON-DC1, dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité**.
2. Activez **Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré**.
3. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 8 : Vérifier qu'un utilisateur ne disposant pas de droits d'administration ne peut pas se connecter à un serveur membre

1. Basculez vers LON-SVR1.
2. Ouvrez une fenêtre Windows PowerShell et à l'invite de commande Windows PowerShell, tapez la commande suivante :

```
Gpupdate /force
```

3. Déconnectez-vous de LON-SVR1.
4. Essayez de vous connecter à **LON-SVR1** en tant qu'**ADATUM\Adam** avec le mot de passe **Pa$$w0rd**.
5. Vérifiez que vous ne pouvez pas vous connecter à LON-SVR1.
6. Pour préparer l'exercice suivant, déconnectez-vous de LON-SVR1 et connectez-vous de nouveau à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devrez avoir utilisé les stratégies de groupe pour sécuriser les serveurs membres.

Exercice 2 : Audit de l'accès au système de fichiers

Scénario

Le directeur du service Marketing s'intéresse à une éventuelle possibilité d'effectuer le suivi des personnes qui accèdent aux fichiers situés dans le partage de fichiers du service. Votre responsable lui a répondu que seuls les utilisateurs dotés d'autorisations sont autorisés à accéder aux fichiers. Toutefois, le directeur du service Marketing voudrait essayer de consigner les accès aux fichiers situés dans le partage de fichiers pour voir quels utilisateurs accèdent à des fichiers spécifiques.

Votre responsable vous a demandé d'activer l'audit pour le système de fichiers qui se trouve dans le partage de fichiers du service Marketing et de passer en revue les résultats avec le directeur du service Marketing.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer l'audit de l'accès aux objets
2. Créer et partager un dossier
3. Activer l'audit sur le dossier Marketing pour les utilisateurs du domaine
4. Créer un nouveau fichier dans le partage de fichiers à partir de LON-CL1
5. Visualiser les résultats dans le journal de sécurité sur le contrôleur de domaine

▶ Tâche 1 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer l'audit de l'accès aux objets

1. Basculez vers **LON-DC1**.
2. Connectez-vous à **LON-DC1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans la console GPMC, modifiez l'objet GPO **Paramètres de sécurité des serveurs membres**.
4. Dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Stratégie d'audit**.
5. Activez **Auditer l'accès aux objets** avec les deux paramètres **Réussite** et **Échec**.
6. Déconnectez-vous de LON-DC1.

▶ Tâche 2 : Créer et partager un dossier

1. Basculez vers **LON-SVR1**.
2. Connectez-vous à **LON-SVR1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Sur LON-SVR1, sur le lecteur C, créez un nouveau dossier avec le nom **Marketing**.
4. Configurez le dossier **Marketing** avec les autorisations de partage **Lecture/écriture** pour l'utilisateur **Adam**.

▶ Tâche 3 : Activer l'audit sur le dossier Marketing pour les utilisateurs du domaine

1. Sur LON-SVR1, dans la fenêtre Disque local (C:), configurez l'audit sur le dossier **Marketing**, avec les paramètres suivants :
   - Sélectionnez un principal : **Utilisateurs du domaine**
   - Type : **Tout**
   - Autorisation : **Lecture et exécution, Affichage du contenu du dossier, Lecture, Écriture**
   - Conservez les valeurs par défaut des autres paramètres.
2. Actualisez la stratégie de groupe en tapant la commande suivante dans une fenêtre PowerShell :

```
gpupdate /force
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Créer un nouveau fichier dans le partage de fichiers à partir de LON-CL1

1. Basculez vers **LON-CL1**.
2. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante :

```
gpupdate /force
```

4. Fermez la fenêtre d'invite de commandes.
5. Déconnectez-vous de LON-CL1, puis connectez-vous de nouveau en tant qu'**ADATUM\Adam** avec le mot de passe **Pa$$w0rd**.
6. Ouvrez le dossier **Marketing** sur LON-SVR1 en utilisant le chemin d'accès UNC suivant : **\\LON-SVR1\Marketing**.
7. Créez un document texte nommé **Employés**.
8. Déconnectez-vous de LON-CL1.

▶ Tâche 5 : Visualiser les résultats dans le journal de sécurité sur le contrôleur de domaine

1. Basculez vers **LON-SVR1**, et démarrez l'**observateur d'événements**.
2. Dans la fenêtre de l'observateur d'événements, développez **Journaux Windows**, puis ouvrez **Sécurité**.
3. Vérifiez que l'événement et les informations suivants s'affichent :
   - Source : **Microsoft Windows Security Auditing**
   - ID d'événement : **4663**
   - Catégorie de la tâche : **Système de fichiers**
   - Une tentative d'accès à un objet a été effectuée.

Résultats : À la fin de cet exercice, vous devrez avoir activé l'audit des accès au système de fichiers.

Exercice 3 : Audit des connexions au domaine

Scénario

Après un examen de la sécurité, le comité de stratégie informatique a décidé de commencer à effectuer le suivi de toutes les connexions des utilisateurs au domaine. Votre responsable vous a demandé d'activer l'audit des connexions au domaine et de vérifier qu'elles fonctionnent.

Les tâches principales de cet exercice sont les suivantes :

1. Modifier l'objet GPO Stratégie de domaine par défaut
2. Exécuter GPUpdate
3. Se connecter à LON-CL1 avec un mot de passe incorrect
4. Examiner les journaux des événements sur LON-DC1
5. Se connecter à LON-CL1 avec le mot de passe correct
6. Examiner les journaux des événements sur LON-DC1

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Modifier l'objet GPO Stratégie de domaine par défaut

1. Basculez vers **LON-DC1**.
2. Connectez-vous à **LON-DC1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Sur LON-DC1, démarrez le **Gestionnaire de serveur**, puis, dans le Gestionnaire de serveur, démarrez la console **GPMC**.
4. Sur LON-DC1, dans la console GPMC, modifiez l'objet GPO **Default Domain Policy**.
5. Dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Stratégie d'audit**.
6. Activez **Auditer les événements de connexion aux comptes** avec les deux paramètres **Réussite** et **Échec**.
7. Mettez à jour la stratégie de groupe en utilisant la commande **gpupdate /force**.

▶ Tâche 2 : Exécuter GPUpdate

1. Basculez vers **LON-CL1**.
2. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante :

```
gpupdate /force
```

4. Fermez la fenêtre d'invite de commandes et déconnectez-vous de LON-CL1.

▶ Tâche 3 : Se connecter à LON-CL1 avec un mot de passe incorrect

- Connectez-vous à LON-CL1 en tant qu'**ADATUM\Adam** avec le mot de passe **password**.

Remarque : Ce mot de passe est intentionnellement incorrect afin de générer une entrée de journal de sécurité indiquant qu'une tentative de connexion infructueuse a été effectuée.

▶ Tâche 4 : Examiner les journaux des événements sur LON-DC1

1. Sur LON-DC1, démarrez l'**observateur d'événements**.
2. Dans la fenêtre de l'**observateur d'événements**, développez **Journaux Windows**, puis cliquez sur **Sécurité**.
3. Examinez les journaux des événements pour rechercher le message suivant : « **ID d'événement 4771 La pré-authentification Kerberos a échoué. Informations sur le compte : ID de sécurité : ADATUM\Adam**. »

▶ Tâche 5 : Se connecter à LON-CL1 avec le mot de passe correct

- Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Adam** avec le mot de passe **Pa$$w0rd**.

Remarque : Ce mot de passe est correct et vous devriez pouvoir vous connecter avec succès en tant qu'**Adam**.

▶ Tâche 6 : Examiner les journaux des événements sur LON-DC1

1. Sur LON-DC1, démarrez l'**observateur d'événements**.
2. Dans la fenêtre de l'**observateur d'événements**, développez **Journaux Windows**, puis cliquez sur **Sécurité**.
3. Examinez les journaux des événements pour rechercher le message suivant : « **ID d'événement 4624 L'ouverture de session d'un compte s'est correctement déroulée. Nouvelle connexion : ID de sécurité : ADATUM\Adam**. »

Résultats : À la fin de cet exercice, vous devrez avoir activé l'audit des connexions au domaine.

▶ Pour préparer l'atelier suivant

- Pour préparer l'atelier pratique suivant, laissez les ordinateurs virtuels s'exécuter.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Restriction de l'accès aux logiciels

Les utilisateurs ont besoin d'avoir accès aux applications qui les aident à effectuer leur travail. Toutefois, des applications inutiles ou indésirables sont souvent installées sur les ordinateurs clients, que ce soit involontairement, dans un but malveillant ou à un usage non professionnel. Les logiciels non pris en charge ou inutilisés ne font pas l'objet d'une maintenance et ne sont pas sécurisés par les administrateurs, si bien qu'ils sont susceptibles de servir de point d'entrée à des personnes malveillantes en leur procurant un accès non autorisé ou en diffusant des virus informatiques. Par conséquent, il est primordial que vous vous assuriez que seuls les logiciels nécessaires sont installés sur tous les ordinateurs de votre organisation. Il est également essentiel que vous empêchiez l'exécution des logiciels non autorisés ou qui ne sont plus utilisés ou pris en charge.

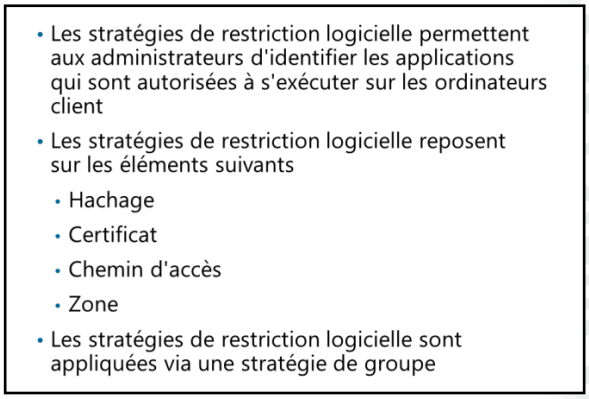
Objectifs de la leçon

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

- expliquer comment utiliser les stratégies de restriction logicielle pour empêcher l'exécution des logiciels non autorisés sur les serveurs et les clients ;
- décrire le rôle d'AppLocker® ;
- décrire les règles AppLocker et la manière de les utiliser pour empêcher l'exécution des logiciels non autorisés sur les serveurs et les clients ;
- décrire comment créer des règles AppLocker.

Que sont les stratégies de restriction logicielle ?

Introduites dans le système d'exploitation Windows XP et le système d'exploitation Windows Server 2003, les stratégies de restriction logicielle (SRP) fournissent aux administrateurs des outils leur permettant d'identifier et de spécifier les applications qui sont autorisées à s'exécuter sur les ordinateurs clients. Vous configurez et déployez les paramètres de stratégie de restriction logicielle sur les clients à l'aide des stratégies de groupe.



Les stratégies de restriction logicielle sont utilisées dans Windows Server 2012 pour assurer la compatibilité avec Windows XP et Windows Vista®. Une stratégie de restriction logicielle définie se compose de règles et de niveaux de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Règles

Les règles régissent la manière dont la stratégie de restriction logicielle répond à une application en cours d'exécution ou d'installation. Les règles sont les éléments principaux d'une stratégie de restriction logicielle, et un groupe de règles détermine comment une stratégie de restriction logicielle répond aux applications qui sont exécutées. Les règles peuvent s'appuyer sur l'un des critères suivants qui s'appliquent au fichier exécutable principal de l'application en question :

- Hachage. Empreinte digitale cryptographique du fichier.
- Certificat. Certificat d'éditeur de logiciels utilisé pour signer numériquement un fichier.
- Chemin d'accès. Chemin d'accès local ou UNC de l'emplacement où le fichier est stocké.
- Zone. Zone Internet.

Niveaux de sécurité

Un niveau de sécurité est attribué à chaque stratégie de restriction logicielle et régit la manière dont le système d'exploitation réagit quand l'application définie dans la règle est exécutée. Les trois paramètres disponibles de niveau de sécurité sont les suivants :

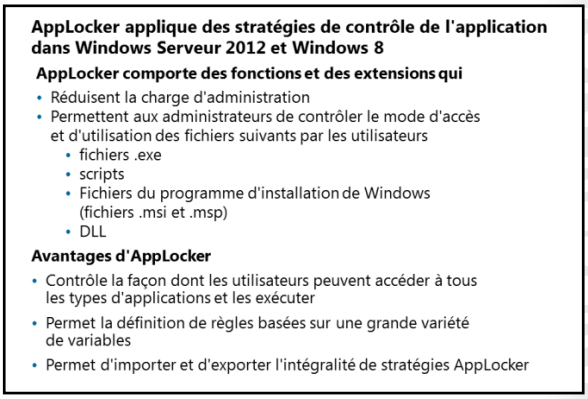
- **Rejeté**. Le logiciel identifié dans la règle ne s'exécutera pas, indépendamment des droits d'accès de l'utilisateur.
- **Utilisateur standard**. Autorise le logiciel identifié dans la règle à s'exécuter en tant qu'utilisateur standard ne bénéficiant pas d'autorisations d'administration.
- **Non restreint**. Autorise le logiciel identifié dans la règle à s'exécuter sans être limité par la stratégie de restriction logicielle.

Ces trois paramètres permettent d'utiliser les stratégies de restriction logicielle de deux manières principales :

- Si un administrateur dispose de la liste complète de tous les logiciels qui devraient être autorisés à s'exécuter sur les clients, le niveau de sécurité par défaut peut être défini sur **Rejeté**. Toutes les applications qui devraient être autorisées à s'exécuter peuvent être identifiées dans des règles de stratégie de restriction logicielle qui appliqueraient le niveau de sécurité **Utilisateur standard** ou **Non restreint** à chaque application individuelle, selon les exigences de sécurité.
- Si un administrateur ne possède pas la liste complète des logiciels qui devraient être autorisés à s'exécuter sur les clients, le niveau de sécurité par défaut peut être défini sur **Non restreint** ou **Utilisateur standard**, selon les exigences de sécurité. Toutes les applications qui ne doivent pas être autorisées à s'exécuter peuvent alors être identifiées à l'aide des règles de stratégie de restriction logicielle, qui utiliseraient le paramètre de niveau de sécurité **Rejeté**.

Les paramètres de stratégie de restriction logicielle se trouvent dans les stratégies de groupe, à l'emplacement suivant : Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de restriction logicielle.

Qu'est-ce qu'AppLocker ?



AppLocker, qui a été introduit dans les systèmes d'exploitation Windows 7 et Windows Server 2008 R2, est une fonctionnalité liée aux paramètres de sécurité, qui contrôle quelles applications les utilisateurs sont autorisés à exécuter.

AppLocker fournit aux administrateurs diverses méthodes pour déterminer rapidement et avec concision l'identité des applications qu'ils souhaitent restreindre ou auxquelles ils souhaitent autoriser l'accès. Vous appliquez AppLocker via unes stratégies de groupe à des objets ordinateur dans une unité d'organisation. Vous pouvez également appliquer des règles AppLocker individuelles à des groupes ou des utilisateurs AD DS individuels.

AppLocker contient également des options de surveillance et d'audit de l'application des règles. AppLocker aide les organisations à empêcher l'exécution de logiciels malveillants ou sans licence, et peut restreindre sélectivement l'installation des contrôles ActiveX®. Il peut également réduire le coût total de possession en vérifiant que les stations de travail sont standardisées dans l'ensemble de l'entreprise et que les utilisateurs exécutent uniquement les logiciels et applications approuvés par l'entreprise.

L'utilisation de la technologie AppLocker permet aux sociétés de réduire la charge d'administration et aide les administrateurs à contrôler la façon dont les utilisateurs peuvent accéder aux fichiers, par exemple aux fichiers .exe, aux scripts, aux fichiers Windows Installer (fichiers .msi et .msp) et aux fichiers .dll, et peuvent les utiliser.

Vous pouvez utiliser AppLocker pour restreindre les logiciels qui :

- ne sont pas autorisés à être utilisés dans la société. Par exemple, les logiciels qui peuvent perturber la productivité des employés, tels que les logiciels de réseaux sociaux, ou les logiciels qui diffusent en continu des fichiers vidéo ou des images susceptibles d'utiliser une bande passante réseau et un espace disque importants ;
- ne sont plus utilisés ou qui ont été remplacés par une version plus récente. Par exemple, les logiciels qui ne font plus l'objet d'une maintenance ou pour lesquels les licences ont expiré ;
- ne sont plus pris en charge dans la société. Les logiciels qui ne sont pas mis à jour avec des mises à jour de sécurité peuvent générer un risque de sécurité ;
- doivent être utilisés uniquement par des services spécifiques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez configurer les paramètres AppLocker en accédant dans la console GPMC à : Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de contrôle de l'application.

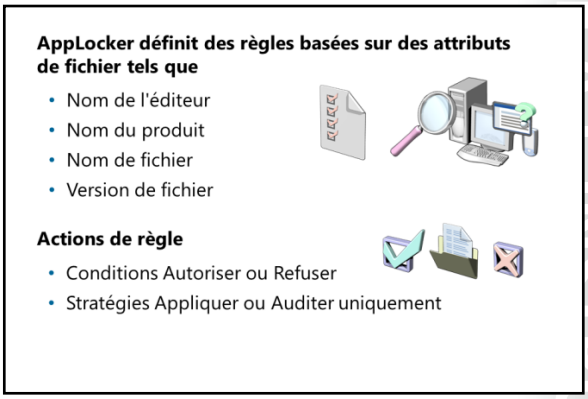
Remarque : AppLocker utilise le service Identité de l'application pour vérifier les attributs d'un fichier. Ce service doit être configuré pour démarrer automatiquement sur chaque ordinateur où AppLocker doit être appliqué. Si le service Identité de l'application ne s'exécute pas, les stratégies AppLocker ne doivent pas être appliquées.

Documentation supplémentaire : Pour plus d'informations sur AppLocker, consultez la présentation d'AppLocker à l'adresse http://go.microsoft.com/fwlink/?LinkID=266745.

Règles AppLocker

AppLocker définit des règles basées sur les attributs de fichier qui sont dérivés de la signature numérique du fichier. Les attributs de fichier présents dans la signature numérique comprennent :

- le nom de l'éditeur,
- le nom du produit,
- Nom de fichier
- la version du fichier.



Configuration par défaut

Par défaut, aucune stratégie Applocker n'est définie, ce qui signifie qu'aucune application n'est bloquée. Vous pouvez configurer des règles par défaut pour chaque collection de règles. Les règles par défaut garantissent que les applications figurant dans les répertoires Program Files et Windows sont autorisées à s'exécuter et que toutes les applications sont autorisées à s'exécuter pour le groupe Administrateurs. Les règles par défaut doivent être activées pour implémenter des stratégies Applocker, car ces applications sont nécessaires pour l'exécution et le fonctionnement normal des systèmes d'exploitation Windows.

Actions de règle Autoriser et Refuser

Autoriser et **Refuser** sont des actions de règle qui autorisent ou refusent l'exécution des applications en fonction d'une liste d'applications que vous configurez. L'action **Autoriser** sur des règles limite l'exécution des applications à une liste d'applications autorisées et bloque toutes les autres. L'action **Refuser** sur des règles adopte l'approche opposée et autorise l'exécution de n'importe quelle application à l'exception de celles figurant dans la liste des applications refusées. Ces actions fournissent également un moyen d'identifier des exceptions à ces actions.

Appliquer ou Auditer uniquement

Lorsque la stratégie AppLocker est définie sur **Appliquer**, les règles sont appliquées et tous les événements sont audités. Lorsque la stratégie AppLocker est définie sur **Auditer uniquement**, les règles sont évaluées et les événements sont consignés dans le journal d'AppLocker, mais aucune application n'a lieu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Création de règles AppLocker

Dans cette démonstration, vous allez apprendre à :

- créer un objet de stratégie de groupe pour appliquer les règles exécutables AppLocker par défaut ;
- appliquer l'objet de stratégie de groupe au domaine ;
- tester la règle AppLocker.

Procédure de démonstration

Créer un objet de stratégie de groupe pour appliquer les règles exécutables AppLocker par défaut

1. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-DC1, ouvrez la console **GPMC**.
3. Créez un nouvel objet GPO nommé **Stratégie de restriction de WordPad**.
4. Modifiez les **paramètres de sécurité** de la **stratégie de restriction de WordPad** en utilisant **AppLocker** pour créer une nouvelle **règle exécutable**.
5. Définissez l'autorisation de la nouvelle règle sur **Refuser**, la condition sur **Éditeur**, puis sélectionnez **wordpad.exe**. Si vous y êtes invité, cliquez sur **OK** pour créer des règles par défaut.
6. Dans l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de contrôle de l'application\AppLocker**.
7. Dans **AppLocker**, configurez l'application avec **Appliquez les règles**.
8. Dans l'**Éditeur de gestion des stratégies de groupe**, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Services système**.
9. Configurez **Propriétés de Identité de l'application** avec **Définir ce paramètre de stratégie**, et **Sélectionnez le mode de démarrage du service** avec **Automatique**.

Appliquer l'objet de stratégie de groupe au domaine

1. Dans la fenêtre **Gestion des stratégies de groupe**, appliquez l'objet GPO **Stratégie de restriction de WordPad** au domaine **Adatum.com**.
2. Ouvrez une fenêtre d'invite de commandes, tapez **gpupdate /force**, puis appuyez sur Entrée.
3. Démarrez **22410B-LON-CL1** et ouvrez une session en tant qu'**ADATUM\Alan**, avec le mot de passe **Pa$$w0rd**.
4. Dans la fenêtre d'invite de commandes, tapez **gpupdate /force**, puis appuyez sur Entrée. Attendez que la stratégie soit mise à jour.

Tester la règle AppLocker

- Sur **LON-CL1**, connectez-vous en tant qu'**ADATUM\Alan**, essayez de démarrer **WordPad**, puis vérifiez que WordPad ne démarre pas.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Configuration du Pare-feu Windows avec fonctions avancées de sécurité

Le Pare-feu Windows avec fonctions avancées de sécurité est un outil important qui permet d'améliorer la sécurité de Windows Server 2012. Ce composant logiciel enfichable contribue à empêcher divers problèmes de sécurité tels que la numérisation des ports ou les programmes malveillants. Le Pare-feu Windows avec fonctions avancées de sécurité possède plusieurs profils de pare-feu et applique pour chacun d'eux des paramètres uniques à différents types de réseaux. Vous pouvez configurer manuellement les règles du Pare-feu Windows sur chaque serveur, ou les configurer de manière centralisée à l'aide des stratégies de groupe.

Objectifs de la leçon

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

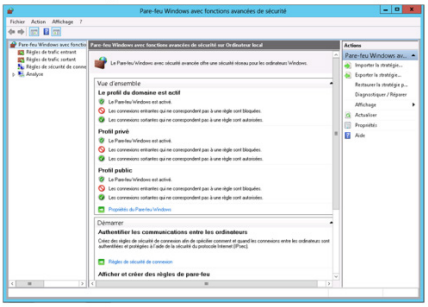
- décrire les fonctionnalités du Pare-feu Windows avec fonctions avancées de sécurité ;
- expliquer pourquoi un pare-feu basé sur l'hôte est important ;
- décrire les profils de pare-feu ;
- décrire les règles de sécurité de connexion ;
- expliquer comment déployer les règles du Pare-feu Windows.

Qu'est-ce que le Pare-feu Windows avec fonctions avancées de sécurité ?

Le Pare-feu Windows est un pare-feu basé sur l'hôte qui est inclus dans Windows Server 2012. Ce composant logiciel enfichable s'exécute sur l'ordinateur local et restreint l'accès réseau en direction et en provenance de cet ordinateur.

À la différence d'un pare-feu de périmètre, qui fournit une protection seulement contre les menaces provenant d'Internet, un pare-feu basé sur l'hôte assure une protection contre des menaces d'une origine quelconque. Par exemple, le Pare-feu Windows protège un hôte d'une menace interne au réseau local (LAN).

Le Pare-feu Windows est un pare-feu hôte avec état qui autorise ou bloque le trafic réseau selon la configuration



Règles de trafic entrant et sortant

Les règles de trafic entrant contrôlent la communication initialisée par un autre périphérique ou ordinateur sur le réseau, avec l'ordinateur hôte. Par défaut, toute communication entrante est bloquée, à l'exception du trafic qui est explicitement autorisé par une règle de trafic entrant.

Les règles de trafic sortant contrôlent la communication initialisée par l'ordinateur hôte et destinée à un périphérique ou un ordinateur sur le réseau. Par défaut, toute communication sortante est autorisée, à l'exception du trafic qui est explicitement bloqué par une règle de trafic sortant. Si vous choisissez de bloquer toutes les communications sortantes à l'exception du trafic explicitement autorisé, vous devez soigneusement cataloguer les logiciels autorisés à s'exécuter sur cet ordinateur et la communication réseau requise par ces logiciels.

Vous pouvez créer des règles de trafic entrant et sortant en fonction des ports UDP (User Datagram Protocol) et TCP (Transmission Control Protocol). Vous pouvez également créer des règles de trafic entrant et sortant qui autorisent un accès réseau exécutable spécifique, indépendamment du numéro de port utilisé.

Règles de sécurité de connexion

Vous utilisez les règles de sécurité de connexion pour configurer IPsec pour Windows Server 2012. Quand ces règles sont configurées, vous pouvez authentifier la communication entre les ordinateurs, puis utiliser ces informations pour créer des règles de pare-feu en fonction de comptes d'utilisateur et d'ordinateur spécifiques.

Options de configuration supplémentaires

Le Pare-feu Windows avec fonctions avancées de sécurité est un composant logiciel enfichable MMC (Microsoft Management Console) qui vous permet d'effectuer la configuration avancée du Pare-feu Windows.

Le Pare-feu Windows dans Windows 8 et Windows Server 2012 comporte les fonctionnalités suivantes :

- Il prend en charge le filtrage du trafic entrant et sortant.
- Il intègre des paramètres de filtrage de pare-feu et de protection IPsec.
- Il vous permet de configurer les règles de contrôle du trafic réseau.
- Il fournit des profils prenant en charge l'emplacement réseau.
- Il vous permet d'importer ou d'exporter des stratégies.

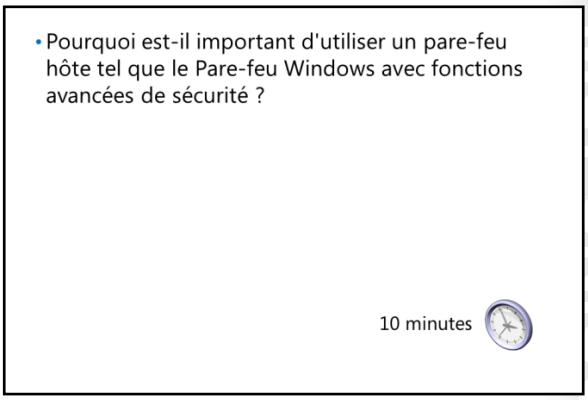
Vous pouvez configurer les paramètres du Pare-feu Windows sur chaque ordinateur individuellement, ou à l'aide d'une stratégie de groupe dans : Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Pare-feu Windows avec fonctions avancées de sécurité.

Remarque : Windows Server 2012 introduit l'option supplémentaire d'administration du Pare-feu Windows à l'aide de l'interface de ligne de commande Windows PowerShell.

Discussion : Pourquoi un pare-feu basé sur l'hôte est-il important ?

Examinez la question de discussion et prenez part à une discussion pour identifier les avantages de l'utilisation d'un pare-feu basé sur l'hôte tel que le Pare-feu Windows avec fonctions avancées de sécurité.

Question : Pourquoi est-il important d'utiliser un pare-feu hôte tel que le Pare-feu Windows avec fonctions avancées de sécurité ?

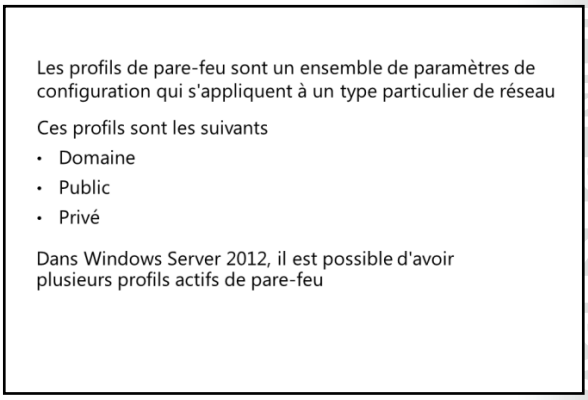


UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Profils de pare-feu

Le Pare-feu Windows avec fonctions avancées de sécurité utilise des profils de pare-feu pour fournir une configuration cohérente pour les réseaux d'un type spécifique et vous permet de définir un réseau comme réseau avec domaine, réseau public ou réseau privé.

Avec le Pare-feu Windows avec fonctions avancées de sécurité, vous pouvez définir un jeu de configuration pour chaque type de réseau ; chaque jeu de configuration est appelé *profil de pare-feu*. Les règles de pare-feu sont activées uniquement pour des profils de pare-feu spécifiques.



Le Pare-feu Windows avec fonctions avancées de sécurité inclut les profils répertoriés dans le tableau ci-dessous.

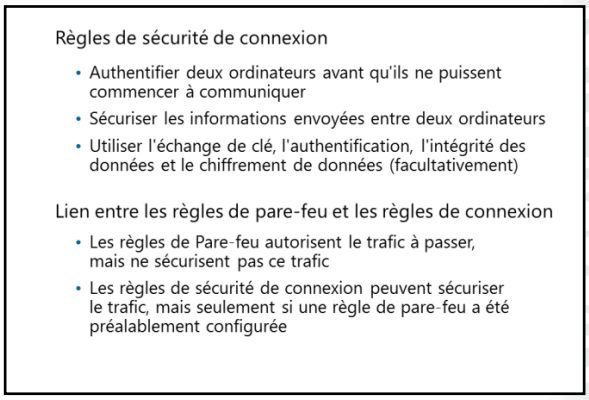
Profil	Description
Public	À utiliser quand vous êtes connecté à un réseau public non approuvé. À l'exception des réseaux avec domaine, tous les réseaux sont classés en tant que réseaux publics. Par défaut, le profil Public (qui est le plus restrictif) est utilisé dans Windows Vista, Windows 7 et Windows 8.
Privé	À utiliser quand vous êtes connecté derrière un pare-feu. Un réseau est classé comme privé seulement si un administrateur ou une application identifie le réseau comme privé. Les réseaux marqués comme Résidentiel ou Professionnel dans Windows Vista, Windows 7 et Windows 8 sont ajoutés au profil privé.
Domaine	À utiliser quand votre ordinateur fait partie d'un domaine de système d'exploitation Windows. Les systèmes d'exploitation Windows identifient automatiquement les réseaux dans lesquels il est possible d'authentifier l'accès au contrôleur de domaine. Le profil de domaine est attribué à ces réseaux et ce paramètre ne peut pas être modifié Aucun autre réseau ne peut être placé dans cette catégorie.

Windows Server 2012 permet à plusieurs profils de pare-feu d'être actifs simultanément sur un serveur. Cela signifie qu'un serveur multi-résident qui est connecté au réseau interne et au réseau de périmètre peut appliquer le profil de pare-feu de domaine au réseau interne et le profil de pare-feu public ou privé au réseau de périmètre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Règles de sécurité de connexion

Une règle de sécurité de connexion force l'authentification entre deux ordinateurs homologues avant qu'ils ne puissent établir une connexion et transmettre des informations sécurisées. Elle sécurise également ce trafic en chiffrant les données transmises entre les ordinateurs. Le Pare-feu Windows avec fonctions avancées de sécurité utilise la sécurité IPsec pour mettre en œuvre ces règles.



Les règles de sécurité de connexion configurables sont les suivantes :

- Isolation. Une règle d'isolement isole des ordinateurs en limitant les connexions basées sur des informations d'identification, telles que l'appartenance à un domaine ou l'état d'intégrité. Les règles d'isolement vous permettent d'implémenter une stratégie d'isolement pour des serveurs ou des domaines.
- Exemption d'authentification. Vous pouvez utiliser une exemption d'authentification pour désigner des connexions qui ne nécessitent pas d'authentification. Vous pouvez désigner des ordinateurs en spécifiant une adresse IP spécifique, une plage d'adresses IP, un sous-réseau ou un groupe prédéfini tel qu'une passerelle.
- Serveur à serveur. Une règle de serveur à serveur protège les connexions entre des ordinateurs spécifiques. Ce type de règle protège habituellement les connexions entre serveurs. Lorsque vous créez la règle, spécifiez les points de terminaison du réseau entre lesquels les communications sont protégées. Désignez ensuite les conditions requises et l'authentification à utiliser.
- *Tunnel*. Une règle de tunnel vous permet de protéger les connexions entre des ordinateurs de passerelle. En général, vous pouvez utiliser une règle de tunnel lorsque vous vous connectez via Internet entre deux passerelles de sécurité.
- Personnalisée. Utilisez une règle personnalisée pour authentifier les connexions entre deux points de terminaison lorsque vous ne pouvez pas définir les règles d'authentification dont vous avez besoin à l'aide des autres règles disponibles dans l'Assistant Nouvelle règle de sécurité de connexion.

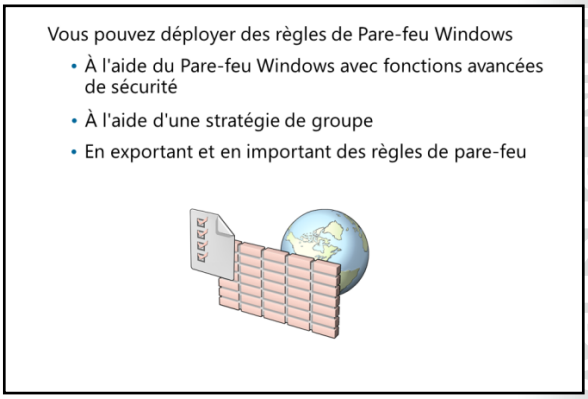
Interactions entre les règles de pare-feu et les règles de sécurité de connexion

Les règles de pare-feu autorisent le trafic à traverser le pare-feu, mais ne sécurisent pas ce trafic. Pour sécuriser le trafic avec IPsec, vous pouvez créer des règles de sécurité de connexion. Toutefois, les règles de sécurité de connexion ne permettent pas au trafic de traverser un pare-feu. Pour cela, vous devez créer une règle de pare-feu. Les règles de sécurité de connexion ne s'appliquent pas aux programmes et aux services, mais plutôt entre les ordinateurs qui constituent les deux points de terminaison.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Déploiement des règles de pare-feu

La manière dont vous déployez les règles de Pare-feu Windows est une considération importante. Le choix de la méthode appropriée garantit un déploiement précis et à moindre effort des règles. Vous pouvez déployer les règles de Pare-feu Windows selon les méthodes suivantes :



- Manuellement. Vous pouvez configurer individuellement les règles de pare-feu sur chaque serveur. Toutefois, dans un environnement comportant un nombre important de serveurs, il s'agit d'une tâche intensive et sujette aux erreurs. Cette méthode est généralement utilisée uniquement à des fins de test et de dépannage.
- Utilisation d'une stratégie de groupe. La méthode privilégiée pour distribuer les règles de pare-feu consiste à utiliser une stratégie de groupe. Après avoir créé et testé un objet de stratégie de groupe avec les règles de pare-feu requises, vous pouvez déployer ces règles de pare-feu avec rapidité et précision sur un grand nombre d'ordinateurs.
- Exportation et importation des règles de pare-feu. Le Pare-feu Windows avec fonctions avancées de sécurité offre également l'option d'importer et d'exporter les règles de pare-feu. Vous pouvez exporter les règles de pare-feu pour créer une sauvegarde avant de configurer manuellement les règles de pare-feu pendant le dépannage.

Remarque : Lorsque vous importez des règles de pare-feu, elles sont traitées comme un ensemble complet et remplacent toutes les règles de pare-feu actuellement configurées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Configuration d'AppLocker et du Pare-feu Windows

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, en Angleterre. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8.

Vous avez travaillé pour A. Datum pendant plusieurs années en tant que spécialiste du support technique. Votre fonction consistait à examiner les ordinateurs de bureau pour résoudre les problèmes d'application et les problèmes réseau. Vous avez récemment accepté une promotion au sein de l'équipe d'assistance technique des serveurs. En tant que nouveau membre de l'équipe, votre rôle consiste à aider à déployer et configurer de nouveaux serveurs et services dans l'infrastructure existante, conformément aux instructions fournies par votre responsable informatique.

Votre responsable vous a chargé d'implémenter AppLocker pour empêcher l'exécution d'applications non standard. Il vous a également demandé de créer de nouvelles règles de Pare-feu Windows pour tous les serveurs membres qui exécutent des applications Web.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer des stratégies AppLocker ;
- configurer le Pare-feu Windows.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22410B-LON-DC1 22410B-LON-SVR1 22410B-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 **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22410B-LON-DC1**, puis, dans le volet Actions, cliquez sur **Se connecter**.
3. Si nécessaire, connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
4. Répétez les étapes 2 à 4 pour **22410B-LON-SVR1** et **22410B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration des stratégies AppLocker

Scénario

Votre responsable vous a chargé de configurer de nouvelles stratégies AppLocker pour contrôler l'utilisation des applications sur les postes de travail des utilisateurs. La nouvelle configuration doit autoriser l'exécution des programmes uniquement à partir d'emplacements approuvés. Tous les utilisateurs doivent être en mesure d'exécuter les applications à partir des répertoires C:\Windows et C:\Program Files.

Vous devez également ajouter une exception pour exécuter une application personnalisée qui réside dans un emplacement non standard. La première phase de l'implémentation consignera la conformité aux règles. La seconde phase de l'implémentation empêchera l'exécution des programmes non autorisés.

Les tâches principales de cet exercice sont les suivantes :

1. Créer une unité d'organisation pour les ordinateurs clients
2. Placer LON-CL1 dans l'unité d'organisation Ordinateurs clients
3. Créer un objet GPO de contrôle de logiciels et le lier à l'unité d'organisation Ordinateurs clients
4. Exécuter GPUpdate
5. Exécuter app1.bat dans le dossier C:\CustomApp
6. Afficher les événements AppLocker® dans un journal des événements
7. Créer une règle qui autorise l'exécution des logiciels figurant dans un emplacement spécifique
8. Modifier l'objet GPO Contrôle de logiciels pour appliquer des règles
9. Vérifier qu'une application peut encore être exécutée
10. Vérifier qu'une application ne peut pas être exécutée

▶ Tâche 1 : Créer une unité d'organisation pour les ordinateurs clients

1. Basculez vers **LON-DC1**.
2. Ouvrez **Utilisateurs et ordinateurs Active Directory**.
3. Créez une nouvelle unité d'organisation appelée **Unité d'organisation Ordinateurs clients**.

▶ Tâche 2 : Placer LON-CL1 dans l'unité d'organisation Ordinateurs clients

- Sur LON-DC1, dans la console Utilisateurs et ordinateurs Active Directory, placez **LON-CL1** dans **Unité d'organisation Ordinateurs clients**.

▶ Tâche 3 : Créer un objet GPO de contrôle de logiciels et le lier à l'unité d'organisation Ordinateurs clients

1. Sur LON-DC1, ouvrez la console **GPMC**.
2. Dans la console GPMC, dans le conteneur **Objets de stratégie de groupe**, créez un nouvel objet de stratégie de groupe nommé **Objet GPO Contrôle de logiciels**.
3. Modifiez l'objet GPO Contrôle de logiciels.
4. Dans la fenêtre de l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/Stratégies de contrôle de l'application/AppLocker**.

5. Créez les règles par défaut pour les éléments suivants :
   - **Règles de l'exécutable**
   - **Règles Windows Installer**
   - **Règles de script**
   - **Règles d'applications empaquetées**
6. Configurez l'application des règles avec l'option **Auditer uniquement** pour les éléments suivants :
   - **Règles de l'exécutable**
   - **Règles Windows Installer**
   - **Règles de script**
   - **Règles d'applications empaquetées**
7. Dans l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\ Paramètres Windows\Paramètres de sécurité**, cliquez sur **Services système**, puis double-cliquez sur **Identité de l'application**.
8. Dans la boîte de dialogue **Propriétés de : Identité de l'application**, cliquez sur **Définir ce paramètre de stratégie** et, sous **Sélectionnez le mode de démarrage du service**, cliquez sur **Automatique**, puis cliquez sur **OK**.
9. Fermez l'Éditeur de gestion des stratégies de groupe.
10. Dans la console GPMC, liez **Objet GPO Contrôle de logiciels** à **Unité d'organisation Ordinateurs clients**.

▶ Tâche 4 : Exécuter GPUpdate

1. Basculez vers **LON-CL1**.
2. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante :

```
gpupdate /force
```

3. Fermez la fenêtre d'invite de commandes et redémarrez **LON-CL1**.

▶ Tâche 5 : Exécuter app1.bat dans le dossier C:\CustomApp

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpresult /R
```

   Examinez le résultat de la commande et vérifiez que **Objet GPO Contrôle de logiciels** est affiché sous Paramètres de l'ordinateur, Objets Stratégie de groupe appliqués. Si **Objet GPO Contrôle de logiciels** n'est pas affiché, redémarrez LON-CL1 et répétez les étapes 1 et 2.

3. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
C:\CustomApp\app1.bat
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 6 : Afficher les événements AppLocker® dans un journal des événements

1. Sur LON-CL1, démarrez l'**observateur d'événements**.
2. Dans la fenêtre de l'**observateur d'événements**, accédez à **Journaux des applications et des services/Microsoft/Windows/AppLocker**, puis passez en revue les événements.
3. Cliquez sur **Script** et examinez le journal des événements 8005 qui contient le texte suivant : **L'exécution de %OSDRIVE%\CUSTOMAPP\APP1.BAT a été autorisée**.

Remarque : Si aucun événement ne s'affiche, assurez-vous que le service Identité de l'application a démarré et réessayez.

▶ Tâche 7 : Créer une règle qui autorise l'exécution des logiciels figurant dans un emplacement spécifique

1. Sur LON-DC1, modifiez l'objet GPO Contrôle de logiciels.
2. Accédez à l'emplacement de paramétrage suivant : **Configuration ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/Stratégies de contrôle de l'application/AppLocker**.
3. Créez une nouvelle règle de script avec la configuration suivante :
   - Autorisations : **Autoriser**
   - Conditions : **Chemin d'accès**
   - Chemin d'accès : **%OSDRIVE%\CustomApp\app1.bat**
   - Nom et description : **Règle d'application personnalisée**

▶ Tâche 8 : Modifier l'objet GPO Contrôle de logiciels pour appliquer des règles

1. Utilisez l'option **Appliquer les règles** pour configurer la mise en application des règles suivantes :
   - **Règles de l'exécutable**
   - **Règles Windows Installer**
   - **Règles de script**
   - **Règles d'applications empaquetées**
2. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 9 : Vérifier qu'une application peut encore être exécutée

1. Basculez vers **LON-CL1**.
2. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante :

```
gpupdate /force
```

3. Fermez la fenêtre d'invite de commandes et redémarrez **LON-CL1**.
4. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Tony** avec le mot de passe **Pa$$w0rd**.
5. Ouvrez une invite de commandes et vérifiez que vous pouvez exécuter l'application **app1.bat**, qui figure dans le dossier **C:\CustomApp**.

▶ Tâche 10 : Vérifier qu'une application ne peut pas être exécutée

1. Sur LON-CL1, à partir du dossier **CustomApp**, copiez **app1.bat** dans le dossier **Documents**.
2. Vérifiez que l'application ne peut pas être exécutée à partir du dossier **Documents** et que le message suivant apparaît : « **Ce programme est bloqué par une stratégie de groupe. Pour plus d'informations, contactez votre administrateur système.** »

Résultats : À la fin de cet exercice, vous devrez avoir configuré des stratégies AppLocker pour tous les utilisateurs dont les comptes d'ordinateur sont situés dans l'unité d'organisation des ordinateurs clients. Les stratégies que vous avez configurées doivent autoriser ces utilisateurs à exécuter les applications figurant dans les dossiers C:\Windows et C:\Program Files, et à exécuter l'application personnalisée app1.bat dans le dossier C:\CustomApp.

Exercice 2 : Configuration du Pare-feu Windows

Scénario

Votre responsable vous a chargé de configurer les règles du Pare-feu Windows pour un ensemble de nouveaux serveurs d'applications. Ces serveurs d'applications ont une application Web à l'écoute sur un port non standard. Vous devez configurer le Pare-feu Windows pour autoriser la communication réseau via ce port. Vous utiliserez un filtrage de sécurité pour garantir que les nouvelles règles du Pare-feu Windows s'appliquent uniquement aux serveurs d'applications.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un groupe nommé Serveurs d'applications
2. Ajouter LON-SVR1 en tant que membre du groupe
3. Créer un nouvel objet GPO Serveurs d'applications
4. Lier l'objet GPO Serveurs d'applications à l'unité d'organisation Serveurs membres
5. Utiliser le filtrage de sécurité pour limiter l'objet GPO Serveurs d'applications aux membres du groupe Serveurs d'applications
6. Exécuter GPUpdate sur LON-SVR1
7. Afficher les règles de pare-feu sur LON-SVR1

▶ Tâche 1 : Créer un groupe nommé Serveurs d'applications

- Sur LON-DC1, dans Utilisateurs et ordinateurs Active Directory, dans l'**unité d'organisation Serveurs membres**, créez un nouveau groupe de sécurité global nommé **Serveurs d'applications**.

▶ Tâche 2 : Ajouter LON-SVR1 en tant que membre du groupe

- Dans la console Utilisateurs et ordinateurs Active Directory, dans l'unité d'organisation Serveurs membres, ouvrez **Propriétés de : Serveurs d'applications**, puis ajoutez **LON-SVR1** en tant que membre du groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Créer un nouvel objet GPO Serveurs d'applications

1. Sur LON-DC1, ouvrez la console **GPMC**.
2. Dans la console GPMC, dans le conteneur **Objets de stratégie de groupe**, créez un nouvel objet GPO nommé **Objet GPO Serveurs d'applications**.
3. Dans la fenêtre de l'Éditeur de gestion des stratégies de groupe, accédez 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 - LDAP://CN={GUID}**.
4. Configurez une règle de trafic entrant avec les paramètres suivants :
   - Type de règle : **Personnalisée**
   - Type de protocole : **TCP**
   - Ports spécifiques : **8080**
   - Étendue : **Toute adresse IP**
   - Action : **Autoriser la connexion**
   - Profil **: Domaine** (désactivez les deux cases à cocher **Privé** et **Public**)
   - Nom : **Règle de pare-feu de service de serveur d'applications**
5. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 4 : Lier l'objet GPO Serveurs d'applications à l'unité d'organisation Serveurs membres

- Dans la console GPMC, liez l'**objet GPO Serveurs d'applications** à l'**unité d'organisation Serveurs membres**.

▶ Tâche 5 : Utiliser le filtrage de sécurité pour limiter l'objet GPO Serveurs d'applications aux membres du groupe Serveurs d'applications

1. Sur LON-DC1, ouvrez la console **GPMC**.
2. Développez **Unité d'organisation Serveurs membres**, puis cliquez sur **Objet GPO Serveurs d'applications**.
3. Dans le volet de droite, sous Filtrage de sécurité, supprimez **Utilisateurs authentifiés** et configurez l'**objet GPO Serveurs d'applications** pour qu'il s'applique uniquement au groupe de sécurité **Serveurs d'applications**.

▶ Tâche 6 : Exécuter GPUpdate sur LON-SVR1

1. Basculez vers **LON-SVR1**.
2. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante :

```
gpupdate /force
```

3. Fermez la fenêtre d'invite de commandes.
4. Redémarrez **LON-SVR1**, puis connectez-vous à nouveau en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 7 : Afficher les règles de pare-feu sur LON-SVR1

1. Basculez vers **LON-SVR1**.
2. Démarrez le **Pare-feu Windows avec fonctions avancées de sécurité**.
3. Dans la fenêtre du Pare-feu Windows avec fonctions avancées de sécurité, dans **Règles de trafic entrant**, vérifiez que la **règle de pare-feu de service de serveur d'applications** que vous avez créée auparavant à l'aide d'une stratégie de groupe est configurée.
4. Vérifiez que vous ne pouvez pas modifier la **règle de pare-feu de service de serveur d'applications**, car elle est configurée via une stratégie de groupe.

Résultats : À la fin de cet exercice, vous devrez avoir utilisé une stratégie de groupe pour configurer le Pare-feu Windows avec fonctions avancées de sécurité afin de créer des règles pour les serveurs d'applications.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-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 22410B-LON-SVR1 et 22410B-LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Le modèle de défense en profondeur prescrit-il des technologies spécifiques à utiliser pour protéger les serveurs dotés de systèmes d'exploitation Windows Server ?

Question : Quel paramètre devez-vous configurer pour garantir que seules trois tentatives de connexion non valides sont autorisées pour les utilisateurs ?

Question : <Ajoutez une question de discussion ici>

Question : Vous créez un objet de stratégie de groupe avec des règles standardisées de pare-feu pour les serveurs dans votre organisation. Vous avez testé ces règles sur un serveur autonome dans votre environnement de test. Les règles apparaissent sur les serveurs après l'application de l'objet GPO, mais elles ne prennent pas effet. Quelle est la cause la plus probable de ce problème ?

Question : L'année dernière, votre organisation a développé une stratégie de sécurité qui incluait tous les aspects d'un modèle de défense en profondeur. S'appuyant sur cette stratégie, votre organisation a implémenté des stratégies et des paramètres de sécurité sur l'environnement complet de l'infrastructure informatique. Hier, vous avez lu dans un article que de nouvelles menaces contre la sécurité ont été détectées sur Internet, mais maintenant vous vous rendez compte que la stratégie de votre société n'inclut pas de plan d'analyse et d'atténuation des risques pour ces nouvelles menaces. Que devez-vous faire ?

Outils

Outil	Utilisation	Emplacement
Console de gestion des stratégies de groupe	Outil graphique servant à créer, modifier et appliquer des objets GPO	Gestionnaire de serveur/Outils
AppLocker	Applique des paramètres de sécurité contrôlant quelles applications les utilisateurs sont autorisés à exécuter	Éditeur d'objets de stratégie de groupe dans la console GPMC
Pare-feu Windows avec fonctions avancées de sécurité	Pare-feu basé sur l'hôte inclus en tant que fonctionnalité dans Windows Server 2012 et Windows Server 2008	Gestionnaire de serveur/Outils s'il est configuré individuellement ou Éditeur d'objets de stratégie de groupe dans la console GPMC pour un déploiement à l'aide d'une stratégie de groupe
Responsable de la conformité de sécurité	Déploiement de stratégies de sécurité conformément aux recommandations du Guide de la sécurité Microsoft et aux meilleures pratiques de l'industrie	À télécharger à partir du site Web de Microsoft, à l'adresse http://go.microsoft.com/fwlink/?LinkID=266746.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Méthode conseillée

Voici les meilleures pratiques recommandées :

- Effectuez toujours une évaluation détaillée des risques de sécurité avant de planifier les fonctionnalités de sécurité que votre organisation doit déployer.
- Créez un objet de stratégie de groupe distinct pour les paramètres de sécurité qui s'appliquent à un type différent d'utilisateurs dans votre organisation, car chaque service peut avoir des besoins de sécurité différents.
- Assurez-vous que les paramètres de sécurité que vous configurez sont raisonnablement faciles à utiliser afin que les employés les acceptent. Fréquemment, des stratégies de sécurité très fortes sont trop complexes ou difficiles pour que les employés les adoptent.
- Testez toujours les configurations de sécurité que vous envisagez d'implémenter à l'aide d'un objet de stratégie de groupe dans un environnement isolé, non destiné à la production. Une fois seulement que vous avez réussi ces tests, vous pouvez déployer les stratégies dans votre environnement de production.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
L'utilisateur ne peut pas se connecter localement à un serveur.	
Après la configuration de l'audit, trop d'événements sont consignés dans le journal des événements de sécurité de l'observateur d'événements.	
Certains utilisateurs se plaignent que leurs applications métier ne peuvent plus accéder à des ressources sur le serveur.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 13

Implémentation de la virtualisation de serveur avec Hyper-V

Table des matières :

Vue d'ensemble du module	**13-1**
Leçon 1 : Vue d'ensemble des technologies de virtualisation	**13-2**
Leçon 2 : Implémentation d'Hyper-V	**13-9**
Leçon 3 : Gestion du stockage d'ordinateur virtuel	**13-17**
Leçon 4 : Gestion des réseaux virtuels	**13-25**
Atelier pratique : Implémentation de la virtualisation de serveur avec Hyper-V	**13-30**
Contrôle des acquis et éléments à retenir	**13-37**

Vue d'ensemble du module

La virtualisation de serveur est un élément du système d'exploitation Windows Server® depuis la version de Windows Server 2008 et l'introduction du rôle Hyper-V®. Avec la virtualisation de serveur, votre organisation peut faire des économies grâce à la consolidation de serveurs. Cependant, pour utiliser la virtualisation de serveur de manière plus efficace, les administrateurs de serveurs doivent pouvoir déterminer les charges de serveur qui s'exécuteront effectivement sur les ordinateurs virtuels, et les charges de travail de serveur qui doivent demeurer déployées dans un environnement de serveur plus traditionnel.

Ce module décrit le rôle Hyper-V dans Windows Server 2012, les composants du rôle, comment mieux déployer le rôle, et les nouvelles fonctionnalités du rôle de Hyper-V qui sont présentées avec Windows Server 2012.

Objectifs

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

- décrire les technologies de virtualisation ;
- implémenter Hyper-V ;
- gérer le stockage d'ordinateur virtuel ;
- gérer les réseaux virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble des technologies de virtualisation

Vous pouvez déployer de nombreux types de technologies de virtualisation différents au sein de réseaux où des systèmes d'exploitation Windows® sont déployés. Les types de technologies de virtualisation que vous sélectionnez sont fonction des objectifs de votre organisation. Bien que ce module soit principalement axé sur la virtualisation de serveur, dans cette leçon vous allez découvrir d'autres types de technologies de virtualisation, ainsi que les situations dans lesquelles il convient de les déployer.

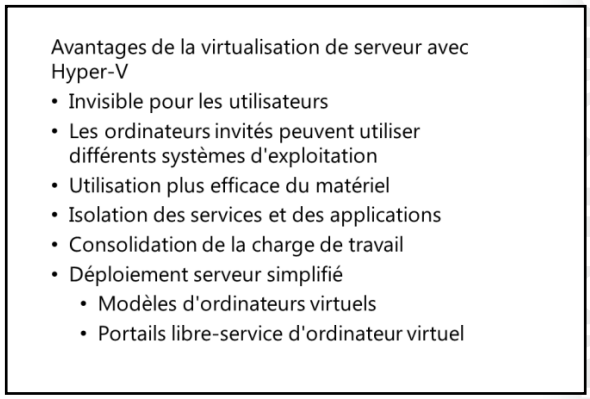
Objectifs de la leçon

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

- décrire la virtualisation de serveur avec Hyper-V ;
- décrire Windows Azure™ ;
- expliquer quand vous devez utiliser la virtualisation de bureau ;
- déterminer les composants requis pour implémenter la virtualisation de présentation ;
- expliquer les avantages de la virtualisation d'application Microsoft par comparaison au déploiement d'applications traditionnel.

Virtualisation de serveur avec Hyper-V

Avec la virtualisation de serveur, vous pouvez créer des ordinateurs virtuels distincts et les exécuter simultanément sur un serveur unique qui exécute Hyper-V. Ces ordinateurs virtuels sont appelés *invités*. L'ordinateur qui exécute Hyper-V est appelé *serveur de virtualisation* ou *système d'exploitation de gestion*.



Les ordinateurs physiques virtuels fonctionnent comme des ordinateurs normaux. Lorsque les utilisateurs se connectent sur un ordinateur virtuel invité via une connexion de Bureau à distance ou une session à distance Windows PowerShell®, vous devez soigneusement examiner les propriétés de l'ordinateur sur lequel l'utilisateur travaille afin de déterminer s'il s'agit d'un ordinateur virtuel ou d'une machine physique déployée de manière traditionnelle. Les ordinateurs virtuels qui sont hébergés sur le même serveur de virtualisation sont indépendant les uns des autres. Vous pouvez exécuter plusieurs ordinateurs virtuels qui utilisent différents systèmes d'exploitation sur un serveur de virtualisation de manière simultanée, à condition que le serveur de virtualisation dispose de suffisamment de ressources.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Utilisation des ordinateurs virtuels et du matériel

Implémenter des ordinateurs virtuels vous permet d'utiliser le matériel de manière plus efficace. Dans la plupart des cas, un service ou une application ne consomme qu'une faible fraction des ressources d'un serveur de virtualisation. Cela signifie que vous pouvez installer plusieurs services et applications sur le même serveur de virtualisation puis les déployer sur plusieurs ordinateurs virtuels. Cela garantit une utilisation plus efficace des ressources de ce serveur de virtualisation. Par exemple, supposez que vous disposiez de quatre services et applications distincts, chacun consommant 10 à 15 pour cent des ressources matérielles d'un serveur de virtualisation. Vous pouvez installer ces services et applications sur des ordinateurs virtuels, puis les placer sur le même matériel où, en moyenne, ils consomment au total 40 à 60 pour cent du matériel du serveur de virtualisation.

Il s'agit là d'un exemple simplifié. Dans les environnements réels, vous devez procéder à des préparations adéquates avant d'installer des ordinateurs virtuels. Vous devez vous assurer que les besoins en ressources matérielles de tous les ordinateurs virtuels qui sont hébergés sur le serveur de virtualisation n'excèdent pas les ressources matérielles du serveur.

Isolation des services et des applications sur les ordinateurs virtuels

Maintenir la fiabilité d'un service ou d'une application particuliers peut constituer un réel défi et cela devient encore plus compliqué lorsque vous déployez plusieurs services et applications sur le même serveur. Par exemple, vous devrez peut-être déployer deux systèmes d'exploitation distincts au sein d'une filiale, mais ces systèmes d'exploitation seront en conflit s'ils s'exécutent sur le même ordinateur. Si vous ne pouvez disposer que d'un seul serveur, vous pouvez résoudre ce problème en exécutant ces applications au sein d'ordinateurs virtuels sur le même serveur.

Consolidation de serveurs

Avec la virtualisation de serveur, vous pouvez consolider des serveurs qui devraient autrement s'exécuter sur du matériel distinct sur un serveur de virtualisation unique. Étant donné que chaque ordinateur virtuel sur un serveur de virtualisation est isolé des autres ordinateurs virtuels sur le même serveur, il est possible de déployer des services et des applications qui sont incompatibles entre eux sur le même ordinateur physique, à condition que vous les hébergiez sur des ordinateurs virtuels. Microsoft Exchange Server® 2010, SQL Server® 2012 et les services de domaines Active Directory® sont des exemples de ces services et applications. Cela signifie qu'une organisation doit seulement déployer un serveur physique au lieu des trois serveurs qui auraient été nécessaires par le passé.

Méthode conseillée : Nous vous recommandons de ne pas déployer un serveur de boîte aux lettres Microsoft Exchange sur un ordinateur qui contient un rôle de contrôleur de domaine. Nous vous recommandons également de ne pas déployer une instance de moteur de base de données SQL Server 2012 sur un ordinateur qui contient le rôle de contrôleur de domaine. Déployez plutôt chacune de ces charges de travail sur des ordinateurs virtuels distincts puis exécutez ces derniers en tant qu'invités sur le même serveur de virtualisation; cette configuration est prise en charge.

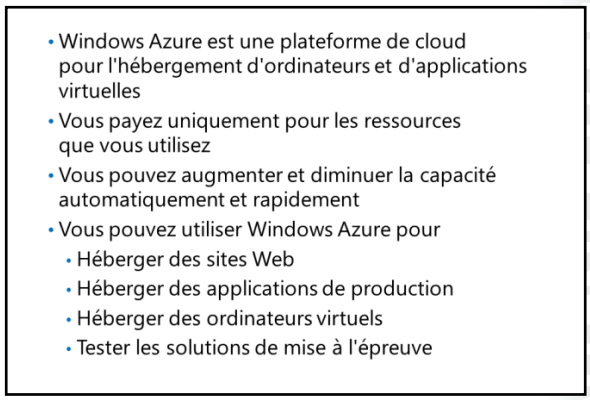
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Simplification du déploiement de serveur

Vous pouvez également utiliser la virtualisation pour simplifier le processus du déploiement de serveur :

- Des modèles d'ordinateur virtuel pour des configurations de serveur courantes sont fournis avec des produits tels que Microsoft System Center 2012 - Virtual Machine Manager (VMM). Dans ces modèles, nombre de paramètres sont préconfigurés à l'aide de valeurs courantes de sorte que vous n'avez pas à configurer chaque paramètre vous-même.
- Vous pouvez également créer des portails libre-service d'ordinateurs virtuels qui permettent aux utilisateurs finaux de configurer automatiquement des serveurs et des applications approuvés. Cela réduit la charge de travail de l'équipe d'administration de systèmes. Pour créer ces portails libre-service d'ordinateurs virtuels, vous utilisez VMM et Microsoft System Center 2012 - Service Manager.

Qu'est-ce que Windows Azure ?



Windows Azure est une plateforme en cloud sur laquelle vous pouvez acheter de la capacité, pour des ordinateurs virtuels, pour des applications, ou encore pour des services tels que des bases de données SQL Server sur SQL Azure™. L'un des avantages que présente l'utilisation de Windows Azure est que vous payez seulement la capacité que vous utilisez au lieu de payer un taux fixe. Par exemple, au lieu de payer un taux forfaitaire mensuel pour louer un serveur en armoire à un fournisseur d'hébergement, vous payez moins lorsque le serveur est moins occupé et vous payez plus lorsque le serveur devient plus occupé.

La capacité en cloud est élastique, ce qui signifie qu'elle peut se développer ou se réduire rapidement en fonction des besoins. Par exemple, dans une solution hébergée de manière traditionnelle, vous pouvez choisir un châssis spécifique de serveur, mais si ensuite vos besoins augmentent en termes de capacité ou de performances, vous devez basculer vers un matériel de serveur de classe supérieure. Tout cela demande du temps et de la planification. De même, si vos besoins en termes de capacité ou de performances diminuent, vous devez déterminer si la migration vers une classe de matériel inférieure vaut le coût, ou si votre organisation doit continuer à payer une classe de matériel dont vous n'avez maintenant plus besoin, et dont vous n'aurez peut-être plus besoin à l'avenir. Avec un fournisseur d'hébergement, la capacité est ajustée automatiquement et vous n'avez pas à dépenser du temps ou de l'argent à passer d'un serveur à l'autre.

Les ordinateurs virtuels, les applications et les services en cloud peuvent être utiles lorsque vous devez fournir des solutions de mise à l'épreuve pour les projets proposés. Au lieu d'acheter du matériel de test puis d'y déployer une solution de mise à l'épreuve, vous pouvez déployer rapidement un ordinateur virtuel en cloud, puis y déployer la solution de mise à l'épreuve. Ensuite, une fois la solution de mise à l'épreuve validée, vous pouvez ignorer l'ordinateur virtuel (ou le conserver), en fonction des besoins de votre entreprise. En plus d'être plus rapide, cette solution est moins onéreuse que l'achat de matériel pour la solution de mise à l'épreuve, et vous pouvez choisir de l'ignorer si le projet n'est pas approuvé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Hébergement de sites Web ou d'applications de production

Sur les plateformes en cloud telles que Windows Azure, vous pouvez déployer des applications sans avoir à déployer l'infrastructure de serveur sous-jacente. Par exemple, si vous avez besoin d'une base de données, au lieu de déployer à la fois Windows Server 2012 et SQL Server 2012, puis de déployer la base de données spécifique, vous pouvez louer le serveur de base de données en cloud et y héberger la base de données.

Pour une stratégie en cloud réussie, vous devez déterminer les services et les applications qu'il est plus économique de déployer sur une plateforme en cloud et les services et applications qu'il est plus économique de déployer dans un environnement de serveur plus traditionnel sur votre site. Beaucoup de facteurs propres à votre organisation entrent en jeu dans cette décision, et une stratégie qui peut être la meilleure pour une organisation peut ne pas être appropriée pour une autre.

Virtualisation de bureau

La virtualisation de bureau inclut les technologies suivantes

- Hyper-V client (local)
- VDI

Hyper-V client

Vous pouvez installer le rôle Hyper-V sur des ordinateurs qui exécutent les systèmes d'exploitation Windows 8 Pro et Windows 8 Entreprise. Cela vous permet d'exécuter des ordinateurs virtuels invités sur des ordinateurs clients. Avec Hyper-V client, fonctionnalité Hyper-V dans les systèmes d'exploitation Windows 8 Pro et Windows 8 Entreprise, la configuration processeur requise est légèrement différente de celle de Hyper-V sur Windows Server 2012. Plus précisément, avec les systèmes d'exploitation clients Windows 8, l'ordinateur doit disposer d'une plateforme x64 qui prenne en charge la traduction d'adresse de second niveau (SLAT), et au moins 4 gigaoctets (Go) de mémoire vive (RAM). Ce n'est pas le cas de Hyper-V sur Windows Server 2012 qui ne requiert pas la traduction d'adresse de second niveau (SLAT).

Hyper-V client sur Windows 8

Le rôle Hyper-V client sur Windows 8 prend en charge de nombreuses fonctionnalités qui sont disponibles avec Hyper-V sur Windows Server 2012, mais il ne prend pas en charge des fonctionnalités Windows Server 2012 telles que la migration d'ordinateurs virtuels. Hyper-V client ne prend pas non plus en charge la publication des applications qui sont installées sur l'ordinateur virtuel invité dans le menu **Démarrer** du système d'exploitation de gestion. Il s'agissait d'une fonctionnalité du mode XP sur Windows 7, qui utilise Windows Virtual PC. (Windows Virtual PC est la fonctionnalité de virtualisation de client disponible sur certains ordinateurs exécutant des éditions spécifiques de Windows 7.)

Hyper-V client dans les environnements d'entreprise

Dans les environnements d'entreprise, Hyper-V client est souvent utilisé à des fins de développement, ou pour permettre à des utilisateurs spécifiques d'exécuter des versions précédentes du système d'exploitation Windows, ce qui leur permet d'accéder à des applications qui sont incompatibles avec Windows 8.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Infrastructure VDI (Microsoft Virtual Desktop Infrastructure)

Dans l'infrastructure VDI, les systèmes exploitation sont hébergés de manière centralisée en tant qu'ordinateurs virtuels et les clients se connectent à ces ordinateurs virtuels au moyen de logiciels clients tel que RDC. Vous pouvez configurer un serveur pour la prise en charge de VDI en sélectionnant une installation des Services Bureau à distance (RDS) dans l'Assistant Ajout de rôles et de fonctionnalités. Lorsque vous configurez un serveur de virtualisation pour qu'il fonctionne en tant que serveur VDI, vous pouvez installer la fonctionnalité Hôte de virtualisation des services Bureau à distance en plus du rôle Hyper-V.

L'infrastructure VDI peut simplifier la gestion des systèmes d'exploitation clients car :

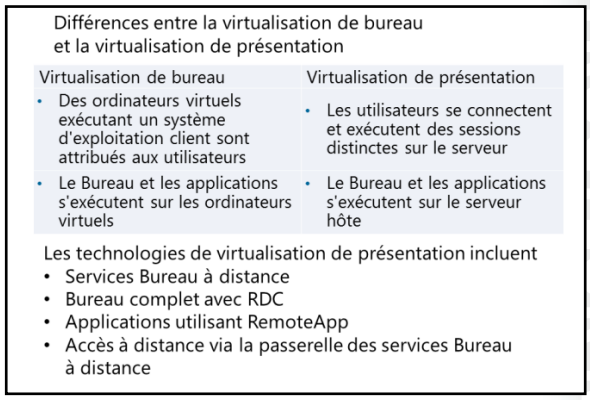
- elle garantit que tous les ordinateurs clients qui sont hébergés sur un serveur unique sont sauvegardés régulièrement ;
- elle héberge les ordinateurs virtuels clients sur un serveur de virtualisation hautement disponible.
- en cas de défaillance d'un ordinateur client, elle s'assure que les utilisateurs peuvent encore accéder à leur ordinateur virtuel à l'aide d'autres méthodes RDC.

Vous pouvez également utiliser l'infrastructure VDI pour implémenter la stratégie Apportez vos propres terminaux (Bring Your Own Device, BYOD). Dans ce scénario, les employés apportent leur propre ordinateur au bureau et utilisent le logiciel RDC pour se connecter à l'ordinateur virtuel auquel ils sont attribués.

Virtualisation de présentation

La virtualisation de présentation diffère de la virtualisation de bureau comme suit :

- Dans la virtualisation de bureau, chaque utilisateur se voit affecter un ordinateur virtuel qui lui est propre et qui exécute un système d'exploitation client. Dans la virtualisation de présentation, les utilisateurs ouvrent et exécutent des sessions distinctes sur un ou plusieurs serveurs. Par exemple, les utilisateurs Alex et Brad pourraient être connectés simultanément au même serveur de Bureau à distance, tout en exécutant différentes sessions avec RDC.



- Avec la virtualisation de bureau, les applications s'exécutent sur des ordinateurs virtuels. Avec la virtualisation de présentation, le Bureau et les applications s'exécutent sur le serveur de virtualisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sur les réseaux qui utilisent Windows Server 2012, la virtualisation de présentation est assurée par le rôle de serveur Services Bureau à distance. Les clients peuvent accéder à la virtualisation de présentation comme suit :

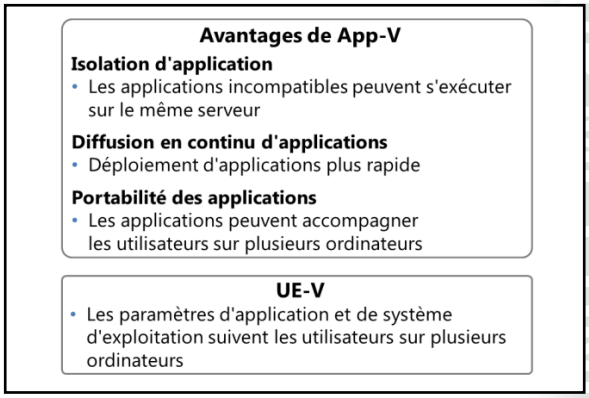
- Bureau complet. Les clients peuvent utiliser un client de Bureau à distance tel que RDC pour accéder à une session de bureau complète et exécuter des applications sur le serveur de virtualisation Windows Server 2012.
- Applications RemoteApp. Au lieu d'utiliser un client de bureau complet tel que RDC, la fonctionnalité RemoteApp de Windows Server permet aux applications qui s'exécutent sur le serveur Windows Server 2012 de s'afficher sur l'ordinateur client. Vous pouvez déployer les applications RemoteApp sous la forme de fichiers Windows Installer (.msi) à l'aide de méthodes traditionnelles de déploiement de logiciels. Cela vous permet d'associer des types de fichier aux applications RemoteApp.
- Accès au Bureau à distance par le Web. Avec l'Accès Bureau à distance par le Web, les clients peuvent accéder à un site Web sur un serveur spécialement configuré, puis lancer des applications RemoteApp et des sessions de Bureau à distance depuis leur navigateur.

Passerelle des services Bureau à distance

La Passerelle des services Bureau à distance permet aux clients externes d'accéder au Bureau à distance et à RemoteApp sans recours au réseau privé virtuel (VPN), ou à DirectAccess, fonctionnalité des systèmes d'exploitation Windows 7 et Windows 8. La Passerelle des services Bureau à distance est un service de rôle que vous pouvez installer sur un ordinateur exécutant Windows Server 2012. Vous déployez les serveurs de Passerelle des services Bureau à distance sur les réseaux de périmètre. Vous configurez ensuite le client RDC avec l'adresse des serveurs Passerelle des services Bureau à distance. Lorsque vous faites cela, le client vérifie si le serveur Bureau à distance cible est au sein du réseau organisationnel. Si le serveur Bureau à distance est sur le réseau, le client établit une connexion directe à celui-ci. Si le serveur Bureau à distance n'est pas sur le réseau, le client route la connexion vers ce dernier via le serveur de passerelle Bureau à distance.

Qu'est-ce que Microsoft Application Virtualization ?

Avec la virtualisation d'application, les applications ne sont pas installées de manière définitive sur les ordinateurs clients mais elles sont déployées à partir d'un serveur pour les clients lorsque des utilisateurs finaux souhaitent utiliser l'application. Microsoft Application Virtualization (App-V) utilise Microsoft Application Virtualization Desktop Client (installé sur le client). App-V est disponible en tant que composant de Microsoft Desktop Optimization Pack, et il ne s'agit pas d'un rôle ou d'une fonctionnalité Windows Server 2012 native.



Fonctionnalités et avantages de App-V

App-V présente trois avantages : isolation d'application, diffusion en continu d'applications et portabilité des applications.

Isolation d'application

App-V isole l'application du système d'exploitation et l'exécute dans un environnement virtuel distinct. App-V isole aussi les applications des autres applications exécutées sur le même ordinateur. Cela signifie que vous pouvez exécuter des applications qui peuvent être incompatibles lorsqu'elles sont exécutées ensemble sur le même ordinateur. Par exemple, vous pouvez utiliser App-V pour déployer et exécuter différentes versions de Microsoft Office simultanément.

Diffusion en continu d'applications

La diffusion en continu d'applications est une autre fonctionnalité utile d'App-V. Lorsqu'une application est diffusée en continu, seuls les composants en cours d'utilisation de cette application sont transmis à l'ordinateur client. Ceci accélère le déploiement d'applications car une seule partie de l'application doit être transmise via le réseau à l'ordinateur client.

Portabilité des applications

Lorsque App-V est déployé avec le Microsoft System Center 2012 Configuration Manager, les utilisateurs peuvent utiliser les mêmes applications sur plusieurs ordinateurs clients, sans qu'une installation traditionnelle soit nécessaire sur ces ordinateurs clients. Par exemple, un utilisateur peut se connecter à l'ordinateur d'un collègue, puis demander à App-V de diffuser une application sur cet ordinateur afin qu'il puisse l'utiliser sur ce dernier. L'application n'est pas installée en local, et lorsque l'utilisateur se déconnecte, l'application n'est plus accessible aux autres utilisateurs de cet ordinateur.

Virtualisation de l'expérience utilisateur

Tout comme App-V permet à des utilisateurs d'accéder à leurs applications à partir de différents ordinateurs clients, Microsoft User Experience Virtualization (UE-V) permet à des utilisateurs d'avoir les mêmes paramètres de système d'exploitation et d'application sur plusieurs périphériques qui exécutent Windows 7 et Windows 8. Ainsi, lorsqu'un utilisateur configure un paramètre pour une application fournie via App-V sur un ordinateur (par exemple, la configuration d'un onglet personnalisé sur un ruban dans un produit Microsoft Office), ce paramètre est disponible automatiquement lorsque cette application est fournie via App-V à un autre ordinateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Implémentation d'Hyper-V

Comprendre le fonctionnement d'Hyper-V et des ordinateurs virtuels est essentiel pour le déploiement efficace d'une virtualisation de serveur dans un environnement réseau de Windows Server 2012. Cette leçon présente Hyper-V, ainsi que les configurations matérielles requises pour le déploiement d'Hyper-V sur un ordinateur exécutant Windows Server 2012. Elle décrit également les composants d'un ordinateur virtuel (en mettant l'accent sur la mémoire dynamique), ainsi que les avantages des services d'intégration d'ordinateur virtuel. Elle explique enfin comment mesurer l'utilisation des ressources d'ordinateur virtuel avec des applets de commande Windows PowerShell.

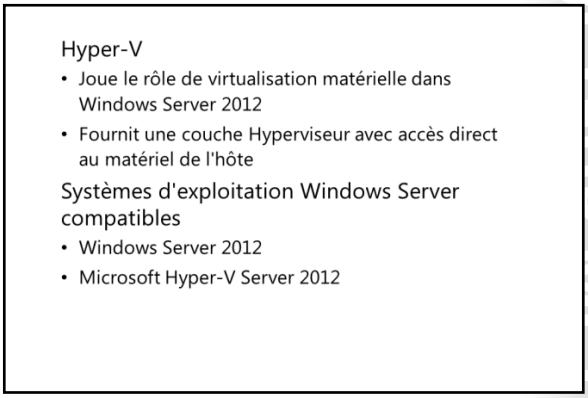
Objectifs de la leçon

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

- installer le rôle Hyper-V sur un serveur ;
- décrire le matériel approprié pour le déploiement de Hyper-V ;
- décrire les composants matériels d'un ordinateur virtuel ;
- configurer la mémoire dynamique ;
- configurer les services d'intégration d'un ordinateur virtuel ;
- configurer les actions de démarrage et d'arrêt d'un ordinateur virtuel ;
- exécuter des tâches de contrôle des ressources Hyper-V.

Qu'est-ce que Hyper-V ?

Hyper-V est le rôle de virtualisation matérielle disponible dans Windows Server 2012.
La virtualisation matérielle fournit une couche Hyperviseur qui accède directement au matériel du serveur hôte. Le système d'exploitation hôte et tous les ordinateurs virtuels exécutés sur l'hôte accèdent au matériel via la couche Hyperviseur. Ce terme s'oppose aux produits de virtualisation logicielle tels que Microsoft Virtual Server 2005 R2, qui utilisent le système d'exploitation du serveur de virtualisation pour accorder un accès indirect au matériel du serveur.



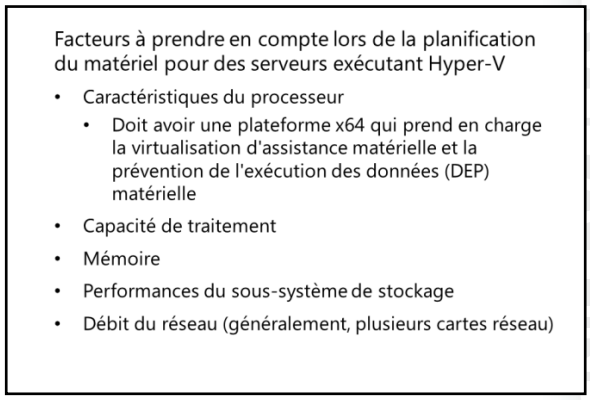
Vous pouvez déployer Hyper-V sur un ordinateur qui exécute Windows Server 2012 à l'aide de l'Assistant Ajout de rôles et de fonctionnalités. Vous pouvez configurer Windows Server 2012 en tant que serveur de virtualisation à l'aide du rôle Hyper-V. Windows Server 2012 peut ensuite héberger des ordinateurs virtuels invités qui exécutent des systèmes d'exploitation pris en charge. Vous pouvez gérer l'administration des ordinateurs virtuels en local à l'aide de Windows PowerShell, ou vous pouvez gérer cette administration à distance via la console du Gestionnaire Hyper-V.

Vous pouvez installer le rôle Hyper-V à la fois dans l'installation minimale de Windows Server 2012, et Windows Server 2012 dans la configuration minimale non serveur. Il existe également une édition Microsoft Hyper-V Server 2012 qui comprend seulement les composants nécessaires à l'hébergement des ordinateurs virtuels.

Remarque : Dans certaines documentations, le serveur de virtualisation (par exemple, l'ordinateur Windows Server 2012 qui exécute Hyper-V) est appelé *partition parente*, et un ordinateur virtuel qui s'exécute sur le serveur est appelé *partition enfant*.

Configuration matérielle requise pour Hyper-V

Le serveur sur lequel vous prévoyez d'installer le rôle Hyper-V doit présenter la configuration matérielle suivante :



- Le serveur doit avoir une plateforme x64 qui prend en charge la virtualisation d'assistance matérielle et la prévention de l'exécution des données (DEP) matérielle.
- Le serveur doit avoir une capacité de processeur suffisante pour répondre aux exigences des ordinateurs virtuels invités.

  Un ordinateur virtuel hébergé sur Hyper-V dans Windows Server 2012 peut prendre en charge jusqu'à 64 processeurs virtuels.
- Le serveur doit avoir suffisamment de mémoire pour prendre en charge l'ensemble des ordinateurs virtuels qui doivent s'exécuter simultanément, et pour exécuter le système d'exploitation Windows Server 2012 hôte.

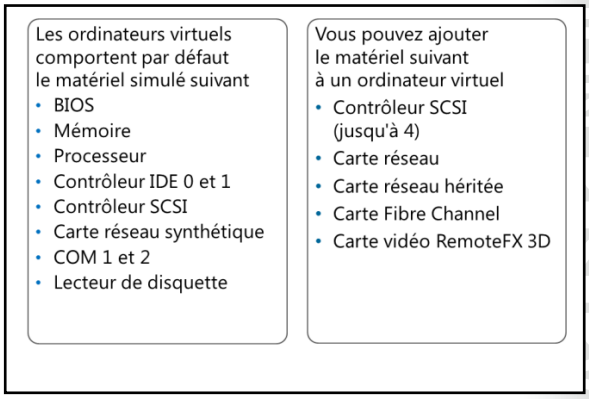
  Le serveur doit avoir au moins 4 Go de RAM.

  Un ordinateur virtuel hébergé sur Hyper-V dans Windows Server 2012 peut prendre en charge au maximum 2 téraoctets (To) de mémoire vive (RAM).
- Les performances du sous-système de stockage doivent répondre aux exigences d'entrée/sortie (E/S) des ordinateurs virtuels invités. Qu'il s'agisse d'un déploiement en local ou au sein de réseaux de stockage (SAN), vous devrez peut-être placer différents ordinateurs virtuels sur des disques physiques distincts, ou vous devrez peut-être déployer des disques RAID, des disques SSD, des disques SSD hybrides, ou une combinaison de ces trois technologies.
- Les cartes réseau du serveur de virtualisation doivent pouvoir prendre en charge le débit de réseau nécessaire aux ordinateurs virtuels invités. Vous pouvez améliorer les performances réseau en installant plusieurs cartes réseau et en utilisant plusieurs cartes d'interface réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Matériel des ordinateurs virtuels



Les ordinateurs virtuels utilisent du matériel virtuel (ou *simulé*). Le système d'exploitation de gestion, Windows Server 2012 avec Hyper-V, utilise ce matériel virtuel pour modérer l'accès au matériel réel. Par exemple, vous pouvez mapper une carte réseau virtuelle à un réseau virtuel lui-même mappé à une interface réseau réelle.

Les ordinateurs virtuels comportent par défaut le matériel simulé suivant :

- BIOS. Simule le BIOS d'un ordinateur. Sur un ordinateur autonome, vous pouvez configurer plusieurs paramètres relatifs au BIOS, et vous pouvez procéder de même sur un ordinateur virtuel. En voici quelques-uns :
  - ordre de démarrage du matériel virtuel de l'ordinateur virtuel ;
  - périphérique à partir duquel démarre l'ordinateur virtuel (par exemple, un lecteur DVD, un disque IDE, une carte réseau héritée ou un lecteur de disquette) ;
  - verrouillage numérique activé ou non au démarrage.
- Mémoire. Vous pouvez allouer jusqu'à 1 To de ressources mémoire à un ordinateur virtuel individuel.
- Processeur. Vous pouvez allouer jusqu'à 64 processeurs virtuels à un seul ordinateur virtuel.
- Contrôleur IDE 0. Un ordinateur virtuel peut uniquement prendre en charge deux contrôleurs IDE et, par défaut, deux de ces contrôleurs sont alloués à chaque ordinateur virtuel. Chaque contrôleur IDE peut prendre en charge deux périphériques.

Vous pouvez connecter des disques durs virtuels (VHD) ou des lecteurs DVD virtuels à un contrôleur IDE. Si l'ordinateur virtuel démarre à partir d'un disque VHD ou d'un lecteur DVD virtuel, le périphérique de démarrage doit être connecté à un contrôleur IDE. Vous pouvez utiliser des contrôleurs IDE pour connecter des disques VHD et des lecteurs DVD à des ordinateurs virtuels qui utilisent un système d'exploitation qui ne prend pas en charge les services d'intégration.

- Contrôleur IDE 1. Permet de déployer des disques durs virtuels et des lecteurs DVD supplémentaires sur l'ordinateur virtuel.
- Contrôleur SCSI. Vous pouvez utiliser un contrôleur SCSI uniquement sur des ordinateurs virtuels dont les systèmes d'exploitation prennent en charge les services d'intégration.
- Carte réseau synthétique. Les cartes réseau synthétiques représentent des cartes réseau d'ordinateur. Vous pouvez uniquement utiliser les cartes réseau synthétiques avec les systèmes d'exploitation pris en charge par les ordinateurs virtuels invités.
- COM 1. Permet de configurer une connexion via un canal nommé.
- COM 2. Permet de configurer une connexion supplémentaire via un canal nommé.
- Lecteur de disque. Permet de mapper une image de disquette virtuelle à un lecteur de disque virtuel.

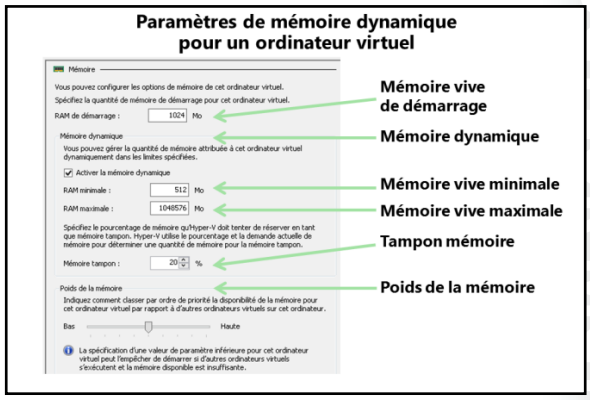
Vous pouvez ajouter le matériel suivant à un ordinateur virtuel en modifiant les propriétés de cet ordinateur virtuel puis en cliquant sur **Ajout de matériel** :

- Contrôleur SCSI. Vous pouvez ajouter jusqu'à quatre périphériques SCSI virtuels. Chaque contrôleur prend en charge jusqu'à 64 disques.
- Carte réseau. Un seul ordinateur virtuel peut avoir huit cartes réseau synthétiques au maximum.
- Carte réseau héritée. Vous pouvez utiliser les cartes réseau héritées avec tous les systèmes d'exploitation qui ne prennent pas en charge les services d'intégration. Vous pouvez également utiliser des cartes réseau héritées pour déployer des images de système d'exploitation au sein du réseau. Un seul ordinateur virtuel peut avoir jusqu'à quatre cartes réseau héritées.
- Carte Fibre Channel. Si vous ajoutez une carte Fibre Channel à un ordinateur virtuel, ce dernier peut alors se connecter directement à un réseau SAN Fibre Channel. Vous pouvez uniquement ajouter une carte Fibre Channel à un ordinateur virtuel si le serveur de virtualisation comporte un adaptateur de bus hôte (HBA) Fibre Channel (HBA) qui comporte également un pilote Windows Server 2012 prenant en charge Fibre Channel virtuel.
- Carte vidéo RemoteFX 3D. Si vous ajoutez une carte vidéo RemoteFX 3D à un ordinateur virtuel, ce dernier peut alors afficher des graphiques hautes performances grâce à Microsoft DirectX® et à la puissance de traitement des graphiques sur le serveur Windows Server 2012 hôte.

Documentation supplémentaire : Pour plus d'informations sur les cartes Fibre Channel virtuelles, consultez la Vue d'ensemble d'Hyper-V Fibre Channel virtuel à l'adresse http://go.microsoft.com/fwlink/?LinkId=269712.

Configuration de la mémoire dynamique

Dans la première version de Hyper-V avec Windows Server 2008, vous pouviez attribuer uniquement une quantité statique de mémoire aux ordinateurs virtuels. À moins que vous n'ayez pris des précautions spéciales pour mesurer la quantité précise de mémoire requise par un ordinateur virtuel, il est probable que vous ayez sous-alloué ou sur-alloué de la mémoire.



La mémoire dynamique a été introduite avec Windows Server 2008 R2 Service Pack 1 (SP1). Avec la mémoire dynamique vous pouvez :

- allouer une quantité de mémoire minimum à un ordinateur virtuel ;
- autoriser l'ordinateur virtuel à demander de la mémoire supplémentaire si besoin est ;
- configurer une quantité de mémoire maximum pour un ordinateur virtuel.

Ainsi, grâce à la mémoire dynamique, vous n'avez plus besoin de deviner la quantité de mémoire nécessaire pour un ordinateur virtuel ; au lieu de cela, vous pouvez configurer Hyper-V de sorte que l'ordinateur virtuel se voit allouer autant de mémoire que nécessaire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avec Windows Server 2012, vous pouvez modifier certaines valeurs minimum et maximum de mémoire dynamique pendant l'exécution de l' l'ordinateur virtuel. Cela n'était pas possible avec Windows Server 2008 R2 SP1. Vous pouvez effectuer cette tâche à partir de la boîte de dialogue **Paramètres** d'un ordinateur virtuel.

Remarque : Les ordinateurs virtuels doivent prendre en charge les services d'intégration Hyper-V pour pouvoir utiliser la mémoire dynamique.

Pagination intelligente

Les ordinateurs virtuels peuvent avoir besoin de plus de mémoire au démarrage qu'en mode de fonctionnement normal. La pagination intelligente, nouvelle fonctionnalité de Windows Server 2012, attribue de la mémoire provisoire supplémentaire à un ordinateur virtuel lorsque vous redémarrez ce dernier. Cela signifie que vous pouvez allouer de la mémoire en fonction des besoins de l'ordinateur virtuel en mode de fonctionnement normal, et non en fonction de ses besoins en mémoire au démarrage. La pagination intelligente utilise la pagination de disque pour attribuer de la mémoire provisoire supplémentaire à un ordinateur virtuel lors de son redémarrage. Toutefois, l'utilisation de la pagination intelligente peut se traduire par une baisse des performances car cette fonction emploie des ressources de disque qui seraient autrement utilisées par le serveur hôte et par d'autres ordinateurs virtuels.

Remarque : Vous pouvez configurer la mémoire d'un ordinateur virtuel à l'aide de l'applet de commande Windows PowerShell **Set-VMMemory**.

Documentation supplémentaire : Pour plus d'informations sur la mémoire dynamique Hyper-V, voir Hyper-V Dynamic Memory Overview à l'adresse http://go.microsoft.com/fwlink/?LinkId=269713.

Configuration des services d'intégration d'un ordinateur virtuel

Vous devez installer les services d'intégration d'ordinateur virtuel si vous souhaitez utiliser des fonctionnalités telles que l'arrêt du système d'exploitation, la synchronisation, et si vous souhaitez installer des composants matériels virtuels, tels que des cartes SCSI et des cartes réseau synthétiques, sur les ordinateurs virtuels.

Services d'intégration possibles
- Arrêt du système d'exploitation
- Synchronisation date/heure
- Échange de données
- Pulsation
- Sauvegarde (instantané de volume)

Les systèmes d'exploitation invités d'ordinateur virtuel qui sont pris en charge par Hyper-V et qui peuvent utiliser les services d'intégration sont les suivants :

- Windows Server 2012
- Windows Server 2008 R2 avec SP1
- Windows Server 2008 avec Service Pack 2 (SP2)
- Windows Server 2003 R2 avec SP2

- Windows Home Server 2011
- Windows MultiPoint® Server 2012
- Windows Small Business Server 2011
- Windows Server 2003 avec SP2
- CentOS 6.0-6.2
- CentOS 5.5-5.7
- Red Hat Enterprise Linux 6.0-6.2
- Red Hat Enterprise Linux 5.5-5.7
- SUSE Linux Enterprise Server 11 avec SP1 ou SP2
- SUSE Linux Enterprise Server 10 avec SP4
- Windows 7 avec SP1
- Windows Vista® avec SP2
- Windows XP avec SP3

Remarque : La prise en charge du système d'exploitation Windows XP expirera en avril 2014. La prise en charge de Windows Server 2003 et Windows Server 2003 R2 expirera en juillet 2015.

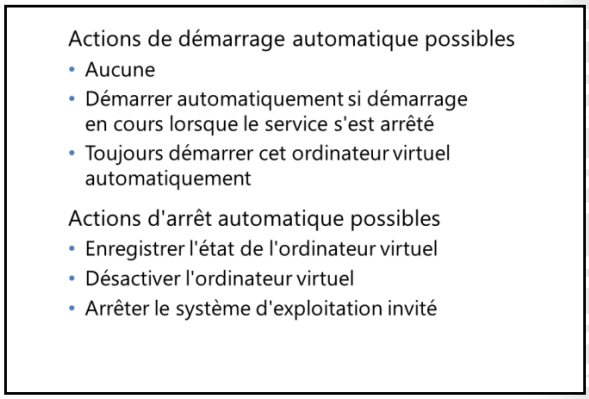
Vous pouvez installer les composants des services d'intégration Hyper-V sur un système d'exploitation ; pour cela, affichez la fenêtre Connexion à un ordinateur virtuel, puis dans le menu **Action**, cliquez sur l'élément **Insérer le disque d'installation des services d'intégration**. Vous pouvez ensuite installer les pilotes appropriés au système d'exploitation manuellement ou automatiquement. Vous pouvez également activer les composants d'intégration de l'ordinateur virtuel suivants :

- Arrêt du système d'exploitation. Permet au serveur qui exécute Hyper-V d'initialiser un arrêt normal de l'ordinateur virtuel invité.
- Synchronisation date/heure. Permet à l'ordinateur virtuel d'utiliser le processeur du serveur de virtualisation à des fins de synchronisation de la date et de l'heure.
- Échange de données. Permet au serveur qui exécute Hyper-V d'écrire des données dans le Registre de l'ordinateur virtuel.
- Pulsation. Permet à Hyper-V de déterminer si l'ordinateur virtuel a cessé de répondre.
- Sauvegarde (instantané de volume). Permet au fournisseur du service de cliché instantané de volume (VSS) de créer des instantanés de l'ordinateur virtuel à des fins d'opération de sauvegarde, sans interruption du fonctionnement normal de l'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des actions de démarrage et d'arrêt d'un ordinateur virtuel



Vous pouvez utiliser les actions de démarrage et d'arrêt d'un ordinateur virtuel pour vous assurer que les principaux ordinateurs virtuels démarrent toujours automatiquement à chaque redémarrage de Hyper-V, et qu'ils s'arrêtent normalement si le serveur reçoit une commande d'arrêt. Lorsque vous configurez les actions de démarrage et d'arrêt d'un ordinateur virtuel, vous sélectionnez les étapes qui doivent être effectuées par le serveur qui exécute Hyper-V sur des ordinateurs virtuels spécifiques lors de l'arrêt ou du démarrage du serveur physique. Pour configurer les paramètres de démarrage et d'arrêt de chaque ordinateur virtuel, vous modifiez les propriétés de l'ordinateur virtuel.

Options de démarrage automatique

Vous pouvez configurer les options suivantes dans la fenêtre Actions de démarrage automatique :

- Aucune. L'ordinateur virtuel ne démarre pas automatiquement au démarrage du serveur qui exécutant Hyper-V, même si l'ordinateur virtuel était à l'état d'exécution lorsque le serveur a été arrêté.
- Démarrer automatiquement s'il était en cours d'exécution lors de l'arrêt du service. L'ordinateur virtuel redémarre s'il était en cours d'exécution lorsque le serveur exécutant Hyper-V a reçu la commande d'arrêt, ou si l'ordinateur virtuel était en cours d'exécution lorsque le serveur a été mis hors tension suite à une panne.
- Toujours démarrer cet ordinateur virtuel automatiquement. L'ordinateur virtuel démarre systématiquement au démarrage du serveur exécutant Hyper-V. Vous pouvez configurer un délai de démarrage afin de vous assurer que plusieurs ordinateurs virtuels n'essaient pas de démarrer en même temps.

Options d'arrêt automatique

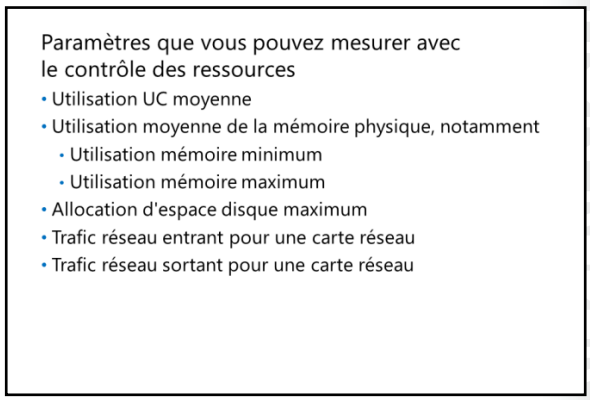
Vous pouvez configurer les options suivantes dans la fenêtre Actions d'arrêt automatique :

- Enregistrer l'état de l'ordinateur virtuel. Cette option enregistre l'état actif de l'ordinateur virtuel sur le disque, y compris la mémoire, lorsque le serveur reçoit une commande d'arrêt. Cela permet à l'ordinateur virtuel de redémarrer au redémarrage du serveur qui exécute Hyper-V.
- Désactiver l'ordinateur virtuel. L'ordinateur virtuel est désactivé lorsque le serveur reçoit une commande d'arrêt. Des données peuvent être perdues lorsque cela se produit.
- Arrêter le système d'exploitation invité**.** L'ordinateur virtuel est arrêté de façon normale lorsque le serveur reçoit une commande d'arrêt. Cette option est disponible uniquement si les composants des services d'intégration sont installés sur l'ordinateur virtuel.

Remarque : Vous pouvez également configurer des actions automatiques de démarrage et d'arrêt d'un ordinateur virtuel à l'aide de l'applet de commande Windows PowerShell **Set-VM** avec les paramètres **AutomaticStartAction** et **AutomaticStopAction**.

Contrôle des ressources Hyper-V

Le contrôle des ressources vous permet de suivre l'utilisation des ressources d'ordinateurs virtuels qui sont hébergées sur des serveurs Windows Server 2012 où le rôle Hyper-V est installé.



Grâce au contrôle des ressources, vous pouvez mesurer les paramètres suivants sur des ordinateurs virtuels Hyper-V individuels :

- utilisation UC moyenne ;
- utilisation moyenne de la mémoire physique, notamment :
  - utilisation mémoire minimum ;
  - utilisation mémoire maximum ;
- allocation d'espace disque maximum ;
- trafic réseau entrant pour une carte réseau ;
- trafic réseau sortant pour une carte réseau.

En mesurant la quantité de ressources utilisée par chaque ordinateur virtuel, une organisation peut facturer des services ou des clients en fonction du volume de ressources utilisé par ses ordinateurs virtuels, au lieu d'appliquer un forfait fixe par ordinateur virtuel. Une organisation comportant uniquement des clients internes peut également utiliser ces mesures pour dégager des modèles d'utilisation et prévoir de futures extensions. Pour effectuer des tâches de contrôle des ressources, à partir d'une interface de ligne de commande PowerShell, utilisez les applets de commande suivantes :

- **Enable-VMResourceMetering**. Démarre la collecte de données pour chaque ordinateur virtuel.
- **Disable-VMResourceMetering**. Désactive le contrôle des ressources sur chaque ordinateur virtuel.
- **Reset-VMResourceMetering**. Réinitialise les compteurs de contrôle des ressources sur les ordinateurs virtuels.
- **Measure-VM**. Affiche des statistiques de contrôle des ressources pour un ordinateur virtuel spécifique.

Remarque : Vous ne pouvez utiliser aucun outil d'interface graphique pour exécuter le contrôle des ressources.

Documentation supplémentaire : Pour plus d'informations concernant le contrôle des ressources pour Hyper-V, voir Hyper-V Resource Metering Overview à l'adresse http://go.microsoft.com/fwlink/?LinkId=269714.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Gestion du stockage d'ordinateur virtuel

Hyper-V fournit de nombreuses et différentes options de stockage d'ordinateur virtuel. Si vous savez quelle option est appropriée pour une situation donnée, vous pouvez vous assurer du bon fonctionnement d'un ordinateur virtuel. Toutefois, une mauvaise compréhension des différentes options de stockage de l'ordinateur virtuel peut entraîner le déploiement de disques durs virtuels qui consomment de l'espace ou chargent les performances inutilement sur le serveur de virtualisation.

Dans cette leçon, vous allez découvrir les différents types de disque dur virtuel, les différents formats de disque dur virtuel et les avantages et inconvénients dans l'utilisation d'instantanés d'ordinateurs virtuels.

Objectifs de la leçon

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

- décrire la finalité du système VHD ;
- expliquer comment créer un type VHD ;
- expliquer comment gérer des VHD ;
- expliquer comment déployer des disques durs virtuels de différenciation pour réduire le stockage ;
- expliquer comment utiliser des instantanés d'ordinateur virtuel.

Qu'est-ce qu'un disque dur virtuel (VHD) ?

Un disque VHD est un fichier qui représente un lecteur de disque dur traditionnel que vous pouvez configurer avec des partitions et un système d'exploitation. Vous pouvez utiliser des disques VHD sur des ordinateurs virtuels, et vous pouvez monter des disques VHD en tant que volumes locaux à l'aide des systèmes d'exploitation Windows Server 2008 R2, Windows Server 2012, Windows® 8 et Windows 7. Windows Server 2012 prend en charge le démarrage à partir d'un disque VHD ; cela vous permet de configurer un ordinateur pour qu'il démarre sur un système d'exploitation Windows Server 2012 déployé sur un disque VHD, ou sur certaines éditions du système d'exploitation Windows 8 qui sont déployées sur un disque VHD.. Vous pouvez créer un disque VHD avec :

Un disque dur virtuel est un fichier qui représente un lecteur de disque dur classique

Le format VHDX présente les avantages suivants par rapport au format VHD

- Les disques peuvent être de plus grande taille (64 To au lieu de 2 To)
- Le disque est moins susceptible d'être endommagé
- Le format prend en charge un meilleur alignement lorsqu'il est déployé sur un disque secteur de grande taille
- Le format prend en charge une taille de bloc supérieure pour les disques dynamiques et les disques de différenciation

- la console du Gestionnaire Hyper-V ;
- la console de gestion des disques ;
- l'outil en ligne de commande (diskpart.exe) de DiskPart ;
- l'applet de commande Windows PowerShell **New-VHD**.

Remarque : Certaines éditions de Windows 7 et Windows Server 2008 R2 prennent également en charge le démarrage à partir d'un disque VHD.

Disques VHD au format .vhd et disques au format .vhdx

Les disques VHD utilisent l'extension .vhd. Windows Server 2012 présente un nouveau type de disque VHD laquelle utilise l'extension .vhdx. Les disques VHD au nouveau format présentent les avantages suivants par rapport aux disques VHD qui étaient utilisés dans Hyper-V sur Windows Server 2008 et Windows Server 2008 R2 :

- Les disques VHD au format .vhdx peuvent avoir la taille de 64 To, alors que le format VHD est limité à 2 To.
- Les disques VHD au format .vhdx sont moins susceptibles d'être endommagés si une panne de courant se produit sur le serveur de virtualisation.
- Le format .vhdx prend en charge un meilleur alignement lorsqu'il est déployé sur un disque secteur de grande taille.
- Les disques VHD au format .vhdx peuvent contenir des VHD de taille dynamique et des VHD de différenciation de plus grande taille, ce qui signifie que les VHD de taille dynamique et les VHD de différenciation fonctionnent mieux.

Vous pouvez convertir un disque VHD du format .vhd au format .vhdx à l'aide de l'Assistant Modification de disque dur virtuel ; cette opération peut être nécessaire si vous avez mis à niveau un serveur de virtualisation Windows Server 2008 ou Windows Server 2008 R2 vers Windows Server 2012. Vous pouvez également convertir un disque VHD du format .vhdx au format .vhd.

Prise en charge du partage SMB

Windows Server 2012 prend maintenant en charge le stockage de tous les fichiers des ordinateurs virtuels, notamment des disques VHD sur partages de fichiers SMB 3.0. Il s'agit d'une alternative au stockage de ces fichiers sur Internet SCSI (iSCSI) ou sur les périphériques SAN Fibre Channel. Lors de la création d'un ordinateur virtuel dans Hyper-V sur Windows Server 2012, vous pouvez spécifier un partage réseau lorsque vous choisissez l'emplacement du disque VHD ou lorsque vous connectez un disque VHD existant. Le partage de fichiers doit prendre en charge SMB 3.0. Cela signifie que vous devez placer les disques VHD sur les partages de fichiers qui sont hébergés sur des serveurs de fichiers avec Windows Server 2012. Les versions antérieures de Windows Server ne prennent pas en charge SMB 3.0.

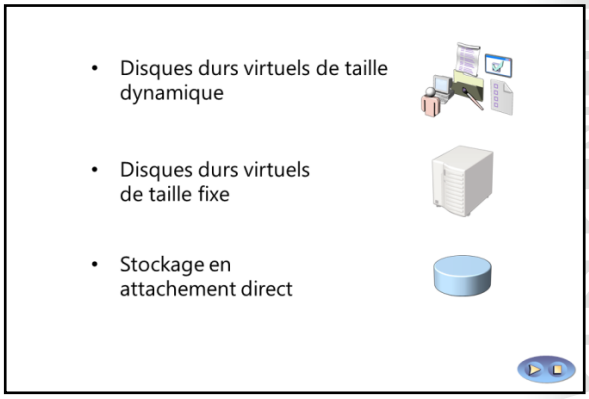
Documentation supplémentaire : Pour plus d'informations sur les formats de disque VHD, voir Hyper-V Virtual Hard Disk Format Overview à l'adresse http://go.microsoft.com/fwlink/?LinkId=269715.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Création de types de disque virtuel

Lorsque vous configurez un disque VHD, vous avez le choix entre plusieurs types différents de disque, fixe, dynamique et stockage en attachement direct.



Création de disques VHD fixes

Lorsque vous créez des disques VHD fixes, l'espace disque que vous avez spécifié est alloué au cours du processus de création. Cela réduit la fragmentation, ce qui améliore les performances si le disque dur virtuel se trouve sur un périphérique de stockage traditionnel (i.e non SSD). Allouer tout l'espace disque spécifié au cours du processus de création présente néanmoins un inconvénient, très souvent vous ne saurez pas précisément de combien d'espace disque un ordinateur virtuel a besoin. Par conséquent, vous allez peut-être allouer de l'espace qui n'est pas réellement requis.

Remarque : La fragmentation du disque n'est pas réellement un problème lorsque les disques VHD sont hébergés sur des volumes RAID ou sur des disques SSD. Les améliorations de Hyper-V (depuis son introduction avec Windows Server 2008) réduisent également les différences de performances entre les disques VHD dynamiques et fixes.

Pour créer un disque VHD fixe, procédez comme suit :

1. Ouvrez la console du **Gestionnaire Hyper-V**.
2. Dans le volet Actions, cliquez sur **Nouveau**, puis cliquez sur **Disque dur**.
3. Sur la page **Avant de commencer** de l'assistant Nouveau disque dur virtuel, cliquez sur **Suivant**.
4. Dans le nouvel Assistant Nouveau disque dur virtuel, sur la page **Choisir le format du disque**, cliquez sur **VHD** ou **VHDX**, puis sur **Suivant**.
5. Dans la page **Choisir le type de disque**, cliquez sur **Taille fixe**, puis sur **Suivant**.
6. Dans la page **Spécifier le nom et l'emplacement**, entrez un nom pour le disque VHD, puis indiquez un dossier dans lequel héberger le fichier VHD.
7. Dans la page **Configurer le disque**, choisissez l'une des options suivantes :
   - **Créer un nouveau disque dur virtuel vierge de la taille spécifiée**.
   - **Copier le contenu d'un disque physique spécifié**. Avec cette option, vous pouvez répliquer un disque physique existant sur le serveur comme disque VHD. Le disque VHD fixe sera de la même taille que le disque physique. La réplication d'un disque dur physique existant ne modifie pas les données sur ce disque.
   - **Copier le contenu d'un disque dur virtuel spécifié**. Avec cette option, vous pouvez créer un nouveau disque dur fixe en fonction du contenu d'un disque VHD existant.

Remarque : Vous pouvez créer un nouveau disque dur fixe à l'aide de l'applet de commande Windows PowerShell **New-VHD** avec le paramètre **-Fixed** (fixe).

Disques VHD de taille dynamique

Lorsque vous créez un disque VHD de taille dynamique, vous spécifiez une taille maximale, mais le disque utilise seulement l'espace dont il a besoin et il augmente de taille si nécessaire. Un disque VHD de taille dynamique peut être créé au format .vhd ou .vhdx. Un nouveau disque VHD de taille dynamique au format .vhd se voit allouer environ 260 kilo-octets (ko). Un nouveau disque VHD de taille dynamique au format .vhdx se voit allouer environ 4 096 kilo-octets (ko).

Lorsque vous sauvegardez des fichiers sur un disque VHD de taille dynamique, ce dernier augmente de taille. Il n'est possible de réduire un fichier de disque VHD de taille dynamique qu'en effectuant une opération de compactage.

Pour créer un disque VHD de taille dynamique, suivez les étapes de création d'un disque VHD fixe indiquées plus haut, à l'exception de celles de la page Choisir le type de disque (à l'étape 5), cliquez sur **Taille dynamique** au lieu de **Taille fixe**.

Remarque : Vous pouvez créer un nouveau disque dur dynamique à l'aide de l'applet de commande Windows PowerShell **New-VHD** (nouveau disque dur virtuel) avec le paramètre **-Dynamic**.

Stockage en attachement direct

Le stockage en attachement direct permet à un ordinateur virtuel d'accéder à un lecteur de disque physique. Vous pouvez utiliser le stockage en attachement direct pour relier un ordinateur virtuel directement à un numéro d'unité logique iSCSI. Lorsque vous utilisez le stockage en attachement direct, l'ordinateur virtuel doit avoir un accès exclusif au disque cible ; pour vous en assurer, vous devez mettre le disque hors connexion.

Vous pouvez lier un stockage en attachement direct en procédant comme suit :

1. Vérifiez que le disque dur cible est hors connexion. Si ce n'est pas le cas, utilisez la console de gestion des disques sur le serveur de virtualisation pour le mettre hors connexion.
2. Utilisez la console du Gestionnaire Hyper-V pour modifier les propriétés d'un ordinateur virtuel existant.
3. Cliquez sur un contrôleurs IDE ou SCSI, cliquez sur **Ajouter**, puis sur **Disque dur**.
4. Dans la boîte de dialogue **Disque dur**, cliquez sur **Disque dur physique**. Dans le menu déroulant, sélectionnez le disque que vous souhaitez utiliser comme stockage en attachement direct.

Remarque : Si vous reliez un stockage en attachement direct au contrôleur SCSI d'un ordinateur virtuel, il n'est pas nécessaire d'arrêter l'ordinateur virtuel. Si vous souhaitez le connecter au contrôleur IDE d'un ordinateur virtuel, vous devez d'abord arrêter ce dernier.

Question : Pourquoi pourriez-vous envisager d'utiliser des disques VHD au lieu de disques de taille dynamique ?

Question : Dans quelles situations pourriez-vous rencontrer des difficultés si vous utilisez des disques de taille dynamique ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des disques durs virtuels (VHD)

De temps en temps, vous devez exécuter des opérations de maintenance sur des disques VHD. Par exemple, vous souhaitez peut-être convertir un disque VHD dans un autre format car vos besoins évoluent, ou vous voulez condenser un disque VHD pour libérer de l'espace. Vous pouvez effectuer les opérations de maintenance suivantes sur les disques VHD :

Opérations de maintenance possibles sur les disques durs virtuels

- Conversion du format fixe au format dynamique
- Conversion du format dynamique au format fixe
- Conversion du format VHD au format VHDX
- Conversion du format VHDX au format VHD
- Réduction d'un disque dur virtuel dynamique
- Développement d'un disque dur virtuel fixe ou dynamique

- convertir le disque du format fixe au format dynamique ;
- convertir le disque du format dynamique au format fixe ;
- convertir un disque VHD du format .vhd au format .vhdx
- convertir un disque VHD du format .vhdx au format .vhd
- compacter un disque VHD de taille dynamique ;
- développer un disque VHD de taille dynamique ;
- développer un disque VHD fixe.

Conversion d'un disque

Lorsque vous convertissez un disque VHD, le contenu du disque VHD existant est copié sur un disque VHD nouvellement créé. Par exemple, lorsque vous convertissez un disque VHD fixe en disque VHD de taille dynamique, un nouveau disque dynamique est créé, le contenu du disque fixe est copié sur ce nouveau disque dynamique, puis le disque fixe est supprimé.

Pour convertir un disque VHD en disque dynamique ou inversement, procédez comme suit :

1. Dans le volet Actions de la console du Gestionnaire Hyper-V, cliquez sur **Modifier le disque**.
2. Dans l'Assistant Modification de disque dur virtuel, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Disque dur virtuel local**, cliquez sur **Parcourir**, puis sélectionnez le disque VHD que vous voulez convertir.
4. Dans la page **Choisir une action**, cliquez sur **Convertir**, puis sur **Suivant**.
5. Dans la page **Convertir un disque dur virtuel**, choisissez le format **VHD** ou **VHDX**.
6. Dans la page **Convertir un disque dur virtuel**, choisissez **Taille fixe** ou **Taille dynamique**. Si vous souhaitez également convertir le type de disque dur, choisissez le type approprié, puis cliquez sur **Suivant**.
7. Dans la page **Configurer un disque**, choisissez l'emplacement du disque.

Modification de la taille d'un disque

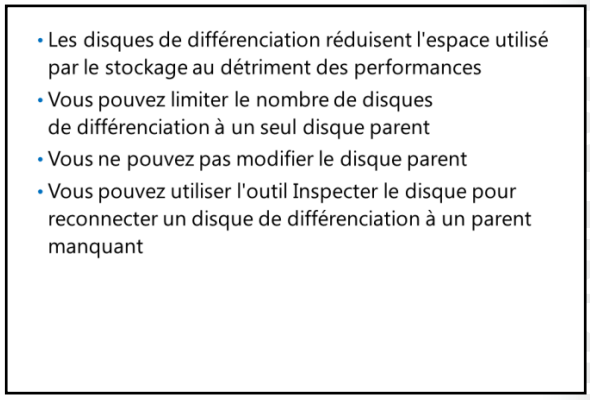
Vous pouvez compacter un disque VHD de taille dynamique qui n'utilise pas tout l'espace qui lui est alloué. Cependant, vous ne pouvez pas compacter un disque VHD fixe ; vous devez d'abord le convertir en disque VHD de taille dynamique avant de le compacter. Vous pouvez développer des disques VHD de taille dynamique et des disques VHD fixes.

Pour modifier la taille d'un disque VHD, vous pouvez utiliser l'une des deux méthodes suivantes. Ces méthodes sont les suivantes :

1. Utilisez les applets de commande Windows PowerShell **resize-partition** et **resize-vhd**.
2. Dans l'Assistant Modification de disque dur virtuel, sélectionnez l'option **Compacter** ou **Développer**.

Réduction des besoins de stockage avec les disques VHD de différenciation

Les disques VHD de différenciation sont des disques VHD distincts qui enregistrent les modifications apportées à un disque parent. Vous pouvez utiliser des disques VHD de différenciation pour réduire la quantité d'espace disque consommée par les disques VHD ; cela accroît les performances du disque en réduisant l'espace utilisé. Les disques VHD de différenciation fonctionnent bien avec les disques SSD. Ils fonctionnent bien également lorsque l'espace disponible sur le volume parent est limité et que les performances du disque compensent les inconvénients en termes de performances liés à l'utilisation d'un disque VHD de différenciation.



Vous pouvez lier plusieurs disques VHD de différenciation à un seul disque parent. Toutefois, si vous modifiez le disque parent, les liens à tous les disques VHD de différenciation échouent.

Vous pouvez reconnecter un disque VHD de différenciation au disque parent à l'aide de l'outil Inspecter le disque, lequel est disponible dans le volet Actions de la console du Gestionnaire Hyper-V. Vous pouvez également utiliser l'outil Inspecter le disque pour localiser le disque parent d'un disque VHD de différenciation.

Vous pouvez créer un disque VHD de différenciation à l'aide de la console du Gestionnaire Hyper-V ou à l'aide de l'applet de commande Windows PowerShell **New-VHD**.

Pour créer un disque VHD de différenciation à l'aide de la console du Gestionnaire Hyper-V, procédez comme suit :

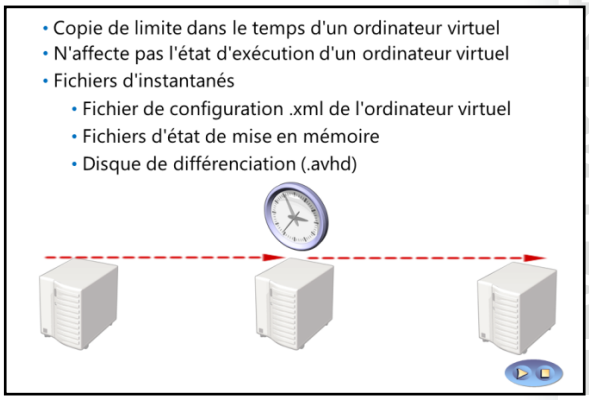
1. Ouvrez la console du **Gestionnaire Hyper-V**.
2. Dans le volet Actions, cliquez sur **Nouveau**, puis sur **Disque dur**.
3. Dans l'Assistant Nouveau disque dur virtuel, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Choisir le format du disque**, cliquez sur **VHD**, puis sur **Suivant**.
5. Dans la page **Choisir le type de disque**, cliquez sur **Différenciation**, puis sur **Suivant**.
6. Dans la page **Spécifier le nom et l'emplacement**, indiquez l'emplacement du disque dur parent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour créer un disque VHD de différenciation à l'aide de l'applet de commande Windows PowerShell **New-VHD**, suivez le modèle de l'exemple suivant. Pour créer un nouveau disque VHD de différenciation nommé c:\diff-disk.vhd qui utilise le disque VHD c:\parent.vhd, utilisez la commande Windows PowerShell suivante :

```
New-VHD c:\diff-disk.vhd -ParentPath C:\parent.vhd
```

Utilisation d'instantanés



Les instantanés sont une image statique des données sur un ordinateur virtuel à un moment donné. Les instantanés sont enregistrés au format .avhd ou .avhdx selon le format du disque VHD. Vous pouvez prendre un instantané d'un ordinateur virtuel à partir du volet **Actions** de la fenêtre Connexion à un ordinateur virtuel, ou à partir de la console du Gestionnaire Hyper-V. Chaque ordinateur virtuel peut avoir un maximum de 50 instantanés.

Vous pouvez prendre des instantanés à tout moment, même lorsqu'un ordinateur virtuel est arrêté. Lorsque vous prenez un instantané d'un ordinateur virtuel en cours d'exécution, cet instantané inclut le contenu de la mémoire de l'ordinateur virtuel.

Lorsque vous prenez des instantanés de plusieurs ordinateurs virtuels qui font partie du même groupe, par exemple un contrôleur de domaine virtuel et un serveur membre virtuel, vous devez prendre ces instantanés simultanément. Cela garantit que des éléments tels que les mots de passe de compte d'ordinateur sont les mêmes sur tous les instantanés.

Souvenez-vous que lorsque vous rétablissez un ordinateur sur un instantané, son état est rétabli à une limite dans le temps. Si vous restaurez un ordinateur à un point antérieur à l'exécution d'une modification de mot de passe d'ordinateur avec un contrôleur de domaine, il sera nécessaire de le reconnecter au domaine ou d'exécuter la commande **netdom resetpwd**.

Instantanés et sauvegardes

Les instantanés ne constituent pas une solution de remplacement pour les sauvegardes. Les instantanés sont enregistrés sur le même volume que les disques VHD. Si ce volume échoue, les instantanés et le fichier VHD sont perdus.

Exportation d'instantanés

Il est possible d'exporter l'instantané d'un ordinateur virtuel. Dans ce cas, Hyper-V crée des disques VHD complets qui représentent l'état de l'ordinateur virtuel au moment de la prise de l'instantané. Si vous choisissez d'exporter l'intégralité d'un ordinateur virtuel, tous les instantanés associés à cet ordinateur virtuel sont également exportés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fichiers de disque VHD de différenciation

Lorsque vous créez un instantané, Hyper-V écrit des fichiers VHD de différenciation (.avhd, ou .avhdx) qui enregistrent les données qui différencient l'instantané de l'instantané précédent ou du disque VHD parent. Lorsque vous supprimez des instantanés, ces données sont ignorées ou fusionnées dans l'instantané précédent ou le disque VHD parent. Par exemple :

- Si vous supprimez l'instantané le plus récent, les données sont ignorées. Avec Hyper-V dans Windows Server 2012, cet espace est récupéré immédiatement et non pas lorsque l'ordinateur virtuel est arrêté.
- Si vous supprimez le deuxième instantané le plus récent, les données sont fusionnées de sorte que les états des instantanés les plus récents et les plus anciens conservent leur intégrité.

Gestion des instantanés

Lorsque vous appliquez un instantané, l'ordinateur virtuel est rétabli à la configuration qui était la sienne au moment de la prise de l'instantané. Le rétablissement à un instantané ne supprime aucun instantané existant. Si vous appliquez un instantané après avoir fait une modification de configuration dans un instantané différent, vous êtes invité à prendre un autre instantané. Vous n'aurez besoin de créer un nouvel instantané que si vous souhaitez retourner à cette configuration actuelle.

Il est possible de créer des arborescences d'instantanés qui ont différents branches. Par exemple, prenons le scénario suivant :

Vous prenez un instantané d'un ordinateur virtuel le lundi, le mardi et le mercredi. Le jeudi, vous appliquez l'instantané du mardi. Immédiatement après avoir appliqué l'instantané du mardi, vous apportez des modifications à la configuration de l'ordinateur virtuel.

Dans ce scénario, la branche d'origine est la série d'instantanés pris le lundi, le mardi et le mercredi. Vous créez une nouvelle branche en appliquant l'instantané du mardi et en apportant des modifications à l'ordinateur virtuel. Plusieurs branches peuvent exister, à condition de ne pas dépasser la limite de 50 instantanés par ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Gestion des réseaux virtuels

Hyper-V propose plusieurs options pour la communication réseau entre les ordinateurs virtuels. Vous pouvez configurer des ordinateurs virtuels qui communiquent avec un réseau externe d'une manière semblable à celle utilisée pour le déploiement traditionnel d'hôtes physiques. Vous pouvez configurer des ordinateurs virtuels pour qu'ils communiquent seulement avec un nombre limité d'autres ordinateurs virtuels qui sont hébergés sur le même serveur. Si vous connaissez les options disponibles pour les réseaux virtuels Hyper-V, vous pourrez en tirer profit pour répondre au mieux aux besoins de votre organisation.

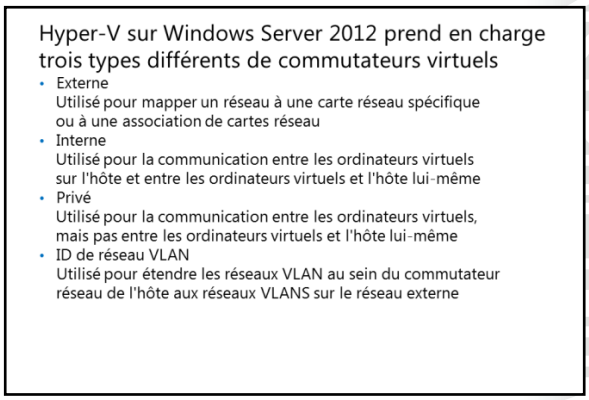
Objectifs de la leçon

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

- décrire les commutateurs virtuels ;
- décrire la virtualisation de réseau Hyper-V ;
- expliquer comment gérer le pool d'adresses MAC d'un ordinateur virtuel ;
- expliquer comment configurer les cartes réseau virtuelles.

Qu'est-ce qu'un commutateur virtuel ?

Un commutateur virtuel est une version virtuelle d'un commutateur réseau. (Le terme *réseau virtuel*, qui était utilisé dans Windows Server 2008, a été remplacé par le terme *commutateur virtuel* dans Windows Server 2012.) Les commutateurs virtuels contrôlent le flux du trafic réseau entre les ordinateurs virtuels qui sont hébergés sur le serveur de virtualisation, et entre les ordinateurs virtuels et le reste du réseau organisationnel. Vous gérez les commutateurs virtuels via le gestionnaire de commutateur virtuel, lequel est accessible via le volet Actions de la console du Gestionnaire Hyper-V. Hyper-V sur Windows Server 2012 prend en charge trois types différents de commutateurs virtuels :



- Externe. Ce type de commutateur mappe un réseau à une carte réseau spécifique ou à une association de cartes réseau. Windows Server 2012 prend en charge le mappage d'un réseau externe à une carte réseau sans fil si vous avez installé le service de réseau local sans fil sur le serveur de virtualisation et si le serveur de virtualisation a une carte compatible.
- Interne. Les commutateurs virtuels internes assurent la communication entre les ordinateurs virtuels sur le serveur de virtualisation et entre les ordinateurs virtuels et le serveur de virtualisation lui-même.
- Privé. Les commutateurs privés assurent uniquement la communication entre les ordinateurs virtuels sur le serveur de virtualisation. Vous ne pouvez pas utiliser des commutateurs privés pour la communication entre les ordinateurs virtuels et le serveur de virtualisation lui-même.

Lors de la configuration d'un réseau virtuel, vous pouvez également configurer un ID de réseau virtuel (VLAN) à associer au réseau. Cela vous permet d'étendre les réseaux VLAN existants sur le réseau externe aux réseaux VLAN au sein du commutateur réseau du serveur de virtualisation. Les réseaux VLAN vous permettent de partitionner le trafic réseau et ils fonctionnent en tant que réseaux logiques distincts. Le trafic peut uniquement passer d'un réseau VLAN à un autre s'il traverse un routeur.

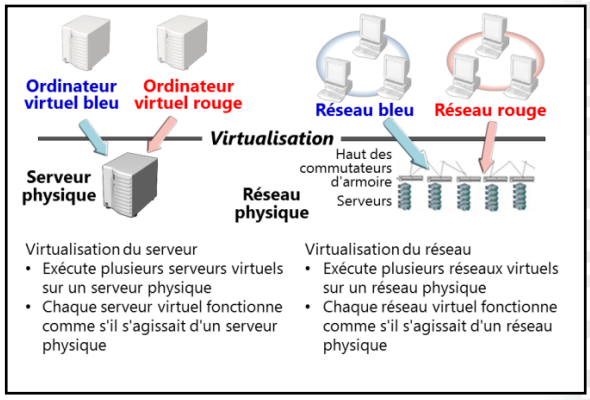
Vous pouvez configurer les extensions suivantes pour chaque type de commutateur virtuel :

- Capture NDIS Microsoft. Cette extension permet la capture des données qui traversent le commutateur virtuel.
- Plateforme de filtrage Microsoft Windows. Cette extension permet le filtrage des données qui traversent le commutateur virtuel.

Documentation supplémentaire : Pour plus d'informations sur les commutateurs virtuels, voir Hyper-V Virtual Switch Overview à l'adresse http://go.microsoft.com/fwlink/?LinkId=269716.

Virtualisation de réseau Hyper-V

La virtualisation de réseau Hyper-V vous permet d'isoler les ordinateurs virtuels qui partagent le même serveur physique. Par exemple, si vous fournissez une infrastructure en tant que service (IaaS) à différentes entreprises, vous devez isoler leurs ordinateurs virtuels les uns des autres. Avec la virtualisation de réseau, vous pouvez affecter les ordinateurs virtuels à des réseaux VLAN distincts afin d'isoler le trafic réseau. Vous déployez la virtualisation de réseau essentiellement dans les scénarios où vous utilisez un serveur qui exécute Hyper-V pour héberger les ordinateurs virtuels d'une autre organisation.



Lorsque vous configurez la virtualisation de réseau, chaque ordinateur virtuel invité a deux adresses IP qui fonctionnent comme suit :

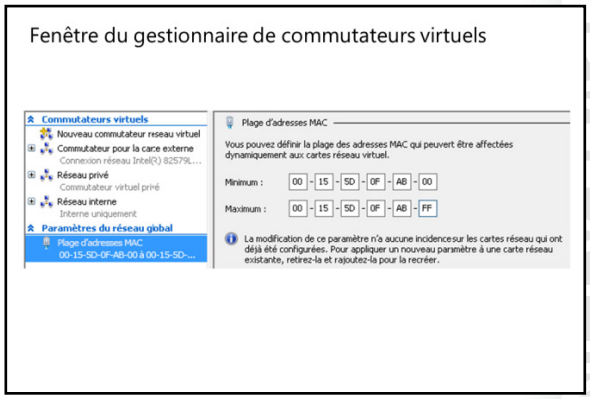
- Adresse IP du client. Cette adresse est attribuée par le client à l'ordinateur virtuel. Cette adresse IP est configurée de sorte que la communication avec le réseau interne du client soit possible même si l'ordinateur virtuel est hébergé sur un serveur de virtualisation qui est connecté à un réseau IP public distinct. Pour afficher l'adresse IP du client, à partir d'une invite de commandes sur l'ordinateur virtuel, exécutez **IPCONFIG**.
- Adresse IP du fournisseur. Cette adresse est attribuée par le fournisseur d'hébergement. Cette adresse est visible pour le fournisseur d'hébergement et pour les autres hôtes sur le réseau physique, mais elle n'est pas visible par l'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La virtualisation de réseau vous permet d'héberger plusieurs ordinateurs qui utilisent la même adresse client (par exemple, 192.168.15.101) sur le même serveur qui exécute Hyper-V, car les ordinateurs virtuels ont des adresses IP de différents fournisseurs.

Documentation supplémentaire : Pour plus d'informations sur la virtualisation de réseau, voir Hyper-V Network Virtualization Overview à l'adresse http://go.microsoft.com/fwlink/?LinkId=269717.

Gestion des adresses MAC d'un ordinateur virtuel



À moins que vous spécifiiez une adresse MAC statique, Hyper-V alloue dynamiquement une adresse à chaque carte réseau d'ordinateur virtuel d'un pool d'adresses MAC. Vous pouvez configurer la plage d'adresses de ce pool avec le paramètre **Plage d'adresses MAC** de la console du gestionnaire de commutateur virtuel. Par défaut, un serveur exécutant Hyper-V a un pool de 255 adresses MAC.

Lorsque les ordinateurs virtuels utilisent des réseaux privés ou internes, l'adresse MAC qui est allouée aux cartes réseau n'a pas vraiment d'importance car le serveur qui exécute Hyper-V vérifie qu'aucune adresse MAC en double n'est attribuée aux différents ordinateurs virtuels. Toutefois, lorsque plusieurs serveurs exécutent Hyper-V et hébergent des ordinateurs virtuels utilisant des cartes connectées à des réseaux externes, vous devez vous assurer que chaque serveur utilise un pool d'adresses MAC différent. Cela garantit que des serveurs distincts qui se connectent au même réseau n'attribuent pas les mêmes adresses MAC aux ordinateurs virtuels qu'ils hébergent.

Lorsque les adresses IP sont allouées aux ordinateurs virtuels via une réservation DHCP, vous devez penser à utiliser des adresses MAC statiques. Une réservation DHCP vérifie qu'une adresse IP particulière est toujours allouée à une adresse MAC spécifique.

Vous pouvez configurer la plage d'adresses MAC en procédant comme suit :

1. Ouvrez la console du **Gestionnaire Hyper-V**.
2. Sélectionnez l'hôte Hyper-V que vous souhaitez configurer.
3. Dans le volet Actions, cliquez sur **Gestionnaire de commutateur virtuel**.
4. Sous **Paramètres du réseau global**, cliquez sur **Plage d'adresses MAC**.
5. Spécifiez une plage minimum et maximum pour l'adresse MAC.

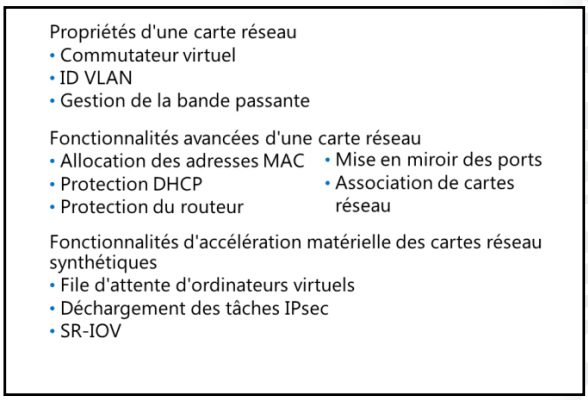
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les adresses MAC sont au format hexadécimal. Lors de la configuration des plages de plusieurs hôtes Hyper-V, vous devez penser à modifier les valeurs de la deuxième des dernières paires de chiffres. Le tableau suivant comporte des exemples de plages pour plusieurs hôte Hyper-V.

Hôte Hyper-V	Plage d'adresses MAC
Hôte 1	Minimum : 00-15-5D-0F-AB-00 Maximum : 00-15-5D-0F-AB-FF
Hôte 2	Minimum : 00-15-5D-0F-AC-00 Maximum : 00-15-5D-0F-AC-FF
Hôte 3	Minimum : 00-15-5D-0F-AD-00 Maximum : 00-15-5D-0F-AD-FF

Configuration des cartes réseau virtuel

Les cartes réseau virtuel permettent à l'ordinateur virtuel de communiquer au moyen de commutateurs virtuels que vous configurez dans la console du gestionnaire de commutateur virtuel. Vous pouvez modifier les propriétés d'un ordinateur virtuel pour modifier les propriétés d'une carte réseau. Dans le volet Carte réseau de la boîte de dialogue **Paramètres** de l'ordinateur virtuel, vous pouvez configurer les élément suivants :



- Commutateur virtuel. Vous configurez le commutateur virtuel auquel se connecte la carte réseau.
- ID VLAN. Vous spécifiez un ID VLAN que l'ordinateur virtuel utilise pour la communication qui traverse cette carte.
- Gestion de la bande passante. Vous allouez une bande passante minimum et maximum pour la carte. L'allocation de bande passante minimum est réservée par Hyper-V pour la carte réseau, même lorsque les cartes réseau virtuelles sur les autres ordinateurs virtuels fonctionnent à plein rendement.

Les cartes réseau synthétiques et les cartes réseau héritées prennent en charge les fonctionnalités avancées suivantes :

- Allocation des adresses MAC. Vous pouvez configurer une adresse MAC à attribuer depuis le pool d'adresses MAC, ou vous pouvez configurer la carte réseau pour l'utilisation d'une adresse MAC fixe. Vous pouvez également configurer l'usurpation d'adresse MAC. Cela est utile lorsque l'ordinateur virtuel doit fournir un accès réseau spécifique, notamment lorsque l'ordinateur virtuel exécute un émulateur d'appareil mobile qui a besoin d'un accès réseau.
- Protection DHCP. Cette fonctionnalité supprime les messages DHCP des ordinateurs virtuels qui fonctionnent en tant que serveurs DHCP non autorisés. Cela peut être utile dans les scénarios où vous gérez un serveur exécutant Hyper-V qui héberge des ordinateurs virtuels pour d'autres, mais qui n'a pas de contrôle direct sur la configuration de ces ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Protection du routeur. Cette fonctionnalité supprime les messages d'annonce et de redirection des ordinateurs virtuels qui sont configurés en tant que routeurs non autorisés. Cela peut être nécessaire dans les scénarios où vous n'avez pas de contrôle direct sur la configuration des ordinateurs virtuels.
- Mise en miroir des ports. Cette fonctionnalité vous permet de copier les paquets entrants et sortants d'une carte réseau vers un autre ordinateur virtuel que vous avez configuré pour la surveillance.
- Association de cartes réseau. Cette fonctionnalité vous permet d'ajouter la carte réseau virtuel à une équipe existante sur le serveur exécutant Hyper-V.

Les cartes réseau synthétiques requièrent que le système d'exploitation invité prenne en charge les services d'intégration. Outre les fonctionnalités avancées répertoriées précédemment, les cartes synthétiques prennent en charge les fonctionnalités d'accélération matérielle suivantes :

- File d'attente d'ordinateurs virtuels. Cette fonctionnalité utilise le filtrage de paquet matériel pour fournir le trafic réseau directement à l'invité. Cela améliore les performances car il n'est pas nécessaire de copier le paquet du système d'exploitation de gestion sur l'ordinateur virtuel. La file d'attente d'ordinateurs virtuels requiert que l'ordinateur hôte dispose d'une carte réseau qui prenne en charge cette fonctionnalité.
- Déchargement des tâches IPsec. Cette fonctionnalité permet l'exécution de tâches d'association de sécurité impliquant des calculs intensifs par la carte réseau de l'hôte. Au cas où il n'y aurait pas suffisamment de ressources matérielles disponibles, le système d'exploitation invité effectue ces tâches. Vous pouvez configurer un nombre maximal d'associations de sécurité déchargées compris entre 1 et 4 096. La tâche de sécurité IP (IPsec) de déchargement requiert que le système d'exploitation invité prenne en charge le support de carte réseau.
- SR-IOV. La virtualisation SR-IOV permet à plusieurs ordinateurs virtuels de partager les mêmes ressources matérielles physiques Peripheral Component Interconnect (PCI) Express. S'il n'y a pas suffisamment de ressources disponibles, la connectivité réseau est assurée via le commutateur virtuel. SR-IOV requiert du matériel spécifique et des pilotes particuliers à installer sur le système d'exploitation invité et peut aussi nécessiter d'être activé dans le BIOS de l'ordinateur.

Les cartes réseau héritées émulent le matériel de carte réseau courant. Vous utilisez des cartes réseau héritées dans les situations suivantes :

- Vous souhaitez prendre en charge des scénarios d'installation de démarrage réseau pour des ordinateurs virtuels. Par exemple, vous souhaitez déployer une image de système d'exploitation d'un serveur WDS (Services de déploiement Windows) ou via le gestionnaire de configuration.
- Vous devez prendre en charge des systèmes d'exploitation qui ne prennent pas en charge les services d'intégration et qui ne disposent pas de pilotes pour la carte réseau synthétique.

Les cartes réseau héritées ne prennent pas en charge les fonctionnalités d'accélération matérielle prises en charge par les cartes réseau synthétiques. Vous ne pouvez pas configurer la file d'attente d'ordinateurs virtuels, le déchargement de tâches IPsec ou la virtualisation SR-IOV pour les cartes réseau héritées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation de la virtualisation de serveur avec Hyper-V

Scénario

La société A. Datum Corporation a un bureau et un centre de données informatiques à Londres qui prennent en charge le site de Londres ainsi que d'autres sites. A. Datum a récemment déployé une infrastructure Windows Server 2012 avec des clients Windows 8. Votre première mission consiste à configurer le service d'infrastructure pour une nouvelle filiale.

Pour utiliser de manière plus efficace le matériel serveur qui est actuellement disponible au niveau des filiales, votre responsable a décidé que tous les serveurs de filiale fonctionneraient en tant qu'ordinateurs virtuels. Vous devez maintenant configurer un réseau virtuel et un nouvel ordinateur virtuel pour ces filiales.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- installer le rôle Hyper-V sur un serveur ;
- configurer les réseaux virtuels ;
- créer et configurer un ordinateur virtuel ;
- utiliser des instantanés d'ordinateurs virtuels.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateur virtuel	22410B-LON-HOST1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

1. Redémarrez l'ordinateur de la classe et, à partir du Gestionnaire de démarrage Windows, sélectionnez **22410B-LON-HOST1**.
2. Connectez-vous à **LON-HOST1** à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.

Exercice 1 : Installation du rôle Hyper V sur un serveur

Scénario

La première étape de migration vers un environnement virtualisé pour la filiale consiste à installer le rôle Hyper-V sur un nouveau serveur Windows Server 2012.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le rôle Hyper-V sur un serveur
2. Terminer l'installation du rôle Hyper-V et vérifier les paramètres

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Installer le rôle Hyper-V sur un serveur

1. Dans le Gestionnaire de serveur, cliquez sur **Serveur local**, puis configurez les paramètres réseau suivants :
   - Adresse IP : **172.16.0.31**
   - Masque de sous-réseau : **255.255.0.0**
   - Passerelle par défaut : **172.16.0.1**
   - Serveur DNS préféré : **172.16.0.10**
2. Utilisez l'Assistant Ajout de rôles et de fonctionnalités pour ajouter le rôle Hyper-V à LON-HOST1 avec les options suivantes :
   - Ne créez pas de commutateur virtuel.
   - Utilisez les emplacements de stockage par défaut.
   - Autorisez le serveur à redémarrer automatiquement si nécessaire.
3. Au bout de quelques minutes, le serveur redémarre automatiquement. Assurez-vous de redémarrer l'ordinateur à partir du menu de démarrage comme **22410B-LON-HOST1**. L'ordinateur redémarrera plusieurs fois.

▶ Tâche 2 : Terminer l'installation du rôle Hyper-V et vérifier les paramètres

1. Connectez-vous à LON-HOST1 à l'aide du compte **Administrateur** avec mot de passe **Pa$$word**.
2. À l'issue de l'installation des outils de **Hyper-V**, cliquez sur **Fermer**.
3. Ouvrez la console du Gestionnaire Hyper-V, puis double-cliquez sur **LON-HOST1**.
4. Éditez les paramètres Hyper-V de LON-HOST1, puis configurez les paramètres suivants :
   - Clavier **Utiliser sur l'ordinateur virtuel**
   - Disques durs virtuels : **C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks**

Résultats : À la fin de cet exercice, vous aurez installé le rôle Hyper-V sur un serveur physique.

Exercice 2 : Configuration d'un réseau virtuel

Scénario

Après l'installation du rôle Hyper-V sur le nouveau serveur, vous devez configurer le réseau virtuel. Vous devez créer un réseau qui est connecté au réseau physique, et un réseau privé qui peut être utilisé uniquement pour la communication entre les ordinateurs virtuels. Le réseau privé sera utilisé une fois que les ordinateurs virtuels sont configurés pour une haute disponibilité. Vous devez également configurer une plage spécifique d'adresses MAC pour les ordinateurs virtuels.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le réseau externe
2. Créer un réseau privé
3. Créer un réseau interne
4. Configurer la plage d'adresses MAC (Media Access Control)

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer le réseau externe

1. Ouvrez la console du **Gestionnaire Hyper-V**, puis double-cliquez sur **LON-HOST1**.
2. Utilisez le **Gestionnaire de commutateur virtuel** pour créer un nouveau commutateur de réseau virtuel externe avec les propriétés suivantes :
   - Nom : **Commutateur pour la carte externe**
   - Réseau externe : mappé à la carte réseau physique de l'ordinateur hôte. (Varie selon l'ordinateur hôte.)

▶ Tâche 2 : Créer un réseau privé

1. Sur LON-HOST1, ouvrez la console du **Gestionnaire Hyper-V**.
2. Utilisez le Gestionnaire de commutateur virtuel pour créer un nouveau commutateur de réseau virtuel externe avec les propriétés ci-après.
   - Nom : **Réseau privé**
   - Type de connexion : **Réseau privé**

▶ Tâche 3 : Créer un réseau interne

1. Sur LON-HOST1, ouvrez la console du **Gestionnaire Hyper-V**.
2. Utilisez le Gestionnaire de commutateur virtuel pour créer un nouveau commutateur de réseau virtuel externe avec les propriétés ci-après.
   - Nom : **Réseau interne**
   - Type de connexion : **Réseau interne**

▶ Tâche 4 : Configurer la plage d'adresses MAC (Media Access Control)

1. Sur LON-HOST1, ouvrez la console du **Gestionnaire Hyper-V**.
2. Utilisez le Gestionnaire de commutateur virtuel pour configurer les paramètres de plage d'adresse MAC suivants :
   - Minimum : **00-15-5D-0F-AB-A0**
   - Maximum : **00-15-5D-0F-AB-EF**

Résultats : À la fin de cet exercice, vous aurez configuré des options de commutateur virtuel sur un serveur Windows Server 2012 physiquement déployé qui exécute le rôle Hyper-V.

Exercice 3 : Création et configuration d'un ordinateur virtuel

Scénario

Vous devez déployer deux ordinateurs virtuels sur LON-HOST1. Vous avez copié un fichier VHD préparé avec sysprepped qui héberge une installation Windows Server 2012.

Pour réduire l'utilisation de l'espace disque au détriment des performances, vous allez créer deux fichiers VHD de différenciation à partir du fichier VHD préparé avec sysprepped. Vous utiliserez ensuite ces fichiers VHD de différenciation comme fichiers VHD pour les nouveaux ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Créer des disques VHD de différenciation
2. Créer des ordinateurs virtuels
3. Activer le contrôle des ressources

▶ Tâche 1 : Créer des disques VHD de différenciation

1. Utilisez l'Explorateur de fichiers pour créer les deux dossiers suivants :
   - **E:\Program Files\Microsoft Learning\Base\LON-GUEST1**
   - **E:\Program Files\Microsoft Learning\Base\LON-GUEST2**

Remarque : La lettre du lecteur peut être différente selon le nombre de lecteurs sur l'ordinateur hôte physique.

2. Dans la console du Gestionnaire Hyper-V, créez un disque VHD avec les propriétés suivantes :
   - Format du disque : **VHD**
   - Type de disque : **Différenciation**
   - Nom : **LON-GUEST1.vhd**
   - Emplacement : **E:\Program Files\Microsoft Learning\Base\LON-GUEST1**
   - Emplacement du parent : **E:\Program Files\Microsoft Learning\Base\Base12A-WS12-TMP_FR.vhd**
3. Ouvrez **Windows PowerShell**, importez le module de Hyper-V à l'aide de la commande suivante :

```
Import-Module Hyper-V
```

4. Dans Windows PowerShell, exécutez la commande suivante :

```
New-VHD "E:\Program Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd"
-ParentPath "E:\Program Files\Microsoft Learning\Base\Base12A-WS12-TMP_FR.vhd"
```

5. Inspectez le disque **E:\Program Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd**.
6. Vérifiez que **LON-GUEST2.vhd** est configuré en tant que disque VHD de différenciation avec **E:\Program Files\Microsoft Learning\Base\Base12A-WS12-TMP_FR.vhd** comme parent.

▶ Tâche 2 : Créer des ordinateurs virtuels

1. Sur LON-HOST1, dans le volet Actions de la console du Gestionnaire Hyper-V, cliquez sur **Nouveau**, puis sur **Ordinateur virtuel**.
2. Créez un ordinateur virtuel avec les propriétés suivantes :
   - Nom : **LON-GUEST1**
   - Emplacement : **E:\Program Files\Microsoft Learning\Base\LON-GUEST1**
   - Mémoire : **1024 Mo**
   - Utiliser la mémoire dynamique : **Oui**
   - Réseau : **Réseau privé**
   - Connecter un disque dur virtuel : **E:\Program Files\Microsoft Learning\Base\LON-GUEST1\LON-GUEST1.vhd**

3. Ouvrez Windows PowerShell, importez le module de Hyper-V à l'aide de la commande suivante :

```
Import-Module Hyper-V
```

4. Dans Windows PowerShell, exécutez la commande suivante :

```
New-VM -Name LON-GUEST2 -MemoryStartupBytes 1024MB -VHDPath "E:\Program
Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd" -SwitchName "Réseau privé"
```

5. Utilisez la console du Gestionnaire Hyper-V pour modifier les paramètres de LON-GUEST2 en configurant ce qui suit :

- Action de démarrage automatique : **Rien**
- Action d'arrêt automatique **Arrêter le système d'exploitation invité**.

▶ Tâche 3 : Activer le contrôle des ressources

1. À l'invite Windows PowerShell, importez le module Hyper-V.
2. Entrez les commandes suivantes :

```
Enable-VMResourceMetering LON-GUEST1
Enable-VMResourceMetering LON-GUEST2
```

Résultats : À la fin de cet exercice, vous aurez déployé deux ordinateurs virtuels distincts en utilisant un fichier VHD préparé avec sysprepped comme disque parent pour deux disques VHD de différenciation.

Exercice 4 : Utilisation d'instantanés d'ordinateur virtuel

Scénario

Vous êtes en train de développer une stratégie pour atténuer l'impact de demandes de modification incorrectement appliquées. Dans le cadre du développement de cette stratégie, vous testez la vitesse et la fonctionnalité des instantanés d'ordinateur virtuel pour restaurer une configuration stable préalablement existante.

Dans cet exercice, vous allez déployer Windows Server 2012 sur un ordinateur virtuel. Vous créerez ensuite une configuration stable pour cet ordinateur virtuel, et vous prendrez un instantané d'ordinateur virtuel. Enfin, vous modifierez la configuration et vous restaurerez l'instantané.

Les tâches principales de cet exercice sont les suivantes :

1. Déployer Windows Server 2012 sur un ordinateur virtuel
2. Créer un instantané d'ordinateur virtuel
3. Modifier l'ordinateur virtuel
4. Rétablir l'instantané d'ordinateur virtuel existant
5. Afficher les données de contrôle des ressources
6. Rétablir les ordinateurs virtuels

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Déployer Windows Server 2012 sur un ordinateur virtuel

1. Utilisez la console du Gestionnaire Hyper-V pour démarrer **LON-GUEST1**.
2. Ouvrez la fenêtre Connexion à un ordinateur virtuel, puis procédez comme suit pour déployer Windows Server 2012 sur l'ordinateur virtuel :
   - Dans la page **Paramètres**, cliquez sur **Ignorer**.
   - Dans la page **Paramètres**, activez la case à cocher **J'accepte les termes du contrat de licence pour l'utilisation de Windows**, puis cliquez sur **Accepter**.
   - Dans la page **Paramètres**, cliquez sur **Suivant** pour accepter les paramètres **Région et langue**.
   - Dans la page **Paramètres**, entrez le mot de passe **Pa$$w0rd** deux fois, puis cliquez sur **Terminer**.
3. Ouvrez une session sur l'ordinateur virtuel avec le compte **Administrateur** et le mot de passe **Pa$$w0rd**.
4. Réinitialisez le nom de l'ordinateur virtuel sur **LON-GUEST1**, puis redémarrez l'ordinateur virtuel.

▶ Tâche 2 : Créer un instantané d'ordinateur virtuel

1. Connectez-vous à l'ordinateur virtuel **LON-GUEST1**, puis vérifiez que le nom de l'ordinateur est défini sur **LON-GUEST1**.
2. Créez un instantané de **LON-GUEST1**, puis nommez-le **Before Change**.

▶ Tâche 3 : Modifier l'ordinateur virtuel

1. Connectez-vous à l'ordinateur virtuel **LON-GUEST1,** puis utilisez la console du Gestionnaire de serveur pour définir le nom d'ordinateur sur **LON-Computer1**.
2. Redémarrez l'ordinateur virtuel.
3. Connectez-vous à l'ordinateur virtuel **LON-GUEST1**, puis vérifiez que le nom de serveur est défini sur **LON-Computer1**.

▶ Tâche 4 : Rétablir l'instantané d'ordinateur virtuel existant

1. Utilisez la fenêtre Connexion à un ordinateur virtuel pour rétablir l'ordinateur virtuel.
2. Vérifiez que le **Nom de l'ordinateur** de l'ordinateur virtuel est maintenant défini sur **LON-GUEST1**.

▶ Tâche 5 : Afficher les données de contrôle des ressources

1. Sur LON-HOST1, importez le module Hyper-V Windows PowerShell.
2. Tapez la commande suivante :

```
Measure-VM LON-GUEST1
```

3. Notez les chiffres relatifs à l'UC moyenne, à la mémoire vive moyenne et à l'utilisation totale de disque, puis fermez Windows PowerShell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 6 : Rétablir les ordinateurs virtuels

À la fin de cet atelier, redémarrez l'ordinateur dans Windows Server 2008 R2.

1. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. Dans la fenêtre Windows PowerShell, entrez la commande suivante et appuyez sur Entrée :

```
Shutdown /r /t 5
```

3. À partir du Gestionnaire de démarrage Windows, cliquez sur **Windows Server 2008 R2**.

Résultats : À la fin de cet exercice, vous aurez utilisé des instantanés d'ordinateur virtuel pour effectuer une récupération à la suite d'une erreur de configuration d'ordinateur virtuel.

Question : Quel type de commutateur réseau virtuel créeriez-vous pour autoriser l'ordinateur virtuel à communiquer avec le réseau local qui est connecté au serveur de virtualisation Hyper-V ?

Question : Comment pouvez-vous garantir qu'aucun ordinateur virtuel unique n'utilise toute la bande passante disponible fournie par le serveur de virtualisation Hyper-V ?

Question : Quelle tâche de configuration de mémoire dynamique, qui n'était pas possible dans les versions précédentes de Hyper-V, pouvez-vous maintenant effectuer sur un ordinateur virtuel hébergé sur le rôle Hyper-V sur un serveur Windows Server 2012 ?

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
Impossible de déployer Hyper-V sur une plateforme x64.	
L'ordinateur virtuel n'utilise pas la mémoire dynamique.	

Méthode conseillée

Lors de la mise en œuvre de la virtualisation de serveur avec Hyper-V, utilisez les meilleures pratiques suivantes :

- Assurez-vous que le processeur de l'ordinateur qui va exécuter Hyper-V prend en charge la virtualisation assistée par le matériel.
- Assurez-vous qu'un serveur de virtualisation est configuré avec la mémoire vive (RAM) adéquate. Disposer de plusieurs ordinateurs virtuels pour paginer le lecteur de disque dur en raison d'une mémoire inadaptée réduit les performances de tous les ordinateurs virtuels sur le serveur.
- Surveillez avec attention les performances des ordinateurs virtuels. Un ordinateur virtuel qui utilise une quantité démesurée de ressources serveur peut réduire les performances de tous les autres ordinateurs virtuels qui sont hébergés sur le même serveur de virtualisation.

Questions de contrôle des acquis

Question : Dans quelles situations utiliseriez-vous une allocation de mémoire fixe au lieu de mémoire dynamique ?

Question : Dans quelles situations devez-vous utiliser des disques VHD au nouveau format .vhdx au lieu de disques VHD à l'ancien format .vhd ?

Question : Vous souhaitez déployer le disque VHD d'un ordinateur virtuel Hyper-V Windows Server 2012 sur un partage de fichiers. Quel système d'exploitation doit être exécuté par le serveur de fichiers pour la prise en charge de cette configuration ?

Outils

Vous pouvez utiliser les outils suivants avec Hyper-V pour déployer et gérer des ordinateurs virtuels.

Nom de l'outil	Utilisé pour	Emplacement
Outil Sysinternals disk2vhd	Convertir des disques durs physiques au format VHD.	Site Web Microsoft TechNet.

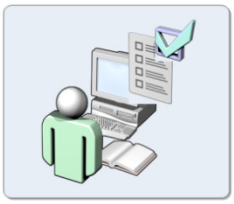
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

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 : Déploiement et gestion de Windows Server 2012

Atelier pratique : Déploiement et gestion de Windows Server 2012

Exercice 1 : Déploiement de Windows Server 2012

▶ Tâche 1 : Installer le serveur Windows Server® 2012

1. Ouvrez la console du **Gestionnaire Hyper-V®**.
2. Cliquez sur **22410B-LON-SVR3**. Dans le volet Actions, cliquez sur **Paramètres**.
3. Sous **Matériel**, cliquez sur **Lecteur de DVD**.
4. Cliquez sur **Fichier image**, puis sur **Parcourir**.
5. Accédez à **C:\Program Files\Microsoft Learning\22410\Drives**, puis cliquez sur **Windows2012_RTM_FR.ISO**.
6. Cliquez sur **Ouvrir**, puis sur **OK**.
7. Dans l'arborescence de la console du Gestionnaire Hyper-V, double-cliquez sur **22410B-LON-SVR3**.
8. Dans la fenêtre Connexion à un ordinateur virtuel, dans le menu **Action**, cliquez sur **Démarrer**.
9. Dans l'Assistant Installation de Windows, dans la page **Windows Server 2012**, vérifiez les paramètres suivants, puis cliquez sur **Suivant**.
   - Langue à installer : **Français (France)**
   - Format horaire et monétaire : **Français (France)**
   - Clavier ou méthode d'entrée : **Français**
10. Dans la page **Windows Server 2012**, cliquez sur **Installer maintenant**.
11. Dans la page **Sélectionner le système d'exploitation à installer**, sélectionnez **Version d'évaluation de Windows Server 2012 Datacenter (serveur avec une interface graphique utilisateur)**, puis cliquez sur **Suivant**.
12. Dans la page **Termes du contrat de licence**, examinez les termes de la licence du système d'exploitation. Activez la case à cocher **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**.
13. Dans la page **Quel type d'installation voulez-vous effectuer ?**, cliquez sur **Personnalisé : installer uniquement Windows (avancé)**.
14. Dans la page **Où souhaitez-vous installer Windows ?**, vérifiez que **Lecteur 0 Espace non alloué** dispose d'assez d'espace pour le système d'exploitation Windows Server 2012, puis cliquez sur **Suivant**.

Remarque : Selon la vitesse du matériel, l'installation prendra approximativement 20 minutes. L'ordinateur virtuel redémarrera plusieurs fois au cours de ce processus.

15. Dans la page **Paramètres**, dans les deux zones **Mot de passe** et **Entrer de nouveau le mot de passe**, entrez le mot de passe **Pa$$w0rd**, puis cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Modifier le nom du serveur

1. Connectez-vous à **LON-SVR3** en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Serveur local**.
3. Cliquez sur le nom généré aléatoirement à côté de **Nom d'ordinateur**.
4. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom d'ordinateur**, cliquez sur **Modifier**.
5. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, dans la zone de texte **Nom d'ordinateur**, entrez le nom **LON-SVR3**, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, cliquez sur **OK**.
7. Fermez la boîte de dialogue **Propriétés système**.
8. Dans la boîte de dialogue **Microsoft Windows**, cliquez sur **Redémarrer maintenant**.

▶ Tâche 3 : Modifier la date et l'heure

1. Connectez-vous au serveur **LON-SVR3** en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur l'affichage de l'heure. Une fenêtre contextuelle contenant un calendrier et une horloge s'affiche.
3. Dans la fenêtre contextuelle, cliquez sur **Modifier les paramètres de la date et de l'heure**.
4. Dans la boîte de dialogue **Date et Heure**, cliquez sur **Changer de fuseau horaire**.
5. Dans la boîte de dialogue **Paramètres de fuseau horaire**, définissez le fuseau horaire sur votre fuseau horaire actuel, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Date et Heure**, cliquez sur **Changer la date et l'heure**.
7. Vérifiez que la date et heure qui s'affichent dans la boîte de dialogue **Réglage de la date et de l'heure** correspondent à la date et l'heure dans la classe, puis cliquez sur **OK**.
8. Cliquez sur **OK** pour fermer la boîte de dialogue **Date et Heure**.

▶ Tâche 4 : Configurer le réseau et l'association de cartes réseau

1. Dans la console du **Gestionnaire de serveur** sur LON-SVR3, cliquez sur **Serveur local**.
2. En regard de la fonction **Association de cartes réseau**, cliquez sur **Désactivé**.
3. Dans la boîte de dialogue **Association de cartes réseau**, maintenez enfoncée la touche **Ctrl** puis, dans l'espace de travail **CARTES ET INTERFACES**, cliquez sur **Connexion au réseau local** et sur **Connexion au réseau local 2**.
4. Cliquez avec le bouton droit sur les cartes réseau sélectionnées, puis cliquez sur **Ajouter à une nouvelle équipe**.
5. Dans la boîte de dialogue **Nouvelle équipe**, dans le champ **Nom de l'équipe**, tapez **LON-SVR3**, puis cliquez sur **OK**.
6. Fermez la boîte de dialogue **Association de cartes réseau**. Actualisez la console du Gestionnaire de serveur.
7. Dans la console du **Gestionnaire de serveur**, à côté de **LON-SVR3**, cliquez sur **Adresse IPv4 attribuée par DHCP, Compatible IPv6**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Dans la boîte de dialogue **Connexions réseau**, cliquez avec le bouton droit sur **LON-SVR3**, puis cliquez sur **Propriétés**.
9. Dans la boîte de dialogue **Propriétés de LON-SVR3**, cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
10. Dans la boîte de dialogue Propriétés de : Protocole Internet version 4 (TCP/IPv4)), entrez les informations d'adresse IP qui suivent, puis cliquez sur **OK** :
    - Adresse IP : **172.16.0.101**
    - Masque de sous-réseau : **255.255.0.0**
    - Passerelle par défaut : **172.16.0.1**
    - Serveur DNS préféré : **172.16.0.10**
11. Cliquez sur **Fermer** pour fermer la boîte de dialogue **Propriétés de LON-SVR3**.
12. Fermez la boîte de dialogue **Connexions réseau**.

▶ Tâche 5 : Ajouter le serveur au domaine

1. Sur LON-SVR3, dans la console du Gestionnaire de serveur, cliquez sur **Serveur local**.
2. À côté de Groupe de travail, cliquez sur **WORKGROUP**.
3. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom d'ordinateur**, cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, dans la zone **Membre d'un**, cliquez sur l'option **Domaine**.
5. Dans la zone **Domaine**, tapez **adatum.com**, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Sécurité de Windows**, entrez les détails suivants, puis cliquez sur **OK** :
    - Nom d'utilisateur : **Administrateur**
    - Mot de passe : **Pa$$w0rd**
7. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, cliquez sur **OK**.
8. Lorsqu'il vous est indiqué que vous devez redémarrer l'ordinateur pour appliquer les modifications, cliquez sur **OK**.
9. Dans la boîte de dialogue **Propriétés système**, cliquez sur **Fermer**.
10. Dans la boîte de dialogue **Microsoft Windows**, cliquez sur **Redémarrer maintenant**.
11. Après le redémarrage de LON-SVR3, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir déployé Windows Server 2012 sur LON-SVR3. Vous devez également avoir configuré LON-SVR3, notamment le changement de nom, la date et l'heure, la mise en réseau et l'association de cartes réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration de l'installation minimale de Windows Server 2012

▶ Tâche 1 : Définir le nom de l'ordinateur

1. Connectez-vous à **LON-CORE** en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez **sconfig.cmd** et appuyez sur Entrée
3. Pour sélectionner **Nom d'ordinateur**, tapez **2** et appuyez sur Entrée.
4. Entrez le nom d'ordinateur **LON-CORE** et appuyez sur Entrée.
5. Dans la boîte de dialogue **Redémarrer**, cliquez sur **Oui**.
6. Connectez-vous au serveur **LON-CORE** à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.
7. À l'invite de commandes, tapez **hostname** et appuyez sur Entrée pour vérifier le nom de l'ordinateur.

▶ Tâche 2 : Changer la date et l'heure de l'ordinateur

1. Vérifiez que vous êtes connecté au serveur LON-CORE en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez **sconfig.cmd**, puis appuyez sur Entrée.
3. Pour sélectionner **Date et Heure**, tapez **9** et appuyez sur Entrée.
4. Dans la boîte de dialogue **Date et Heure**, cliquez sur **Changer de fuseau horaire**. Définissez le fuseau horaire sur celui que votre classe utilise, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Date et Heure**, cliquez sur **Changer la date et l'heure** et vérifiez que la date et heure correspondent à la date et l'heure là où vous vous trouvez. Pour fermer les boîtes de dialogue, cliquez sur **OK** deux fois.
6. Dans la fenêtre d'invite de commandes, tapez **15**, puis appuyez sur Entrée pour quitter **Configuration du serveur**.

▶ Tâche 3 : Configurer le réseau

1. Vérifiez que vous êtes connecté au serveur LON-CORE à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez **sconfig.cmd**, puis appuyez sur Entrée.
3. Pour configurer les **paramètres réseau**, tapez **8**, puis appuyez sur Entrée.
4. Tapez le numéro d'index de la carte réseau que vous souhaitez configurer et appuyez sur Entrée.
5. Dans la page **Paramètres de carte réseau**, tapez **1**, puis appuyez sur Entrée. Ceci définit l'adresse de la carte réseau.
6. Pour sélectionner une configuration d'adresse IP statique, tapez **S**, puis appuyez sur Entrée.
7. À l'invite **Entrer une adresse IP statique :**, tapez **172.16.0.111**, puis appuyez sur Entrée.
8. À l'invite **Entrer un masque de sous-réseau**, tapez **255.255.0.0**, puis appuyez sur Entrée.
9. À l'invite **Entrez la passerelle par défaut**, tapez **172.16.0.1**, puis appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la page **Paramètres de carte réseau**, tapez **2**, puis appuyez sur Entrée. Cela configure l'adresse du serveur DNS.
11. À l'invite **Entrer un nouveau serveur DNS préféré**, tapez **172.16.0.10**, puis appuyez sur Entrée.
12. Dans la boîte de dialogue **Paramètres réseau**, cliquez sur **OK**.
13. Appuyez sur Entrée pour ne pas configurer d'adresse de serveur DNS auxiliaire.
14. Tapez **4** et appuyez sur Entrée pour retourner au menu principal.
15. Tapez **15** et appuyez sur Entrée pour quitter sconfig.cmd.
16. À l'invite de commandes, tapez **ping lon-dc1.adatum.com** pour vérifier la connectivité au contrôleur de domaine à partir de LON-CORE.

▶ Tâche 4 : Ajouter le serveur au domaine

1. Vérifiez que vous êtes connecté au serveur LON-CORE à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.
2. À l'invite de commandes, tapez **sconfig.cmd** et appuyez sur Entrée.
3. Pour basculer vers la configuration de **Domaine ou groupe de travail**, tapez **1**, puis appuyez sur Entrée.
4. Pour joindre un domaine, tapez **D** et appuyez sur Entrée.
5. À l'invite **Nom du domaine à joindre**, tapez **adatum.com** et appuyez sur Entrée.
6. À l'invite **Spécifier un domaine\utilisateur autorisé**, tapez **ADATUM\Administrateur** et appuyez sur Entrée.
7. À l'invite **Tapez le mot de passe associé à l'utilisateur du domaine**, tapez **Pa$$w0rd** et appuyez sur Entrée.
8. À l'invite **Modifier le nom de l'ordinateur**, cliquez sur **Non**.
9. Dans la boîte de dialogue **Redémarrer**, cliquez sur **Oui**.
10. Connectez-vous au serveur LON-CORE à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir configuré un déploiement avec installation minimale de Windows Server 2012 et vérifié le nom du serveur.

Exercice 3 : Gestion des serveurs

▶ Tâche 1 : Créer un groupe de serveurs

1. Connectez-vous à **LON-DC1** à l'aide du compte **Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans la console du Gestionnaire de serveur, cliquez sur **Tableau de bord**, puis cliquez sur **Créer un groupe de serveurs**.
3. Dans la boîte de dialogue **Créer un groupe de serveurs**, cliquez sur l'onglet **Active Directory**, puis sur **Rechercher maintenant**.
4. Dans la zone **Nom du groupe de serveurs**, tapez **LAB-1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR ET UNIQUEMENT

5. Utilisez la flèche pour ajouter **LON-CORE** et **LON-SVR3** au groupe de serveurs. Cliquez sur **OK** pour fermer la boîte de dialogue **Créer un groupe de serveurs**.
6. Dans la console du Gestionnaire de serveur, cliquez sur **LAB-1**. Maintenez enfoncée la touche **Ctrl**, puis sélectionnez **LON-CORE** et **LON-SVR3**.
7. Faites défiler la fenêtre vers le bas et, sous la section **PERFORMANCES**, sélectionnez **LON-CORE** et **LON-SVR3**.
8. Cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Démarrer les compteurs de performances**.

▶ Tâche 2 : Déployer des fonctionnalités et des rôles sur les deux serveurs

1. Dans le Gestionnaire de serveur sur LON-DC1, cliquez sur **LAB-1**.
2. Faites défiler le volet vers le haut, cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, vérifiez que **LON-CORE.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez **Rôle Web Server (IIS)**, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, sélectionnez **Sauvegarde Windows Server**, puis cliquez sur **Suivant**.
8. Dans la page **Rôle Web Server (IIS)**, cliquez sur **Suivant**.
9. Dans la page **Sélectionner des services de rôle**, ajoutez le service de rôle **Authentification Windows**, puis cliquez sur **Suivant**.
10. Dans la page **Confirmer les sélections d'installation**, activez la case à cocher **Redémarrer automatiquement le serveur de destination, si nécessaire**, puis cliquez sur **Installer**.
11. Cliquez sur **Fermer** pour fermer l'Assistant Ajout de rôles et de fonctionnalités.
12. Dans le Gestionnaire de serveur, cliquez avec le bouton droit sur **LON-SVR3**, puis cliquez sur **Ajouter des rôles et des fonctionnalités**.
13. Dans l'Assistant Ajout de rôles et de fonctionnalités, dans la page **Avant de commencer**, cliquez sur **Suivant**.
14. Dans la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou sur une fonctionnalité**. Cliquez sur **Suivant**.
15. Dans la page **Sélectionner le serveur de destination**, vérifiez que **LON-SVR3.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
16. Dans la page **Rôles de serveurs**, cliquez sur **Suivant**.
17. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Sauvegarde Windows Server**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Dans la page **Confirmer les sélections d'installation**, activez la case à cocher **Redémarrer automatiquement le serveur de destination, si nécessaire**, puis cliquez sur **Installer**.
19. Une fois que l'installation a commencé, cliquez sur **Fermer**.
20. Dans le **Gestionnaire de serveur**, cliquez sur le nœud **IIS** et vérifiez que LON-CORE est répertorié.

▶ Tâche 3 : Examiner les services et modifier un paramètre de service

1. Connectez-vous à **LON-CORE** à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans la fenêtre d'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
netsh.exe firewall set service remoteadmin enable ALL
```

3. Connectez-vous à **LON-DC1** à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
4. Dans le Gestionnaire de serveur, cliquez sur **LAB-1**.
5. Cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Gestion de l'ordinateur**.
6. Dans la console Gestion de l'ordinateur, développez **Services et applications**, puis cliquez sur **Services**.
7. Cliquez avec le bouton droit sur le **Service de publication World Wide Web**, puis cliquez sur **Propriétés**. Vérifiez que le paramètre **Type de démarrage** a pour valeur **Automatique**.
8. Dans la boîte de dialogue **Propriétés de Service de publication World Wide Web**, dans l'onglet **Connexion**, vérifiez que le service est configuré pour utiliser le **compte système local**.
9. Dans l'onglet **Récupération**, configurez les paramètres suivants, puis cliquez sur le bouton **Options de redémarrage de l'ordinateur** :
   - Première défaillance : **Redémarrer le service**
   - Deuxième défaillance : **Redémarrer le service**
   - Défaillances suivantes : **Redémarrer l'ordinateur**
   - Réinitialiser le compteur de défaillances après : **1** jours
   - Redémarrer le service après : **1** minute
10. Dans la boîte de dialogue **Options de redémarrage de l'ordinateur**, dans la zone **Redémarrer l'ordinateur après**, tapez **2**, puis cliquez sur **OK**.
11. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de Service de publication World Wide Web**.
12. Fermez la console Gestion de l'ordinateur.

Résultats : À la fin de cet exercice, vous devez avoir créé un groupe de serveurs, déployé des rôles et des fonctionnalités, et configuré les propriétés d'un service.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Utilisation de Windows PowerShell pour gérer les serveurs

▶ Tâche 1 : Utiliser Windows PowerShell® pour se connecter à distance aux serveurs et afficher les informations

1. Connectez-vous à **LON-DC1** à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa$$w0rd**.
2. Dans la console du Gestionnaire de serveur, cliquez sur **LAB-1**.
3. Cliquez avec le bouton droit sur **LON-CORE**, puis cliquez sur **Windows PowerShell**.
4. À l'invite de commandes, tapez **Import-Module ServerManager** et appuyez sur Entrée.
5. Tapez **Get-WindowsFeature** et appuyez sur Entrée pour passer en revue les rôles et les fonctionnalités installés sur LON-CORE.
6. Tapez la commande suivante pour passer en revue les services en cours d'exécution sur LON-CORE, et appuyez sur Entrée :

```
Get-service | where-object {$_.status -eq “Running”}
```

7. Tapez **get-process**, puis appuyez sur Entrée pour afficher la liste des processus sur LON-CORE.
8. Tapez la commande suivante pour passer en revue les adresses IP attribuées au serveur, et appuyez sur Entrée :

```
Get-NetIPAddress | Format-table
```

9. Tapez la commande suivante pour passer en revue les 10 éléments les plus récents dans le journal de sécurité, et appuyez sur Entrée :

```
Get-EventLog Security -Newest 10
```

10. Fermez Windows PowerShell.

▶ Tâche 2 : Utiliser Windows PowerShell pour installer à distance de nouvelles fonctionnalités

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. À l'invite de commandes Windows PowerShell, tapez **import-module ServerManager** et appuyez sur Entrée.
3. Pour vérifier que la fonctionnalité Visionneuse XPS n'a pas été installée sur LON-SVR3, tapez la commande suivante et appuyez sur Entrée :

```
Get-WindowsFeature -ComputerName LON-SVR3
```

4. Pour déployer la fonctionnalité Visionneuse XPS sur LON-SVR3, tapez la commande suivante et appuyez sur Entrée :

```
Install-WindowsFeature XPS-Viewer -ComputerName LON-SVR3
```

5. Pour vérifier que la fonctionnalité Visionneuse XPS est à présent déployée sur LON-SVR3, tapez la commande suivante et appuyez sur Entrée :

```
Get-WindowsFeature -ComputerName LON-SVR3
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la console du **Gestionnaire de serveur**, dans le menu déroulant **Outils**, cliquez sur **Windows PowerShell ISE**.
7. Dans la fenêtre Windows PowerShell ISE, dans le volet de script Untitled1.ps1, tapez ce qui suit en appuyant sur Entrée après chaque ligne :

```
Import-Module ServerManager
Install-WindowsFeature WINS -ComputerName LON-SVR3
Install-WindowsFeature WINS -ComputerName LON-CORE
```

8. Cliquez sur l'icône **Enregistrer**. Sélectionnez la racine de **Disque local (C:)**. Créez un nouveau dossier nommé **Scripts**, puis enregistrez le script dans ce dossier sous le nom **InstallWins.ps1**.
9. Appuyez sur la touche F5 pour exécuter ce script.

Résultats : À la fin de cet exercice, vous devez avoir utilisé Windows PowerShell pour effectuer une installation à distance des fonctionnalités sur plusieurs serveurs.

▶ 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, basculez vers la console du **Gestionnaire Hyper-V®**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-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 **22410B-LON-CORE** et **22410B-LON-SVR3**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2 : Présentation des services de domaine Active Directory

Atelier pratique : Installation de contrôleurs de domaine

Exercice 1 : Installation d'un contrôleur de domaine

▶ Tâche 1 : Ajouter un rôle Services de domaine Active Directory (AD DS) sur un serveur membre

1. Sur LON-DC1, dans le Gestionnaire de serveur, dans la colonne de gauche, cliquez sur **Tous les serveurs**.
2. Cliquez avec le bouton droit sur **Tous les serveurs**, puis cliquez sur **Ajouter des serveurs**.
3. Dans la boîte de dialogue **Ajouter des serveurs**, dans la zone **Nom (CN)**, tapez **LON-SVR1**, puis cliquez sur **Rechercher maintenant**.
4. Sous **Nom**, cliquez sur **LON-SVR1**, puis cliquez sur la flèche pour ajouter le serveur dans la colonne **Sélectionné**.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Ajouter des serveurs**.
6. Dans le Gestionnaire de serveur, dans la fenêtre Serveurs, cliquez avec le bouton droit sur **LON-SVR1**, puis sélectionnez **Ajouter des rôles et des fonctionnalités**.
7. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
8. Dans la fenêtre Sélectionner le type d'installation, assurez-vous que l'option **Installation** basée sur un rôle **ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
9. Dans la page **Sélectionner le serveur de destination**, assurez-vous que l'option **Sélectionner un serveur du pool de serveurs** est sélectionnée. Dans la fenêtre Pool de serveurs, vérifiez que **LON-SVR1.Adatum.com** est en surbrillance, puis cliquez sur **Suivant**.
10. Dans la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services AD DS**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
11. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
12. Sur la page **Services de domaine Active Directory**, cliquez sur **Suivant**.
13. Dans la page **Confirmer les sélections d'installation**, activez la case à cocher **Redémarrer automatiquement le serveur de destination, si nécessaire**, puis cliquez sur **Installer**.
14. L'installation dure quelques minutes. Une fois l'installation terminée, cliquez sur **Fermer** pour fermer l'Assistant Ajout de rôles et de fonctionnalités.

▶ Tâche 2 : Configurer un serveur en tant que contrôleur de domaine

1. Sur LON-DC1, dans le Gestionnaire de serveur, dans la barre de menus, cliquez sur le bouton **Notifications**.
2. Dans la fenêtre Configuration post-déploiement, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
3. Dans l'Assistant Configuration des services de domaine Active Directory, dans la page **Configuration de déploiement**, assurez-vous que la case d'option **Ajouter un contrôleur de domaine à un domaine existant** est sélectionnée, puis, à côté de la ligne **Domaine**, cliquez sur **Sélectionner**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la boîte de dialogue **Sécurité de Windows**, dans la zone **Nom d'utilisateur**, tapez **ADATUM\Administrateur**, puis dans la zone **Mot de passe**, tapez **Pa$$w0rd** et cliquez sur **OK**.
5. Dans la fenêtre Sélectionner un domaine dans la forêt, cliquez sur **Adatum.com**, puis cliquez sur **OK**.
6. Dans la fenêtre Configuration de déploiement, cliquez sur **Suivant**.
7. Dans la page **Options du contrôleur de domaine**, assurez-vous que l'option **Serveur DNS (Domain Name System)** est sélectionnée, puis désactivez la case à cocher à côté de **Catalogue global (GC)**.

Remarque : Vous voudrez généralement également activer le catalogue global, mais dans le cadre de cet atelier pratique, cette opération s'effectue dans la tâche suivante.

8. Dans la section **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**, tapez **Pa$$w0rd** dans les deux zones de texte, puis cliquez sur **Suivant**.
9. Sur la page **Options DNS**, cliquez sur **Suivant**.
10. Sur la page **Options supplémentaires**, cliquez sur **Suivant**.
11. Dans la page **Chemins d'accès**, acceptez les dossiers par défaut, puis cliquez sur **Suivant**.
12. Dans la page **Examiner les options**, cliquez sur **Afficher le script** et examinez le script Windows PowerShell que l'Assistant génère. Fermez le Bloc-notes.
13. Sur la page **Examiner les options**, cliquez sur **Suivant**.
14. Dans la page **Vérification de la configuration requise**, lisez tous les messages d'avertissement, puis cliquez sur **Installer**.
15. Lorsque la tâche se termine correctement, cliquez sur **Fermer**.
16. Attendez que le serveur redémarre.

▶ Tâche 3 : Configurer un serveur en tant que serveur de catalogue global

1. Connectez-vous à LON-SVR1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
3. Quand la fenêtre Sites et services Active Directory s'ouvre, développez **Sites**, développez **Default-First-Site-Name**, développez **Servers**, puis développez **LON-SVR1**.
4. Dans la colonne gauche, cliquez avec le bouton droit sur **NTDS Settings**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de : NTDS Settings**, activez la case à cocher **Catalogue global**, puis cliquez sur **OK**.
6. Fermez la console Sites et services Active Directory.

Résultats : À la fin de cet exercice, vous devez avoir exploré le Gestionnaire de serveur et promu un serveur membre en tant que contrôleur de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Installation d'un contrôleur de domaine selon la méthode IFM

▶ Tâche 1 : Utiliser l'outil Ntdsutil pour générer IFM

1. Sur LON-DC1, pointez dans le coin inférieur droit de l'écran d'accueil, puis cliquez sur l'icône **Accueil** lorsqu'elle apparaît.
2. Dans l'écran d'accueil, tapez **CMD**, puis appuyez sur Entrée.
3. À une invite de commandes, tapez les commandes ci-dessous en appuyant sur Entrée après chaque ligne :

```
Ntdsutil
Activate instance ntds
Ifm
Create sysvol full c:\ifm
```

▶ Tâche 2 : Ajouter le rôle AD DS sur le serveur membre

1. Basculez vers LON-SVR2 et, si nécessaire, connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Pointez dans le coin inférieur droit du Bureau et cliquez sur l'icône **Accueil** lorsqu'elle apparaît.
3. Dans l'écran d'accueil, tapez **CMD**, puis appuyez sur Entrée.
4. Tapez la commande suivante, puis appuyez sur Entrée :

```
Net use k: \\LON-DC1\c$\IFM
```

5. Basculez vers le **Gestionnaire de serveur**.
6. Dans la liste gauche, cliquez sur **Serveur local**.
7. Dans la barre d'outils, cliquez sur **Gérer**, puis cliquez sur **Ajouter des rôles et des fonctionnalités**.
8. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
9. Dans la page **Sélectionner le type d'installation**, assurez-vous que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
10. Dans la page **Sélectionner le serveur de destination**, vérifiez que **LON-SVR2.Adatum.com** est en surbrillance, puis cliquez sur **Suivant**.
11. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Services de domaine Active Directory**.
12. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
13. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
14. Sur la page **Services de domaine Active Directory**, cliquez sur **Suivant**.
15. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Redémarrer automatiquement le serveur de destination, si nécessaire**. Cliquez sur **Oui** dans le message qui s'affiche.
16. Cliquez sur **Installer**.
17. Une fois l'installation terminée, cliquez sur **Fermer**.

Remarque : Si un message s'affiche stipulant qu'il est impossible de créer une délégation pour le serveur DNS, cliquez sur **OK**.

▶ Tâche 3 : Utilisez l'option IFM pour configurer un serveur membre comme nouveau contrôleur de domaine

1. Sur LON-SVR2, ouvrez une fenêtre d'invite de commandes.
2. À l'invite de commandes, tapez les commandes suivantes et appuyez sur Entrée :

```
Robocopy k: c:\ifm /copyall /s
```

3. Fermez la fenêtre d'invite de commandes.
4. Dans la barre d'outils du Gestionnaire de serveur, cliquez sur le bouton **Notifications**.
5. Dans la fenêtre Configuration post-déploiement, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
6. Dans la page **Configuration de déploiement**, assurez-vous que l'option **Ajouter un contrôleur de domaine à un domaine existant** est sélectionnée et confirmez que **Adatum.com** est le domaine cible. Cliquez sur **Suivant**.
7. Dans la page **Options du contrôleur de domaine**, assurez-vous que les options **Serveur DNS (Domain Name System)** et **Catalogue global** sont sélectionnées. Pour le mot de passe **DSRM**, entrez **Pa$$w0rd** dans les deux zones, puis cliquez sur **Suivant**.
8. Sur la page **Options DNS**, cliquez sur **Suivant**.
9. Dans la page **Options supplémentaires**, activez la case à cocher **Installation à partir du support**, dans la zone de texte, tapez **C:\ifm**, puis cliquez sur **Vérifier**.
10. Une fois le chemin d'accès vérifié, cliquez sur **Suivant**.
11. Sur la page **Chemins d'accès**, cliquez sur **Suivant**.
12. Dans la page **Examiner les options**, cliquez sur **Suivant**, puis observez l'Assistant Configuration des services de domaine Active Directory lorsqu'il effectue la vérification des conditions préalables.
13. Cliquez sur **Installer** et patientez pendant qu'AD DS est configuré. Pendant que cette tâche s'exécute, lisez les messages d'information qui s'affichent à l'écran.
14. Attendez que le serveur redémarre.

Résultats : À la fin de cet exercice, vous devez avoir installé un contrôleur de domaine supplémentaire pour la filiale en utilisant l'option IFM.

▶ 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 **22410B-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 **22410B-LON-SVR1**, **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3 : Gestion des objets de services de domaine Active Directory

Atelier pratique : Gestion des objets de services de domaine Active Directory

Exercice 1 : Délégation de l'administration pour une succursale

▶ Tâche 1 : Déléguer l'administration pour les administrateurs d'une filiale

1. Basculez vers **LON-DC1**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez sur **Adatum.com**.
4. Cliquez avec le bouton droit sur **Adatum.com**, pointez la souris sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
5. Dans la boîte de dialogue **Nouvel objet – Unité d'organisation**, dans la zone **Nom**, saisissez **Filiale 1**, puis cliquez sur **OK**.
6. Cliquez avec le bouton droit sur **Filiale 1**, pointez sur **Nouveau**, puis cliquez sur **Groupe**.
7. Dans la boîte de dialogue **Nouvel objet – Groupe**, dans la zone **Nom du groupe**, tapez **Assistance technique Filiale 1**, puis cliquez sur **OK**.
8. Cliquez avec le bouton droit sur **Filiale 1**, pointez sur **Nouveau**, puis cliquez sur **Groupe**.
9. Dans la boîte de dialogue **Nouvel objet – Groupe**, dans la zone **Nom du groupe**, tapez **Administrateurs Filiale 1**, puis cliquez sur **OK**.
10. Cliquez avec le bouton droit sur **Filiale 1**, pointez sur **Nouveau**, puis cliquez sur **Groupe**.
11. Dans la boîte de dialogue **Nouvel objet – Groupe**, dans la zone **Nom du groupe**, tapez **Utilisateurs Filiale 1,** puis cliquez sur **OK**.
12. Dans le volet de navigation, cliquez sur **IT**.
13. Dans le volet d'informations, cliquez avec le bouton droit sur **Holly Dickson**, puis cliquez sur **Déplacer**.
14. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
15. Dans le volet de navigation, cliquez sur l'unité d'organisation **Development**.
16. Dans le volet d'informations, cliquez avec le bouton droit sur **Bart Duncan**, puis cliquez sur **Déplacer**.
17. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
18. Dans le volet de navigation, cliquez sur l'unité d'organisation **Managers**.
19. Dans le volet d'informations, cliquez avec le bouton droit sur **Ed Meadows**, puis cliquez sur **Déplacer**.
20. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
21. Dans le volet de navigation, cliquez sur l'unité d'organisation **Marketing**.
22. Dans le volet d'informations, cliquez avec le bouton droit sur **Connie Vrettos**, puis cliquez sur **Déplacer**.

23. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
24. Dans le volet de navigation, cliquez sur l'unité d'organisation **Research**.
25. Dans le volet d'informations, cliquez avec le bouton droit sur **Barbara Zighetti**, puis cliquez sur **Déplacer**.
26. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
27. Dans le volet de navigation, cliquez sur l'unité d'organisation **Sales**.
28. Dans le volet d'informations, cliquez avec le bouton droit sur **Arlene Huff**, puis cliquez sur **Déplacer**.
29. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
30. Dans le volet de navigation, cliquez sur **Filiale 1**.
31. Dans le volet de navigation, cliquez sur **Computers**.
32. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-CL1**, puis cliquez sur **Déplacer**.
33. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
34. Basculez vers **LON-CL1**.
35. Suspendez votre pointeur de la souris dans le coin inférieur droit de l'écran, puis cliquez sur **Paramètres**.
36. Cliquez sur **Marche/Arrêt**, puis sur **Redémarrer**.
37. Lorsque l'ordinateur est redémarré, ouvrez une session en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
38. Basculez vers **LON-DC1**.
39. Si nécessaire, basculez vers **Utilisateurs et ordinateurs Active Directory**.
40. Dans le volet de détails, cliquez avec le bouton droit sur **Filiale 1**, cliquez sur **Délégation de contrôle...**, puis sur **Suivant**.
41. Dans la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.
42. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs ou des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Administrateurs Filiale 1**, puis cliquez sur **OK**.
43. Dans la page **Utilisateurs ou groupes**, cliquez sur **Suivant**.
44. Dans la page **Tâches à déléguer**, dans la liste **Déléguer les tâches courantes suivantes**, activez les cases à cocher, puis cliquez sur **Suivant**.
    - **Créer, supprimer et gérer les comptes d'utilisateurs**
    - **Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session**
    - **Lire toutes les informations sur l'utilisateur**
    - **Créer, supprimer et gérer les groupes**
    - **Modifier l'appartenance à un groupe**
    - **Gérer les liens de stratégie de groupe**
45. Dans la page **Fin de l'Assistant Délégation de contrôle**, cliquez sur **Terminer**.
46. Dans le volet de détails, cliquez avec le bouton droit sur **Filiale 1**, cliquez sur **Délégation de contrôle...**, puis sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

47. Dans la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.
48. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs ou des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Administrateurs Filiale 1**, puis cliquez sur **OK**.
49. Dans la page **Utilisateurs ou groupes**, cliquez sur **Suivant**.
50. Dans la page **Tâches à déléguer**, cliquez sur **Créer une tâche personnalisée à déléguer**, puis sur **Suivant**.
51. Dans la page **Type d'objet Active Directory**, sélectionnez **Seulement des objets suivants dans le dossier**, activez les cases à cocher suivantes, puis cliquez **Suivant** :
    - **Objets Ordinateur**
    - **Créer les objets sélectionnés dans ce dossier**
    - **Supprimer les objets sélectionnés dans ce dossier**
52. Dans la page **Autorisations**, activez les cases à cocher **Générales** et **Contrôle total**, puis cliquez sur **Suivant**.
53. Dans la page **Fin de l'Assistant Délégation de contrôle**, cliquez sur **Terminer**.

▶ Tâche 2 : Déléguer un administrateur pour l'assistance technique de la filiale

1. Sur LON-DC1, dans le volet de détails, cliquez avec le bouton droit sur **Filiale 1**, cliquez sur **Délégation de contrôle**, puis sur **Suivant**.
2. Dans la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs ou des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Assistance technique Filiale 1**, puis cliquez sur **OK**.
4. Dans la page **Utilisateurs ou groupes**, cliquez sur **Suivant**.
5. Dans la page **Tâches à déléguer**, dans la liste **Déléguer les tâches courantes suivantes**, activez les cases à cocher, puis cliquez sur **Suivant**.
    - **Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session ;**
    - **Lire toutes les informations sur l'utilisateur ;**
    - **Modifier l'appartenance à un groupe ;**
6. Dans la page **Fin de l'Assistant Délégation de contrôle**, cliquez sur **Terminer**.

▶ Tâche 3 : Ajouter un membre aux Administrateurs de la filiale

1. Sur LON-DC1, dans le volet de navigation, cliquez sur **Filiale 1**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur **Holly Dickson**, puis cliquez sur **Ajouter à un groupe**.
3. Dans la boîte de dialogue **Sélectionnez des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Administrateurs Filiale 1**, puis cliquez sur **OK**.
4. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**.
5. Dans le volet d'informations, cliquez avec le bouton droit sur **Administrateurs Filiale 1**, puis cliquez sur **Ajouter à un groupe**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la boîte de dialogue **Sélectionnez des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Opérateurs de serveur**, puis cliquez sur **OK**.
7. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**.
8. Sur votre ordinateur hôte, dans la fenêtre 22410B-LON-DC1, dans le menu **Action**, cliquez sur **Ctrl+Alt+Suppr**.
9. Sur LON-DC1, cliquez sur **Se déconnecter**.
10. Connectez-vous à LON-DC1 en tant que **ADATUM\Holly** avec le mot de passe **Pa$$w0rd**. Vous pouvez ouvrir une session localement sur un contrôleur de domaine car Holly appartient indirectement au groupe local de domaine Opérateurs de serveur.
11. Sur le bureau, dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
12. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, dans la zone **Nom d'utilisateur**, tapez **Holly**. Dans la zone **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Oui**.
13. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
14. Dans **Utilisateurs et ordinateurs Active Directory**, développez **Adatum.com**.
15. Dans le volet de navigation, cliquez sur **Sales**.
16. Dans le volet d'informations, cliquez avec le bouton droit sur **Aaren Ekelund**, puis cliquez sur **Supprimer**.
17. Cliquez sur **Oui** pour confirmer.
18. Cliquez sur **OK** pour reconnaître que vous n'avez pas les autorisations nécessaires pour effectuer cette tâche.
19. Dans le volet de navigation, cliquez sur **Filiale 1**.
20. Dans le volet d'informations, cliquez avec le bouton droit sur **Ed Meadows**, puis cliquez sur **Supprimer**.
21. Cliquez sur **Oui** pour confirmer. L'opération réussit car vous disposez des autorisations requises.

▶ Tâche 4 : Ajouter un membre au groupe d'assistance technique de la filiale

1. Sur LON-DC1, dans le volet d'informations, cliquez avec le bouton droit sur **Bart Duncan**, puis cliquez sur **Ajouter à un groupe**.
2. Dans la boîte de dialogue **Sélectionnez des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Assistance technique Filiale 1**, puis cliquez sur **OK**.
3. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**.
4. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.
5. Fermez le Gestionnaire de serveur.
6. Sur le Bureau, cliquez sur **Gestionnaire de serveur**.
7. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, dans la zone **Nom d'utilisateur**, tapez **ADATUM\Administrateur**. Dans la zone **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Oui**.

Remarque : Pour modifier la liste des membres du groupe Opérateurs de serveur, vous devez disposer des autorisations supérieures à celles du groupe Administrateurs Filiale 1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**.
9. Dans la liste **Outils**, cliquez sur **Utilisateurs et ordinateurs Active Directory**.
10. Dans **Utilisateurs et ordinateurs Active Directory**, **Adatum.com** est déjà développé.
11. Dans le volet de navigation, cliquez sur **Filiale 1**.
12. Dans le volet d'informations, cliquez avec le bouton droit sur **Assistance technique Filiale 1**, puis cliquez sur **Ajouter à un groupe**.
13. Dans la boîte de dialogue **Sélectionnez des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Opérateurs de serveur**, puis cliquez sur **OK**.
14. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**.
15. Sur votre ordinateur hôte, dans la fenêtre 22410B-LON-DC1, dans le menu **Action**, cliquez sur **Ctrl+Alt+Suppr**.
16. Sur LON-DC1, cliquez sur **Se déconnecter**.
17. Connectez-vous en tant que **ADATUM\Bart** avec le mot de passe **Pa$$w0rd**. Vous pouvez ouvrir une session localement sur un contrôleur de domaine car Bart appartient, indirectement, au groupe local de domaine Opérateurs de serveur.
18. Sur le Bureau, cliquez sur **Gestionnaire de serveur**.
19. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, dans la zone **Nom d'utilisateur**, tapez **Bart**. Dans la zone **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Oui**.
20. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**.
21. Cliquez sur **Utilisateurs et ordinateurs Active Directory**.
22. Dans **Utilisateurs et ordinateurs Active Directory**, **Adatum.com** est déjà développé.
23. Dans le volet de navigation, cliquez sur **Filiale 1**.
24. Dans le volet d'informations, cliquez avec le bouton droit sur **Connie Vrettos**, puis cliquez sur **Supprimer**.
25. Cliquez sur **Oui** pour confirmer. L'opération échoue car Bart ne dispose pas des autorisations requises. Cliquez sur **OK**.
26. Cliquez avec le bouton droit sur **Connie Vrettos**, puis cliquez sur **Réinitialiser le mot de passe**.
27. Dans la boîte de dialogue **Réinitialiser le mot de passe**, tapez **Pa$$w0rd** dans les zones **Nouveau mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **OK**.
28. Cliquez sur **OK** pour confirmer la réinitialisation du mot de passe.
29. Sur votre ordinateur hôte, dans la fenêtre 22410B-LON-DC1, dans le menu **Action**, cliquez sur **Ctrl+Alt+Suppr**.
30. Sur LON-DC1, cliquez sur **Se déconnecter**.
31. Ouvrez une session sur LON-DC1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir créé une unité d'organisation et délégué son administration au groupe compétent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Création et configuration de comptes d'utilisateurs dans AD DS

▶ Tâche 1 : Créer un modèle utilisateur pour la filiale

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône de l' Explorateur de fichiers.
2. Cliquez sur **Bureau**, puis double-cliquez sur **Ordinateur**.
3. Double-cliquez sur **Disque local (C:)**.
4. Dans le menu, cliquez sur **Nouveau dossier**.
5. Tapez **branch1-userdata**, puis appuyez sur Entrée.
6. Cliquez avec le bouton droit sur **branch1-userdata**, puis cliquez sur **Propriétés**.
7. Dans la boîte de dialogue **Propriétés de : branch1-userdata**, dans l'onglet **Partage**, cliquez sur **Partage avancé**.
8. Activez la case à cocher **Partager ce dossier**, puis cliquez sur **Autorisations**.
9. Dans la boîte de dialogue **Autorisations pour branch1-userdata**, activez la case à cocher **Autoriser Contrôle total**, puis cliquez sur **OK**.
10. Dans la boîte de dialogue **Partage avancé**, cliquez sur **OK**, puis dans la boîte de dialogue **Propriétés de branch1-userdata**, cliquez sur **Fermer**.
11. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. **Adatum.com** est déjà développé.
12. Cliquez avec le bouton droit sur **Filiale 1**, pointez sur **Nouveau**, puis cliquez sur **Utilisateur**.
13. Dans la boîte de dialogue **Nouvel objet – Utilisateur**, dans la zone **Nom complet**, tapez_**Branch_template**.
14. Dans la zone **Nom d'ouverture de session de l'utilisateur**, tapez **Branch_template**, puis cliquez sur **Suivant**.
15. Dans les zones **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**.
16. Activez la case à cocher **Le compte est désactivé**, puis cliquez sur **Suivant**.
17. Cliquez sur **Terminer**.

▶ Tâche 2 : Configurer les paramètres du modèle

1. Sur LON-DC1, à partir de l'unité d'organisation **Filiale 1**, cliquez avec le bouton droit sur **_Branch_template**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de _Branch_template**, sur l'onglet **Adresse**, dans la zone **Ville**, tapez **Slough**.
3. Cliquez sur l'onglet **Membre de**, puis cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Sélectionnez des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **Utilisateurs Filiale 1**, puis cliquez sur **OK**.
5. Cliquez sur l'onglet **Profil**.
6. Sous le Dossier de base, cliquez sur **Connecter**, et dans la zone **à**, saisissez **\\lon-dc1\branch1-userdata\%username%**.
7. Cliquez sur **Appliquer**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Créer un utilisateur pour la filiale d'après le modèle

1. Sur LON-DC1, Cliquez avec le bouton droit sur **_Branch_template**, puis cliquez sur **Copier**.
2. Dans la boîte de dialogue **Copier l'objet – Utilisateur**, dans la zone **Prénom**, tapez **Ed**.
3. Dans la zone **Nom**, tapez **Meadows**.
4. Dans la zone **Nom d'ouverture de session de l'utilisateur**, tapez **Ed**, puis cliquez sur **Suivant**.
5. Dans les zones **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**.
6. Désactivez la case à cocher **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**.
7. Désactivez la case à cocher **Le compte est désactivé**, puis cliquez sur **Suivant**.
8. Cliquez sur **Terminer**.
9. Cliquez avec le bouton droit sur **Ed Meadows**, puis cliquez sur **Propriétés**.
10. Dans la boîte de dialogue **Propriétés de Ed Meadows**, cliquez sur l'onglet **Adresse**. Notez que la ville est déjà configurée.
11. Cliquez sur l'onglet **Profil**. Remarquez que l'emplacement du dossier de base est déjà configuré
12. Sélectionnez l'onglet **Membre de**. Remarquez qu'Ed appartient au groupe Utilisateurs Filiale 1. Cliquez sur **OK**.
13. Sur votre ordinateur hôte, dans la fenêtre 22410B-LON-DC1, dans le menu **Action**, cliquez sur **Ctrl+Alt+Suppr**.
14. Sur LON-DC1, cliquez sur **Se déconnecter**.

▶ Tâche 4 : Se connecter en tant qu'utilisateur pour tester les paramètres de compte

1. Basculez vers **LON-CL1**.
2. Sur votre ordinateur hôte, dans la fenêtre 22410B-LON-CL1, dans le menu, cliquez sur **Ctrl+Alt+Suppr**.
3. Sur LON-CL1, cliquez sur **Se déconnecter**.
4. Ouvrez une session sur LON-CL1 en tant que **ADATUM\Ed** avec le mot de passe **Pa$$w0rd**.
5. Sur l'écran Accueil, cliquez sur **Bureau**.
6. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
7. Dans le volet de navigation, cliquez sur **Bureau**, puis, dans le volet d'informations, double-cliquez sur **Ordinateur**.
8. Vérifiez que le lecteur Z est mappé à **Ed (\\lon-dc1\branch1-userdata) (Z:)**.
9. Double-cliquez sur **Ed (\\lon-dc1\branch1-userdata) (Z:)**.
10. Si vous ne recevez aucune erreur, l'opération a réussi.
11. Sur votre ordinateur hôte, dans la fenêtre 22410B-LON-CL1, dans le menu **Action**, cliquez sur **Ctrl+Alt+Suppr**.
12. Sur LON-CL1, cliquez sur **Se déconnecter**.

Résultats : À la fin de cet exercice, vous devez avoir créé et testé un compte d'utilisateur créé à partir d'un modèle.

Exercice 3 : Gestion des objets ordinateur dans AD DS

▶ Tâche 1 : Réinitialiser un compte d'ordinateur

1. Sur LON-DC1, ouvrez une session en tant que **ADATUM\Holly** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
3. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, dans la zone **Nom d'utilisateur**, tapez **Holly**. Dans la zone **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Oui**.
4. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
5. Dans **Utilisateurs et ordinateurs Active Directory**, **Adatum.com** est déjà développé.
6. Dans le volet de navigation, cliquez sur **Filiale 1**.
7. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-CL1**, puis cliquez sur **Réinitialiser le compte**.
8. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **Oui**, puis sur **OK**.

▶ Tâche 2 : Observer le comportement quand un client ouvre une session

1. Basculez vers **LON-CL1**.
2. Connectez-vous en tant que **ADATUM\Ed** avec le mot de passe **Pa$$w0rd**.
3. Un message s'affiche indiquant **La relation d'approbation entre cette station de travail et le domaine principal a échoué**.
4. Cliquez sur **OK**.

▶ Tâche 3 : Joindre à nouveau le domaine pour reconnecter le compte d'ordinateur

1. Ouvrez une session sur **LON-CL1** en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran Accueil, cliquez avec le bouton droit, cliquez sur **Toutes les applications**, puis dans la liste **Applications**, cliquez sur **Panneau de configuration**.
3. Dans le **Panneau de configuration**, dans la liste **Afficher par**, cliquez sur **Grandes icônes**, puis sur **Système**.
4. Dans la liste de navigation, cliquez sur **Paramètres système avancés**.
5. Dans la boîte de dialogue **Propriétés système**, cliquez sur l'onglet **Nom de l'ordinateur**, puis sur **Identité sur le réseau**.
6. Dans la page **Sélectionnez l'option qui décrit votre réseau**, cliquez sur **Suivant**.
7. Dans la page **Le réseau de votre entreprise appartient-il à un domaine**, cliquez sur **Suivant**.
8. Dans la page **Vous aurez besoin des informations suivantes**, cliquez sur **Suivant**.
9. Dans la page **Entrez vos nom d'utilisateur, mot de passe et nom de domaine pour votre compte de domaine**, dans la zone **Mot de passe**, tapez **Pa$$w0rd**. Ne modifiez pas les autres champs, puis cliquez sur **Suivant**.
10. Dans la boîte de dialogue **Informations sur le domaine et le compte d'utilisateur**, cliquez sur **Oui**.
11. Dans la page **Voulez-vous activer un compte d'utilisateur de domaine sur cet ordinateur**, cliquez sur **Ne pas ajouter de compte d'utilisateur de domaine**, puis sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

12. Cliquez sur **Terminer**, puis sur **OK**.
13. Dans la boîte de dialogue **Microsoft Windows**, cliquez sur **Redémarrer maintenant**.
14. Ouvrez une session en tant que **ADATUM\Ed** avec le mot de passe **Pa$$w0rd**. L'opération réussit car la jonction de l'ordinateur a été rétablie correctement.

Résultats : À la fin de cet exercice, vous devez avoir réinitialisé avec succès une relation d'approbation.

▶ 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 **22410B-LON-CL1**, 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 **22410B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4 : Automatisation de l'administration des domaines de services Active Directory

Atelier pratique : Automatisation de l'administration d'AD DS à l'aide de Windows PowerShell

Exercice 1 : Création de comptes d'utilisateurs et de groupes à l'aide de Windows PowerShell

▶ Tâche 1 : Créer un compte d'utilisateur à l'aide de Windows PowerShell

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell®**.
2. À l'invite Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
New-ADOrganizationalUnit LondonBranch
```

3. Tapez la commande suivante, puis appuyez sur Entrée :

```
New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path
"ou=LondonBranch,dc=adatum,dc=com"
```

4. Tapez la commande suivante, puis appuyez sur Entrée :

```
Set-ADAccountPassword Ty
```

5. Lorsque vous êtes invité à entrer le mot de passe actuel, appuyez sur Entrée.
6. Lorsque vous êtes invité à entrer le mot de passe souhaité, tapez **Pa$$w0rd**, puis appuyez sur Entrée.
7. Lorsque vous êtes invité à entrer à nouveau le mot de passe, tapez **Pa$$w0rd**, puis appuyez sur Entrée.
8. À l'invite Windows PowerShell, tapez **Enable-ADAccount Ty**, puis appuyez sur Entrée.
9. Sur LON-CL1, connectez-vous en tant que **Ty** à l'aide du mot de passe **Pa$$w0rd**.
10. Vérifiez que la connexion est réussie, puis déconnectez-vous de LON-CL1.

▶ Tâche 2 : Créer un groupe à l'aide de Windows PowerShell

1. Sur LON-DC1, à l'invite Windows PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
New-ADGroup LondonBranchUsers -Path "ou=LondonBranch,dc=adatum,dc=com" -GroupScope
Global -GroupCategory Security
```

2. Tapez la commande suivante, puis appuyez sur Entrée :

```
Add-ADGroupMember LondonBranchUsers -Members Ty
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-ADGroupMember LondonBranchUsers
```

Résultats : À la fin de cet exercice, vous devez avoir créé des comptes d'utilisateurs et des groupes à l'aide de Windows PowerShell.

Exercice 2 : Utilisation de Windows PowerShell pour créer des comptes d'utilisateurs en bloc

▶ Tâche 1 : Préparer le fichier .csv

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
2. Dans la fenêtre de l'Explorateur de fichiers, développez **E:**, développez **Labfiles**, puis cliquez sur **Mod04**.
3. Cliquez avec le bouton droit sur **LabUsers.ps1**, puis cliquez sur **Modifier**.
4. Dans l'environnement d'écriture de scripts intégré (ISE) de Windows PowerShell, lisez les commentaires en haut du script, puis identifiez les conditions requises pour l'en-tête du fichier .csv.
5. Fermez Windows PowerShell ISE.
6. Dans l'Explorateur de fichiers, double-cliquez sur **LabUsers.csv**.
7. Dans la fenêtre Comment souhaitez-vous ouvrir ce type de fichier (.csv), cliquez sur **Bloc-notes**.
8. Dans le Bloc-notes, tapez la ligne suivante en haut du fichier : **FirstName,LastName,Department,DefaultPassword**
9. Cliquez sur **Fichier**, puis sur **Enregistrer**.
10. Fermez le Bloc-notes.

▶ Tâche 2 : Préparer le script

1. Sur LON-DC1, dans l'Explorateur de fichiers, cliquez avec le bouton droit sur **LabUsers.ps1**, puis cliquez sur **Modifier**.
2. Dans Windows PowerShell ISE, sous Variables, remplacez **C:\chemin d'accès\file.csv** par **E:\Labfiles\Mod04\LabUsers.csv**.
3. Sous Variables, remplacez **"ou=orgunit,dc=domain,dc=com"** par **"ou=LondonBranch,dc=adatum,dc=com"**.
4. Cliquez sur **Fichier**, puis sur **Enregistrer**.
5. Faites défiler vers le bas et examinez le contenu du script.
6. Fermez Windows PowerShell ISE.

▶ Tâche 3 : Exécuter le script

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. À l'invite Windows PowerShell, tapez **cd E:\Labfiles\Mod04**, puis appuyez sur Entrée.
3. Tapez **.\LabUsers.ps1**, puis appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com"
```

5. Fermez l'invite Windows PowerShell.
6. Sur LON-CL1, connectez-vous en tant que **Luka** à l'aide du mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devez avoir utilisé Windows PowerShell pour créer des comptes d'utilisateurs en bloc.

Exercice 3 : Utilisation de Windows PowerShell pour modifier des comptes d'utilisateurs en bloc

▶ Tâche 1 : Forcer tous les comptes d'utilisateurs de LondonBranch à changer leur mot de passe à la prochaine connexion

1. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. À l'invite Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com" | Format-Wide
DistinguishedName
```

3. Vérifiez que seuls les utilisateurs de l'unité d'organisation **LondonBranch** sont répertoriés.
4. À l'invite Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com" | Set-ADUser -
ChangePasswordAtLogon $true
```

5. Fermez Windows PowerShell.

▶ Tâche 2 : Configurer l'adresse pour les comptes d'utilisateurs de LondonBranch

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, développez **Adatum (local)** et double-cliquez sur **LondonBranch**.
3. Cliquez sur l'en-tête de colonne **Type** pour effectuer un tri selon le type d'objet.
4. Sélectionnez tous les comptes d'utilisateurs, cliquez avec le bouton droit sur ces comptes, puis cliquez sur **Propriétés**.
5. Dans la fenêtre Plusieurs utilisateurs, sous **Organisation**, activez la case à cocher **Adresse**.
6. Dans la zone **Rue**, tapez **Filiale**.
7. Dans la zone **Ville**, tapez **Londres**.
8. Dans la zone **Pays/région**, cliquez sur **Royaume-Uni**, puis sur **OK**.
9. Fermez le Centre d'administration Active Directory.

Résultats : À la fin de cet exercice, vous devez avoir modifié des comptes d'utilisateurs en bloc.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Pour préparer le module suivant

Lorsque vous terminez l'atelier pratique, rétablissez tous les ordinateurs virtuels à leur état initial en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-LON-CL1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22410B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5 : Implémentation du protocole IPv4

Atelier pratique : Implémentation du protocole IPv4

Exercice 1 : Identification des sous-réseaux appropriés

▶ Tâche 1 : Calculer les bits requis pour prendre en charge les hôtes sur chaque sous-réseau

1. Combien de bits sont requis pour prendre en charge 100 hôtes sur le sous-réseau client ?

   Sept bits sont requis pour prendre en charge 100 hôtes sur le sous-réseau client (2^7-2=126, 2^6-2=62).

2. Combien de bits sont requis pour prendre en charge 10 hôtes sur le sous-réseau serveur ?

   Quatre bits sont requis pour prendre en charge 10 hôtes sur le sous-réseau serveur (2^4-2=14,2^3-2=6).

3. Combien de bits sont requis pour prendre en charge 40 hôtes sur le sous-réseau de l'extension future ?

   Six bits sont requis pour prendre en charge 40 hôtes sur le sous-réseau de l'extension future (2^6-2=62, 2^5-2=30).

4. Si tous les sous-réseaux sont de la même taille, peuvent-ils être adaptés ?

   Non, si tous les sous-réseaux sont de la même taille, ils doivent tous utiliser 7 bits pour prendre en charge 126 hôtes. Seule une adresse de classe C comprenant 254 hôtes a été allouée. Trois sous-réseaux de 126 hôtes ne conviennent pas.

5. Quelle fonctionnalité permet à un réseau unique d'être divisé en sous-réseaux de différentes tailles ?

   La création d'un masque de sous-réseau de longueur variable vous permet de définir des masques de sous-réseau distincts lors de la création de sous-réseaux. Par conséquent, la création d'un masque de sous-réseau de longueur variable vous permet d'avoir des sous-réseaux de différentes tailles.

6. Combien de bits hôtes utiliserez-vous pour chaque sous-réseau ? Utilisez l'allocation la plus simple possible, c'est-à-dire un sous-réseau de grande taille et deux sous-réseaux plus petits de même taille.

   Le sous-réseau client est de 7 bits hôtes. Cela permet d'avoir jusqu'à 126 hôtes et d'utiliser la moitié du pool d'adresses allouées.

   Les sous-réseaux serveur et de l'extension future ont 6 bits hôtes. Cela permet d'avoir jusqu'à 62 hôtes sur chaque sous-réseau et d'utiliser l'autre moitié du pool d'adresses.

▶ Tâche 2 : Calculer les masques de sous-réseau et les ID réseau

1. Compte tenu du nombre de bits hôtes alloués, quel est le masque de sous-réseau que vous allez utiliser pour le sous-réseau client ? Calculez le masque de sous-réseau au format binaire et décimal.

   - Le sous-réseau client utilise 7 bits pour l'ID hôte. Par conséquent, vous allez utiliser 25 bits pour le masque de sous-réseau.

Binaire	Décimal
11111111.11111111.11111111.10000000	255.255.255.128

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

2. Compte tenu du nombre de bits hôtes alloués, quel est le masque de sous-réseau que vous allez utiliser pour le sous-réseau serveur ? Calculez le masque de sous-réseau au format binaire et décimal.

   - Le sous-réseau serveur utilise 6 bits pour l'ID hôte. Par conséquent, vous allez utiliser 26 bits pour le masque de sous-réseau.

Binaire	Décimal
11111111.11111111.11111111.11000000	255.255.255.192

3. Compte tenu du nombre de bits hôtes alloués, quel est le masque de sous-réseau que vous allez utiliser pour le sous-réseau de l'extension future ? Calculez le masque de sous-réseau au format binaire et décimal.

   - Le sous-réseau de l'extension future utilise 6 bits pour l'ID hôte. Par conséquent, vous allez utiliser 26 bits pour le masque de sous-réseau.

Binaire	Décimal
11111111.11111111.11111111.11000000	255.255.255.192

4. Pour le sous-réseau client, définissez l'ID réseau, le premier hôte disponible, le dernier hôte disponible et l'adresse de diffusion. Supposons que le sous-réseau client soit le premier sous-réseau alloué à partir du pool d'adresses disponibles. Calculez les versions binaires et décimales de chaque adresse.

   Dans ce tableau, les bits en gras font partie de l'ID réseau.

Description	Binaire	Décimal
ID réseau	**11000000.10101000.1100010.0**0000000	192.168.98.0
Premier hôte	**11000000.10101000.1100010.0**0000001	192.168.98.1
Dernier hôte	**11000000.10101000.1100010.0**1111110	192.168.98.126
Diffusion	**11000000.10101000.1100010.0**1111111	192.168.98.127

5. Pour le sous-réseau serveur, définissez l'ID réseau, le premier hôte disponible, le dernier hôte disponible et l'adresse de diffusion. Supposons que le sous-réseau serveur soit le deuxième sous-réseau alloué à partir du pool d'adresses disponibles. Calculez les versions binaires et décimales de chaque adresse.

   Dans ce tableau, les bits en gras font partie de l'ID réseau.

Description	Binaire	Décimal
ID réseau	**11000000.10101000.1100010.10**000000	192.168.98.128
Premier hôte	**11000000.10101000.1100010.10**000001	192.168.98.129

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Description	Binaire	Décimal
Dernier hôte	**11000000.10101000.1100010.10**111110	192.168.98.190
Diffusion	**11000000.10101000.1100010.10**111111	192.168.98.191

6. Pour le sous-réseau à allouer ultérieurement, définissez l'ID réseau, le premier hôte disponible, le dernier hôte disponible et l'adresse de diffusion. Supposons que le sous-réseau à allouer ultérieurement soit le troisième sous-réseau alloué à partir du pool d'adresses disponibles. Calculez les versions binaires et décimales de chaque adresse.

   Dans ce tableau, les bits en gras font partie de l'ID réseau.

Description	Binaire	Décimal
ID réseau	**11000000.10101000.1100010.11**000000	192.168.98.192
Premier hôte	**11000000.10101000.1100010.11**000001	192.168.98.193
Dernier hôte	**11000000.10101000.1100010.11**111110	192.168.98.254
Diffusion	**11000000.10101000.1100010.11**111111	192.168.98.255

Résultats : À la fin de cet exercice, vous aurez identifié les sous-réseaux requis pour répondre aux exigences du scénario de l'atelier pratique.

Exercice 2 : Résolution des problèmes liés à IPv4

▶ Tâche 1 : Préparer la résolution des problèmes

1. Sur LON-SVR2, dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
2. À l'invite Windows PowerShell, tapez **ping LON-DC1**, puis appuyez sur Entrée.
3. Ouvrez une fenêtre de l'**Explorateur de fichiers**, puis accédez à **\\LON-DC1\E$\Labfiles\Mod05**.
4. Cliquez avec le bouton droit sur **Break.ps1**, cliquez sur Ouvrir, puis cliquez sur **Exécuter avec PowerShell**.
5. Fermez l'Explorateur de fichiers.

▶ Tâche 2 : Résoudre les problèmes de connectivité IPv4 entre LON-SVR2 et LON-DC1

1. Sur LON-SVR2, à l'invite Windows PowerShell, tapez **ping LON-DC1**, puis appuyez sur Entrée. Notez que l'hôte de destination est injoignable.
2. Tapez **tracert LON-DC1**, puis appuyez sur Entrée. Notez que l'hôte est incapable de trouver la passerelle par défaut, et que ce n'est pas la passerelle par défaut qui répond.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Tapez **ipconfig**, puis appuyez sur Entrée. Notez que la passerelle par défaut est correctement configurée.
4. Tapez **ping 10.10.0.1**, puis appuyez sur Entrée. Notez que la passerelle par défaut répond mais que les paquets ne sont pas acheminés vers cette dernière.
5. Tapez **Get-NetRoute**, puis appuyez sur Entrée. Notez que l'entrée de la passerelle par défaut (0.0.0.0) est correcte mais qu'il existe une entrée inutile pour le réseau 172.16.0.0.
6. Tapez **Remove-NetRoute –DestinationPrefix 172.16.0.0/16**, puis appuyez sur Entrée. Cela permet de supprimer l'itinéraire inutile vers le réseau 172.16.0.0. À la place, la passerelle par défaut sera utilisée pour le routage.
7. Appuyez sur **O**, puis sur Entrée pour confirmer la suppression de l'itinéraire des itinéraires actifs.
8. Tapez **ping LON-DC1**, puis appuyez sur Entrée. Notez que le test ping s'effectue maintenant avec succès.

Résultats : À la fin de cet atelier pratique, vous aurez résolu un problème de connectivité IPv4.

▶ 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®-Manager**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-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 **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6 : Implémentation du protocole DHCP (Dynamic Host Configuration Protocol)

Atelier pratique : Implémentation de DHCP

Exercice 1 : Implémentation de DHCP

▶ Tâche 1 : Installer le rôle Serveur DHCP (Dynamic Host Configuration Protocol)

1. Basculez vers **LON-SVR1**.
2. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, 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**, activez la case à cocher **Serveur DHCP**.
7. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Serveur DHCP**, cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. 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 les étendues et les options DHCP

1. Dans **Gestionnaire de serveur -Rableau de bord**, cliquez sur **Outils**, puis sur **DHCP**.
2. Dans la console DHCP, développez et cliquez avec le bouton droit sur **lon-svr1.adatum.com**, puis cliquez sur **Autoriser**.
3. Dans la console DHCP, cliquez avec le bouton droit sur **lon-svr1.adatum.com**, puis cliquez sur **Actualiser**. Remarquez que les icônes en regard d'IPv4 et IPv6 passent du rouge au vert pour indiquer que le serveur DHCP a été autorisé dans Active Directory® Domain Services (AD DS).
4. Dans la console DHCP, dans le volet de navigation, cliquez sur **lon-svr1.adatum.com**, développez et cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**.
5. Dans l'Assistant Nouvelle étendue, cliquez sur **Suivant**.
6. Sur la page **Nom de l'étendue**, dans la zone **Nom**, tapez **Filiale**, puis cliquez sur **Suivant**.
7. Sur la page **Plage d'adresses IP**, renseignez les informations suivantes, puis cliquez sur **Suivant** :
   - Adresse IP de début : **172.16.0.100**
   - Adresse IP de fin : **172.16.0.200**
   - Longueur : **16**
   - Masque de sous-réseau : **255.255.0.0**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Sur la page **Ajout d'exclusions et de retard**, renseignez les informations suivantes :
   - Adresse IP de début : **172.16.0.190**
   - Adresse IP de fin : **172.16.0.200**
9. Cliquez sur **Ajouter**, puis sur **Suivant**.
10. Sur la page **Durée du bail**, cliquez sur **Suivant**.
11. Sur la page **Configuration des paramètres DHCP**, cliquez sur **Suivant**.
12. Sur la page **Routeur (passerelle par défaut)**, dans la zone **Adresse IP**, tapez **172.16.0.1**, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
13. Sur la page **Nom de domaine et serveurs DNS**, cliquez sur **Suivant**.
14. Sur la page **Serveurs WINS**, cliquez sur **Suivant**.
15. Sur la page **Activer l'étendue**, cliquez sur **Suivant**.
16. Sur la page **Fin de l'Assistant Nouvelle étendue**, cliquez sur **Terminer**.

▶ Tâche 3 : Configurer le client pour utiliser DHCP, puis tester la configuration

1. Basculez vers l'ordinateur **LON-CL1.**
2. Déplacez la souris sur l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
3. Dans la zone **Rechercher**, tapez **Panneau de configuration**, puis appuyez sur Entrée.
4. Dans le Panneau de configuration, sous **Réseau et Internet**, cliquez sur **Afficher l'état et la gestion du réseau**.
5. Dans la fenêtre Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
6. Dans la fenêtre **Connexions réseau**, cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
7. Dans la fenêtre Propriétés de Connexion au réseau local, cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
8. Dans la boîte de dialogue **Propriétés de : Protocole Internet version 4 (TCP/IPv4)**, sélectionnez la case d'option **Obtenir une adresse IP automatiquement**, sélectionnez la case d'option **Obtenir les adresses des serveurs DNS automatiquement**, cliquez sur **OK**, puis cliquez sur **Fermer**.
9. Déplacez la souris sur l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
10. Dans la zone **Rechercher**, tapez **Invite de commandes**, puis appuyez sur Entrée.
11. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ipconfig /renew**, puis appuyez sur Entrée.
12. Pour tester la configuration, vérifiez que LON-CL1 a reçu une adresse IP de l'étendue DHCP en saisissant **ipconfig /all** à l'invite de commandes.

    Cette commande renverra les informations telles que l'adresse IP, le masque de sous-réseau et l'état d'activation de DHCP, qui devrait être **Oui**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer un bail en tant que réservation

1. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ipconfig /all**, puis appuyez sur Entrée.
2. Notez l'adresse physique de la carte réseau LON-CL1.
3. Basculez vers **LON-SVR1**.
4. Dans le tableau de bord du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP**.
5. Dans la console DHCP**,** développez **lon-svr1.adatum.com**, **IPv4** et **Filiale**, développez **Réservations**, puis cliquez sur **Nouvelle réservation**.
6. Dans la fenêtre Nouvelle réservation :
   - Dans le champ **Nom de réservation**, tapez **LON-CL1**.
   - Dans le champ **Adresse IP**, tapez **172.16.0.155**.
   - Dans le champ **Adresse MAC**, tapez l'adresse physique que vous avez notée à l'étape 2.
   - Cliquez sur **Ajouter**, puis sur **Fermer**.
7. Basculez vers **LON-CL1**.
8. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ipconfig /release**, puis appuyez sur Entrée. Cette opération oblige LON-CL1 à libérer toutes les adresses IP actuellement louées.
9. À l'invite de commandes, tapez **ipconfig /renew**, puis appuyez sur Entrée. Cette opération oblige LON-CL1 à louer toutes les adresses IP réservées.
10. Vérifiez que l'adresse IP de LON-CL1 est maintenant **172.16.0.155**.

Résultats : À la fin de cet exercice, vous aurez implémenté DHCP, configuré les étendues et options DHCP, et configuré une réservation DHCP.

▶ Pour préparer l'exercice facultatif

Si vous voulez effectuer l'atelier pratique facultatif, rétablissez l'ordinateur virtuel 22410B-LON-CL1. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®-Manager**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-LON-CL1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.

Exercice 2 : Implémenter un agent de relais DHCP (exercice facultatif)

▶ Tâche 1 : Installer un agent de relais DHCP

1. Basculez vers **LON-RTR**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Routage et accès distant**.
3. Dans le volet de navigation, développez **LON-RTR (local)**, développez **IPv4**, cliquez avec le bouton droit sur **Général**, puis cliquez sur **Nouveau protocole de routage**.
4. Dans la liste **Protocoles de routage**, cliquez sur **Agent de relais DHCP**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer un agent de relais DHCP

1. Dans le volet de navigation, cliquez avec le bouton droit sur **Agent de relais DHCP**, puis cliquez sur **Nouvelle interface**.
2. Dans la boîte de dialogue **Nouvelle interface pour Agent de relais DHCP**, cliquez sur **Connexion au réseau local 2**, puis sur **OK**.
3. Dans la boîte de dialogue **Propriétés de : Propriétés de relais DHCP – Con...**, cliquez sur **OK**.
4. Cliquez avec le bouton droit sur **Agent de relais DHCP**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de : Agent de relais DHCP**, dans la zone **Adresse du serveur**, tapez **172.16.0.21**, puis cliquez sur **Ajouter** et **OK**.
6. Fermez la boîte de dialogue Routage et accès distant.

▶ Tâche 3 : Tester l'agent de relais DHCP avec un client

Remarque : Pour tester la manière dont un client reçoit une adresse IP de l'agent de relais DHCP sur un autre sous-réseau, vous devez créer une autre étendue DHCP.

1. Basculez vers **LON-SVR1**.
2. Dans le **tableau de bord du Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DHCP**.
3. Dans la console DHCP , développez **lon-svr1.adatum.com**.
4. Dans la console DHCP, dans le volet de navigation, cliquez sur **lon-svr1.adatum.com**, développez **IPv4**, cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Nouvelle étendue**.
5. Dans l'Assistant Nouvelle étendue, cliquez sur **Suivant**.
6. Sur la page **Nom de l'étendue**, dans la zone **Nom**, tapez **Filiale 2**, puis cliquez sur **Suivant**.
7. Sur la page **Plage d'adresses IP**, renseignez les informations suivantes, puis cliquez sur **Suivant** :
   - Adresse IP de début : **10.10.0.100**
   - Adresse IP de fin : **10.10.0.200**
   - Longueur : **16**
   - Masque de sous-réseau : **255.255.0.0**
8. Sur la page **Ajout d'exclusions et de retard**, renseignez les informations suivantes, cliquez sur **Ajouter**, puis cliquez sur **Suivant** :
   - Adresse IP de début : **10.10.0.190**
   - Adresse IP de fin : **10.10.0.200**
9. Sur la page **Durée du bail**, cliquez sur **Suivant**.
10. Sur la page **Configuration des paramètres DHCP**, cliquez sur **Suivant**.
11. Sur la page **Routeur (passerelle par défaut)**, dans la zone **Adresse IP**, tapez **10.10.0.1**, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
12. Sur la page **Nom de domaine et serveurs DNS**, cliquez sur **Suivant**.
13. Sur la page **Serveurs WINS**, cliquez sur **Suivant**.

14. Sur la page **Activer l'étendue**, cliquez sur **Suivant**.
15. Sur la page **Fin de l'Assistant Nouvelle étendue**, cliquez sur **Terminer**.
16. Pour tester le client, basculez vers **LON-CL2**.
17. Sur l'écran d'accueil, dans la zone **Accueil**, saisissez **Panneau de configuration**, puis appuyez sur Entrée.
18. Sous **Réseau et Internet**, cliquez sur **Afficher l'état et la gestion du réseau**.
19. Dans la fenêtre 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**.
20. Dans la fenêtre Propriétés de Connexion au réseau local, cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
21. Dans la boîte de dialogue **Propriétés de Protocole Internet version 4 (TCP/IPv4)**, cliquez sur **Obtenir une adresse IP automatiquement**, puis sur **Obtenir les adresses des serveurs DNS automatiquement**, sur **OK**, puis sur **Fermer**.
22. Naviguez jusqu'à l'angle inférieur droit, puis dans le menu contextuel, cliquez sur **Rechercher**, tapez **cmd**, et appuyez sur Entrée.
23. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ipconfig /renew**, puis appuyez sur Entrée.
24. Vérifiez que les paramètres d'adresse IP et de serveur DNS sur **LON-CL2** sont obtenus à partir de l'étendue de serveur DHCP **Filiale 2**, installée sur **LON-SVR1**.

Remarque : L'adresse IP doit être comprise dans la plage suivante : **10.10.0.100/16** à **10.10.0.200/16**

Résultats : À la fin de cet exercice, vous aurez implémenté un agent de relais DHCP.

▶ 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 **22410B-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 **22410B-LON-SVR1**, **22410B-LON-RTR**, et **22410B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7 : Implémentation du système DNS (Domain Name System)

Atelier pratique : Implémentation de la réplication DNS

Exercice 1 : Installation et configuration du système DNS

▶ Tâche 1 : Configurer LON-SVR1 en tant que contrôleur de domaine sans installer le rôle serveur DNS (Domain Name System)

1. Dans la console du **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 **LON-SVR1.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, sélectionnez **Services AD DS**.
6. 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 domaine Active Directory**, cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Sur la page **Progression de l'installation**, quand vous voyez s'afficher le message **Installation réussie**, cliquez sur **Fermer**.
11. Dans la console du **Gestionnaire de serveurs**, dans la page de navigation, cliquez sur **AD DS**.
12. Dans la barre de titre, où **Configuration requise pour : Services AD DS à LON-SVR1** s'affiche, cliquez sur **Autres**.
13. Sur la page **Détails et notifications de la tâche Tous les serveurs**, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
14. Dans l' Assistant Configuration des services de domaine Active Directory, dans la page **Configuration de déploiement**, assurez-vous que l'option **Ajouter un contrôleur de domaine à un domaine existant** est sélectionnée, puis cliquez sur **Suivant**.
15. Dans la page **Options du contrôleur de domaine**, désactivez la case à cocher **Serveur DNS (Domain Name System)** et laissez la case à cocher **Catalogue global (GC)** activée. Tapez **Pa$$w0rd** dans les deux champs de texte, puis cliquez sur **Suivant**.
16. Sur la page Options DNS, cliquez sur Suivant. Sur la page **Options supplémentaires**, cliquez sur **Suivant**.
17. Sur la page **Chemins d'accès**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Sur la page **Examiner les options**, cliquez sur **Suivant**.
19. Sur la page **Vérification de la configuration requise**, cliquez sur **Installer**.

Remarque : Le serveur LON-SVR1 redémarre automatiquement dans le cadre de la procédure.

20. Une fois que LON-SVR1 a redémarré, connectez-vous en tant que **ADATUM\Administrateur**.

▶ Tâche 2 : Créer et configurer la zone nwtraders.msft sur LON-DC1

1. Sur l'ordinateur LON-DC1, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Développez **LON-DC1**, **Zones de recherche directes,** et sélectionnez **Nouvelle zone...**.
3. Dans la page **Bienvenue !** de l'**Assistant Nouvelle zone**, cliquez sur **Suivant**.
4. Sur la page **Type de zone**, supprimez la coche de l'option **Enregistrer la zone dans Active Directory**, puis cliquez sur **Suivant**.
5. Dans la page **Nom de la zone**, entrez **nwtraders.msft**, puis cliquez sur **Suivant**.
6. Dans la page **Fichier de zone**, cliquez sur **Suivant**.
7. Dans la page **Mise à niveau dynamique**, cliquez sur **Suivant**.
8. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
9. Développez **nwtraders.msft**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
10. Dans la fenêtre **Nouvel hôte**, dans la zone de texte **Nom**, tapez **www**.
11. Dans la zone **Adresse IP**, tapez **172.16.0.100**.
12. Cliquez sur **Ajouter un hôte**.
13. Cliquez sur **OK**, puis sur **Terminé**.
14. Laissez la console du **Gestionnaire DNS** ouverte.

▶ Tâche 3 : Vérifier les paramètres de configuration sur le serveur DNS existant pour confirmer les indications de racine

1. Sur LON-DC1, cliquez dans la console du Gestionnaire DNS, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : LON-DC1**, cliquez sur l'onglet **Indications de racine**. Assurez-vous que les serveurs d'indications de racine s'affichent.
3. Cliquez sur l'onglet **Redirecteurs**. Assurez-vous que la liste n'affiche aucune entrée et que l'option **Utiliser les indications de racine si aucun redirecteur n'est disponible** est sélectionnée.
4. Cliquez sur **Annuler**.
5. Fermez la console du Gestionnaire DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Ajouter le rôle serveur DNS de la filiale au contrôleur de domaine

1. Sur LON-SVR1, dans la console du 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 **LON-SVR1.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionnez des rôles de serveurs**, sélectionnez **Serveur DNS**.
6. 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 **Serveur DNS**, cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Sur la page **Progression de l'installation**, quand vous voyez s'afficher le message **Installation réussie**, cliquez sur **Fermer**.

▶ Tâche 5 : Vérifier la réplication de la zone intégrée à Active Directory Adatum.com

1. Sur LON-SVR1, dans la console du **Gestionnaire de serveur**, cliquez sur **Outils**.
2. Dans la liste des outils, cliquez sur **DNS**.
3. Dans la console du Gestionnaire DNS, développez **LON-SVR1**, puis **Zones de recherche directes**. Ce conteneur est probablement vide.
4. Revenez au **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
5. Dans la console **Sites et services Active Directory**, développez **Sites**, développez **Default-First-Site-Name**, développez **Servers**, développez **LON-DC1**, puis cliquez sur **NTDS Settings**.
6. Dans le volet droit, cliquez avec le bouton droit sur la connexion de réplication **LON-SVR1**, puis sélectionnez **Répliquer maintenant**.

Remarque : Si vous recevez un message d'erreur, passez à l'étape suivante, puis recommencez cette étape après 3 à 4 minutes.

7. Dans le volet de navigation, développez **LON-SVR1**, puis cliquez sur **NTDS Settings**.
8. Dans le volet droit, cliquez avec le bouton droit sur la connexion de réplication **LON-DC1**, cliquez sur **Répliquer maintenant**, puis sur **OK**.
9. Revenez à la console du Gestionnaire DNS, cliquez avec le bouton droit sur **Zones de recherche directes**, puis cliquez sur **Actualiser**.
10. Assurez-vous que les deux conteneurs **_msdcs.Adatum.com** et **Adatum.com** s'affichent.
11. Fermez le Gestionnaire DNS.

▶ Tâche 6 : Utiliser Nslookup pour tester une résolution non locale

1. Sur LON-SVR1, passez à l'écran d'**accueil**, puis tapez **Panneau de configuration**. Appuyez sur Entrée.
2. Dans le **Panneau de configuration**, cliquez sur **Afficher l'état et la gestion du réseau**.
3. Cliquez sur **Modifier les paramètres de la carte**.
4. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
5. Cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis cliquez sur **Propriétés**.
6. Dans le champ **Serveur DNS préféré**, supprimez l'adresse IP, tapez **127.0.0.1**, cliquez sur **OK**, puis sur **Fermer**.
7. Sur **LON-SVR1**, dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
8. Dans la fenêtre Windows PowerShell, à l'invite de commandes, tapez **Resolve-DNSName www.nwtraders.msft**, puis appuyez sur Entrée. Vous devez normalement recevoir un message d'erreur.
9. Laissez la fenêtre Windows PowerShell ouverte.

▶ Tâche 7 : Configurer la résolution de noms Internet pour effectuer une redirection vers le siège

1. Sur LON-SVR1, ouvrez la console du **Gestionnaire DNS**.
2. Dans la console du Gestionnaire DNS, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de LON-SVR1**, cliquez sur l'onglet **Redirecteurs**, puis cliquez sur **Modifier**.
4. Dans la fenêtre Modifier les redirecteurs, tapez **172.16.0.10**, puis cliquez sur **OK** à deux reprises.
5. Dans la console du Gestionnaire DNS, cliquez avec le bouton droit sur **LON-SVR1**, sélectionnez **Toutes les tâches**, puis cliquez sur **Redémarrer**.

▶ Tâche 8 : Utiliser Nslookup pour confirmer la résolution de noms

1. Sur LON-SVR1, basculez vers une fenêtre **Windows PowerShell**.
2. Dans la fenêtre d'invite de commandes, tapez **nslookup**, puis appuyez sur Entrée.
3. À l'invite de **nslookup**, tapez **www.nwtraders.msft**, puis appuyez sur Entrée.
4. Assurez-vous que vous recevez une adresse IP pour cet hôte sous forme de réponse ne faisant pas autorité.
5. Tapez **quit**, puis appuyez sur Entrée.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré DNS sur LON-SVR1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Création d'enregistrements d'hôtes dans DNS

▶ Tâche 1 : Configurer un client pour utiliser LON-SVR1 en tant que serveur DNS

1. Sur LON-CL1, connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran d'**accueil**, tapez **Panneau de configuration**, puis appuyez sur Entrée.
3. Dans le **Panneau de configuration**, cliquez sur **Afficher l'état et la gestion du réseau**.
4. Cliquez sur **Modifier les paramètres de la carte**.
5. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de : Connexion au réseau local**, cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
7. Supprimez l'adresse IP du **serveur DNS préféré**. Dans la zone **Serveur DNS préféré**, tapez **172.16.0.21**, cliquez sur **OK**, puis sur **Fermer**.

▶ Tâche 2 : Créer plusieurs enregistrements d'hôtes dans le domaine Adatum.com pour des applications Web

1. Sur LON-DC1, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans la console du Gestionnaire DNS, développez **LON-DC1**, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
4. Dans la fenêtre **Nouvel hôte**, configurez les paramètres suivants :
   - Nom : **www**
   - Adresse IP : **172.16.0.200**
5. Cliquez sur **Ajouter un hôte**, puis sur **OK**.
6. Dans la fenêtre **Nouvel hôte**, configurez les paramètres suivants :
   - Nom : **ftp**
   - Adresse IP : **172.16.0.201**
7. Cliquez sur **Ajouter un hôte**, sur **OK**, puis sur **Terminé**.

▶ Tâche 3 : Vérifier la réplication des nouveaux enregistrements sur LON-SVR1

1. Sur LON-SVR1, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans la console du Gestionnaire DNS, développez **LON-SVR1**, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Assurez-vous que les enregistrements de ressources **www** et **ftp** s'affichent. (S'ils ne s'affichent pas, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Actualiser**). L'affichage des enregistrements peut prendre quelques minutes.

▶ Tâche 4 : Utilisez la commande ping pour localiser de nouveaux enregistrements de LON-CL1

1. Sur LON-CL1, cliquez avec le bouton droit sur la barre des tâches, puis cliquez sur **Gestionnaire des tâches**.
2. Dans la fenêtre du Gestionnaire des tâches, cliquez sur **Plus de détails**.
3. Ouvrez le menu **Fichier**, puis cliquez sur **Exécuter une nouvelle tâche**.
4. Dans la fenêtre Créer une tâche, tapez **cmd**, puis appuyez sur Entrée.
5. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ping www.adatum.com**, puis appuyez sur Entrée.
6. Assurez-vous que le nom est résolu en **172.16.0.200**. (Vous ne recevrez pas de réponses.)
7. À l'invite de commandes, tapez **ping ftp.adatum.com**, puis appuyez sur Entrée.
8. Assurez-vous que ce nom est résolu en **172.16.0.201**. (Vous ne recevrez pas de réponses.)
9. Laissez la fenêtre d'invite de commandes ouverte.

Résultats : Après avoir terminé cet exercice, vous aurez configuré les enregistrements DNS.

Exercice 3 : Gestion du cache d'un serveur DNS

▶ Tâche 1 : Utiliser la commande ping pour localiser un enregistrement Internet de LON-CL1

1. Sur LON-CL1, dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ping www.nwtraders.msft**, puis appuyez sur Entrée.
2. Le test ping ne fonctionnera pas, mais assurez-vous que le nom est résolu en adresse IP 172.16.0.100.
3. Laissez la fenêtre d'invite de commandes ouverte.

▶ Tâche 2 : Mettre à jour un enregistrement Internet pour pointer vers l'adresse IP de LON-DC1

1. Sur LON-DC1, ouvrez le **Gestionnaire DNS**.
2. Dans la console du Gestionnaire DNS, développez **LON-DC1**, développez **Zones de recherche directes**, puis cliquez sur **nwtraders.msft**.
3. Dans le volet droit, cliquez avec le bouton droit sur **www**, puis cliquez sur **Propriétés**.
4. Remplacez l'adresse IP par **172.16.0.10**, puis cliquez sur **OK**.
5. Rebasculez vers **LON-CL1**.
6. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ping www.nwtraders.msft**, puis appuyez sur Entrée. Notez que la commande ping ne fonctionnera pas et que l'ancienne adresse IP (172.16.0.100) continuera à s'afficher.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Examiner le contenu du cache DNS

1. Basculez vers **LON-SVR1**.
2. Dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
3. Cliquez sur **LON-SVR1**, sur le menu **Affichage**, puis sur **Affichage détaillé**.
4. Développez LON-SVR1, développez le nœud **Recherches mises en cache**, développez **.(racine)**, développez **msft**, puis cliquez sur **nwtraders**.
5. Dans le volet droit, examinez le contenu mis en cache. Vous verrez que l'enregistrement **www** a l'adresse IP suivante : **172.16.0.100**.
6. Basculez vers **LON-CL1**.
7. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez **ipconfig/displaydns**, puis appuyez sur Entrée.
8. Recherchez les entrées mises en cache. Vous remarquerez que www.nwtraders.msft est résolu en 172.16.0.100.

▶ Tâche 4 : Vider le cache et réessayer la commande ping

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. À l'invite Windows PowerShell, tapez **Clear-DNSServerCache**, puis appuyez sur Entrée. Tapez **o**, puis appuyez sur Entrée.
3. Basculez vers **LON-CL1**.
4. Dans une fenêtre d'invite de commandes, à l'invite de commandes, tapez **ping www.nwtraders.msft**, puis appuyez sur Entrée. L'ancienne adresse IP continue d'être retournée.
5. Dans une fenêtre d'invite de commandes, tapez **ipconfig /flushdns**, puis appuyez sur Entrée.
6. Dans la fenêtre d'invite de commandes, tapez **ping www.nwtraders.msft**, puis appuyez sur Entrée.
7. Le test ping doit maintenant fonctionner sur l'adresse **172.16.0.10**.

Résultats : À la fin de cet exercice, vous aurez examiné le cache du serveur DNS.

▶ 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 **22410B-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 **22410B-LON-SVR1** et **22410B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8 : Implémentation d'IPv6

Atelier pratique : Implémentation d'IPv6

Exercice 1 : Configuration d'un réseau IPv6

▶ Tâche 1 : Vérifier le routage IPv4

1. Sur LON-SVR2, dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
2. À l'invite Windows PowerShell, tapez **ping lon-dc1**, puis appuyez sur Entrée. Remarquez qu'il y a quatre réponses reçues de 172.16.0.10.
3. Tapez **ipconfig**, puis appuyez sur Entrée.
4. Vérifiez que la seule adresse IPv6 répertoriée est une adresse de liaison locale qui ne peut pas être routée.

▶ Tâche 2 : Désactiver le protocole IPv6 sur LON-DC1

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
2. Dans la fenêtre Propriétés, en regard Connexion au réseau local, cliquez sur **172.16.0.10, Compatible IPv6**.
3. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, désactivez la case à cocher **Protocole Internet version 6 (TCP/IPv6)**, puis cliquez sur **OK**.
5. Fermez la fenêtre Connexions réseau.
6. Dans le Gestionnaire de serveur, vérifiez que **Connexion au réseau local** répertorie seulement **172.16.0.10**. Il se peut que vous deviez actualiser l'affichage. À présent, LON-DC1 est un hôte IPv4-uniquement.

▶ Tâche 3 : Désactiver le protocole IPv4 sur LON-SVR2

1. Sur LON-SVR2, dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
2. Dans la boîte de dialogue **PROPRIÉTÉS du serveur local**, en regard de Connexion au réseau local, cliquez sur **10.10.0.24, Compatible IPv6**.
3. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, désactivez la case à cocher **Protocole Internet version 4 (TCP/IPv4)**, puis cliquez sur **OK**.
5. Fermez la fenêtre Connexions réseau.
6. Dans le Gestionnaire de serveur, vérifiez qu'à présent **Connexion au réseau local** mentionne seulement **Compatible IPv6**. Il se peut que vous deviez actualiser l'affichage. À présent, LON-SVR2 est un hôte IPv6-uniquement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer un réseau IPv6 sur LON-RTR

1. Sur LON-RTR, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. Configurez une adresse réseau qui sera utilisée sur le réseau IPv6. À l'invite Windows PowerShell, tapez l'applet de commande suivante, puis appuyez sur Entrée :

```
New-NetRoute -InterfaceAlias "Connexion au réseau local 2" -DestinationPrefix
2001:db8:0:1::/64 -Publish Yes
```

3. Autorisez les clients à obtenir l'adresse de réseau IPv6 automatiquement à partir de LON-RTR. À l'invite Windows PowerShell, tapez l'applet de commande suivante, puis appuyez sur Entrée :

```
Set-NetIPInterface -InterfaceAlias "Connexion au réseau local 2" -AddressFamily IPv6
-Advertising Enabled
```

4. Tapez **ipconfig**, puis appuyez sur Entrée. Notez que la connexion au réseau local 2 a désormais une adresse IPv6 sur le réseau 2001:db8:0:1::/64. Cette adresse est utilisée pour la communication sur le réseau IPv6-uniquement.

▶ Tâche 5 : Vérifier IPv6 sur LON-SVR2

1. Sur LON-SVR2, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. À l'invite Windows PowerShell, saisissez **ipconfig**, puis appuyez sur Entrée. Notez que la connexion au réseau local a maintenant une adresse IPv6 sur le réseau 2001:db8:0:1::/64. L'adresse réseau a été obtenue à partir du routeur via la configuration sans état.

Résultats : À la fin de cet exercice, les stagiaires auront configuré un réseau IPv6-uniquement.

Exercice 2 : Configuration d'un routeur ISATAP

▶ Tâche 1 : Ajouter un enregistrement d'hôte ISATAP au DNS

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le Gestionnaire DNS, développez successivement **LON-DC1** et **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
4. Dans la fenêtre Nouvel hôte, dans la zone **Nom**, tapez **ISATAP**.
5. Dans la zone **Adresse IP**, tapez **172.16.0.1**, puis cliquez sur **Ajouter un hôte**. Les clients ISATAP résolvent ce nom d'hôte pour rechercher le routeur ISATAP.
6. Cliquez sur **OK** pour effacer le message de réussite.
7. Cliquez sur **Terminé** pour fermer la fenêtre Nouvel hôte.
8. Fermez le Gestionnaire DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Activer le routeur ISATAP sur LON-RTR

1. Sur LON-RTR, configurez l'adresse IP de la connexion au réseau local en tant que routeur ISATAP. À l'invite Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Set-NetIsatapConfiguration -Router 172.16.0.1
```

2. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-NetIPAddress | Format-Table InterfaceAlias,InterfaceIndex,IPv6Address
```

3. Enregistrez l'InterfaceIndex de l'interface ISATAP qui a une adresse IPv6 comprenant **172.16.0.1**.

Index d'interface :	

4. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-NetIPInterface -InterfaceIndex IndexYouRecorded -PolicyStore ActiveStore |
Format-List
```

5. Vérifiez que la fonctionnalité de transfert est activée pour l'interface et que la fonctionnalité d'annonce est désactivée.

6. L'interface ISATAP d'un routeur ISATAP doit avoir la fonctionnalité de transfert activée et la fonctionnalité d'annonce désactivée. Tapez la commande suivante, puis appuyez sur Entrée :

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Enabled
```

7. Créez un nouveau réseau IPv6 qui sera utilisé pour le réseau ISATAP. Tapez la commande suivante, puis appuyez sur Entrée :

```
New-NetRoute -InterfaceIndex IndexYouRecorded -DestinationPrefix 2001:db8:0:2::/64 -
Publish Yes
```

8. Affichez la configuration des adresses IP pour l'interface ISATAP. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-NetIPAddress -InterfaceIndex IndexYouRecorded
```

9. Vérifiez qu'une adresse IPv6 est listée sur le réseau 2001:db8:0:2::/64.

▶ Tâche 3 : Supprimer ISATAP de la liste rouge de requêtes globales

1. Sur LON-DC1, à l'invite Windows PowerShell, tapez **regedit**, puis appuyez sur Entrée.
2. Dans la fenêtre Éditeur du Registre, développez **HKEY_LOCAL_MACHINE**, développez **SYSTEM**, développez **CurrentControlSet**, développez **Services**, développez **DNS**, cliquez sur **Parameters**, et double-cliquer sur **GlobalQueryBlockList**.
3. Dans la fenêtre Modifier les chaînes multiples, supprimez **isatap**, puis cliquez sur **OK**.
4. Si une erreur indiquant qu'il y avait une chaîne vide s'affiche, cliquez sur **OK** pour continuer.
5. Fermez l'Éditeur du Registre.
6. À l'invite Windows PowerShell, tapez **Restart-Service DNS -Verbose** et appuyez sur Entrée.
7. Tapez **ping isatap**, puis appuyez sur Entrée. Le nom devrait se résoudre et vous devriez recevoir quatre réponses de 172.16.0.1.

▶ Tâche 4 : Activer LON-DC1 en tant que client ISATAP

1. Sur LON-DC1, à l'invite Windows PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
Set-NetIsatapConfiguration -State Enabled
```

2. Tapez **ipconfig**, puis appuyez sur Entrée.
3. Vérifiez que la carte tunnel pour ISATAP a une adresse IPv6 sur le réseau 2001:db8:0:2/64. Notez que cette adresse comprend l'adresse IPv4 de LON-DC1.

▶ Tâche 5 : Tester la connectivité

1. Sur LON-SVR2, à l'invite Windows PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
ping 2001:db8:0:2:0:5efe:172.16.0.10
```

2. Dans le Gestionnaire de serveur, si nécessaire, cliquez sur **Serveur local**.
3. Dans la boîte de dialogue **PROPRIÉTÉS du serveur local**, en regard de Connexion au réseau local, cliquez sur **Compatible IPv6**.
4. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, cliquez sur **Protocole Internet version 6 (TCP/IPv6)**,, puis sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de : Protocole Internet version 6 (TCP/IPv6)**, cliquez sur **Utiliser l'adresse de serveur DNS suivante**.
7. Dans la zone **Serveur DNS préféré**, tapez **2001:db8:0:2:0:5efe:172.16.0.10**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Propriétés de connexion au réseau local**, cliquez sur **Fermer**.
9. Fermez la fenêtre Connexions réseau.
10. À l'invite Windows PowerShell, tapez **ping LON-DC1**, puis appuyez sur Entrée. Remarquez que quatre réponses sont reçues de LON-DC1.

Remarque : Une commande ping de LON-DC1 à LON-SVR2 ne répond pas, parce que la configuration du pare-feu sur LON-SVR2 bloque les demandes ping.

Résultats : À la fin de cet exercice, les stagiaires auront configuré un routeur ISATAP sur LON-RTR pour permettre la communication entre un réseau IPv6-uniquement et un réseau IPv4-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 **22410B-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 **22410B-LON-RTR** et **22410B-LON-SVR2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9 : Implémentation d'un système de stockage local

Atelier pratique : Implémentation d'un système de stockage local

Exercice 1 : Installation et configuration d'un nouveau disque

▶ Tâche 1 : Initialiser un nouveau disque

1. Connectez-vous à **LON-SVR1** avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Gestion de l'ordinateur**.
3. Dans la console Gestion de l'ordinateur, sous le nœud Stockage, cliquez sur **Gestion des disques**.
4. Dans le volet Disques, cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**.
5. Cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **Initialiser le disque**.
6. Dans la boîte de dialogue **Initialiser le disque**, vérifiez que la case à cocher **Disque 2 est sélectionné**, assurez-vous que les cases à cocher de tous les autres disques sont désactivées, cliquez sur **Partition GPT (GUID Partition Table)**, puis sur **OK**.

▶ Tâche 2 : Créer et formater deux volumes simples sur le disque

1. Dans la console Gestion de l'ordinateur, dans Gestion des disques, cliquez avec le bouton droit sur la zone noire à droite de Disque2, puis cliquez sur **Nouveau volume simple**.
2. Dans l'Assistant Création d'un volume simple, sur la page **Assistant Création d'un volume simple**, cliquez sur **Suivant**.
3. Sur la page **Spécifier la taille du volume**, dans le champ **Taille du volume simple en Mo**, tapez **4000**, puis cliquez sur **Suivant**.
4. Sur la page **Attribuer une lettre de lecteur ou de chemin d'accès**, assurez-vous que la case à cocher **Attribuer la lettre de lecteur suivante** est activée et que la lettre **F** est sélectionnée dans le menu déroulant, puis cliquez sur **Suivant**.
5. Sur la page **Formater une partition**, dans le menu déroulant **Système de fichiers**, cliquez sur **NTFS**, dans la zone de texte **Nom de volume**, tapez **Volume1**, puis cliquez sur **Suivant**.
6. Sur la page **Fin de l'Assistant Création d'un volume simple**, cliquez sur **Terminer**.
7. Dans la fenêtre Gestion de l'ordinateur, cliquez avec le bouton droit sur la zone noire à droite de Disque2, puis cliquez sur **Nouveau volume simple**.
8. Dans l'Assistant Création d'un volume simple, sur la page **Assistant Création d'un volume simple**, cliquez sur **Suivant**.
9. Sur la page **Spécifier la taille du volume**, dans le champ **Taille du volume simple en Mo**, tapez **5000**, puis cliquez sur **Suivant**.
10. Sur la page **Attribuer une lettre de lecteur ou de chemin d'accès**, assurez-vous que la case à cocher **Attribuer la lettre de lecteur suivante** est activée et que la lettre **G** est sélectionnée dans la liste déroulante, puis cliquez sur **Suivant**.
11. Sur la page **Formater une partition**, dans le menu déroulant **Système de fichiers**, cliquez sur **ReFS**, dans la zone de texte Nom de volume, tapez **Volume2**, puis cliquez sur **Suivant**.
12. Sur la page **Fin de l'Assistant Création d'un volume simple**, cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérifier la lettre de lecteur dans une fenêtre de l'Explorateur de fichiers

1. Sur la barre des tâches, ouvrez une fenêtre de l'Explorateur de fichiers, développez **Ordinateur**, puis cliquez sur **Volume1 (F:)**.
2. Dans l'Explorateur de fichiers, cliquez sur **Volume2 (G:)**, cliquez avec le bouton droit sur **Volume2 (G:)**, pointez sur **Nouveau**, puis cliquez sur **Dossier**.
3. Dans le champ **Nouveau dossier**, tapez **Dossier1**, puis appuyez sur Entrée.

Résultats : À la fin de cet exercice, vous devez avoir initialisé un nouveau disque, créé deux volumes simples et les avoir formatés. Vous devez également avoir vérifié que les lettres de lecteur sont disponibles dans l'Explorateur de fichiers.

Exercice 2 : Redimensionnement des volumes

▶ Tâche 1 : Réduire Volume1

1. Sur LON-SVR1, passez à la console Gestion de l'ordinateur.
2. Dans la console Gestion de l'ordinateur, dans Gestion des disques, dans le volet central, cliquez avec le bouton droit sur **Volume1 (F:)**, puis cliquez sur **Réduire le volume**.
3. Dans la fenêtre Réduire F:, dans le champ **Quantité d'espace à réduire (en Mo) :**, tapez **1 000**, puis cliquez sur **Réduire**.

▶ Tâche 2 : Étendre Volume2

1. Sur LON-SVR1, dans Gestion des disques, dans le volet central, cliquez avec le bouton droit sur **Volume2 (G:)**, puis cliquez sur **Étendre le volume**.
2. Dans l'Assistant Extension du volume, sur la page **Bienvenue !**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner les disques**, dans le champ **Sélectionnez l'espace en Mo**, tapez **1 000**, puis cliquez sur **Suivant**.
4. Sur la page **Fin de l'Assistant Extension du volume**, cliquez sur **Terminer**.
5. Dans une fenêtre de l'Explorateur de fichiers, cliquez sur **Volume2 (G:)**, et vérifiez que **Dossier1** est disponible sur le volume.

Résultats : À la fin de cet exercice, vous devez avoir réduit un volume et étendu un autre.

Exercice 3 : Configuration d'un espace de stockage redondant

▶ Tâche 1 : Créer un pool de stockage à partir de cinq disques connectés au serveur

1. Sur LON-SVR1, cliquez sur l'icône du **Gestionnaire de serveur** dans la barre des tâches.
2. Dans le Gestionnaire de serveur, dans le volet gauche, cliquez sur **Service de fichiers et de stockage**, puis dans le volet Serveurs, cliquez sur **Pools de stockage**.
3. Dans le volet POOLS DE STOCKAGE, cliquez sur **TÂCHES**, puis dans le menu déroulant **TÂCHES**, cliquez sur **Nouveau pool de stockage**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la fenêtre de l'Assistant Nouveau pool de stockage, sur la page **Avant de commencer**, cliquez sur **Suivant**.
5. Sur la page **Indiquer un pool de stockage et son sous-système**, dans la zone **Nom**, tapez **StoragePool1**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner les disques physiques pour le pool de stockage**, cliquez sur les disques physiques suivants, puis cliquez sur **Suivant**.
   - **PhysicalDisk3 (LON-SVR1)**
   - **PhysicalDisk4 (LON-SVR1)**
   - **PhysicalDisk5 (LON-SVR1)**
   - **PhysicalDisk6 (LON-SVR1)**
   - **PhysicalDisk7 (LON-SVR1)**
7. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
8. Sur la page **Afficher les résultats**, attendez que la tâche soit terminée, puis cliquez sur **Fermer**.

▶ Tâche 2 : Créer un disque virtuel en miroir triple

1. Sur LON-SVR1, dans le Gestionnaire de serveur, dans le volet Espaces de stockage, cliquez sur **StoragePool1**.
2. Dans le volet DISQUES VIRTUELS, cliquez sur **TÂCHES**, puis dans le menu déroulant **TÂCHES**, cliquez sur **Nouveau disque virtuel**.
3. Dans la fenêtre de l'Assistant Nouveau disque dur virtuel, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le pool de stockage**, cliquez sur **StoragePool1**, puis sur **Suivant**.
5. Sur la page **Spécifier le nom du disque virtuel**, dans la zone **Nom**, tapez **Disque en miroir**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner la disposition de stockage**, dans la liste **Disposition**, cliquez sur **Mirror**, puis sur **Suivant**.
7. Sur la page **Configurer les paramètres de résilience**, cliquez sur **Miroir triple**, puis cliquez sur **Suivant**.
8. Sur la page **Spécifer le type d'approvisionnement**, cliquez sur **Fin**, puis sur **Suivant**.
9. Sur la page **Spécifier la taille du disque virtuel**, dans la zone **Taille du disque virtuel**, tapez **10**, puis cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
11. Sur la page **Afficher les résultats**, attendez que la tâche soit terminée. Assurez-vous que la case à cocher **Créer un volume lorsque l'Assistant se ferme** est activée, puis cliquez sur **Fermer**.
12. Dans la fenêtre de l'Assistant Nouveau volume, sur la page **Avant de commencer**, cliquez sur **Suivant**.
13. Sur la page **Sélectionner le serveur et le disque**, dans le volet Disque, cliquez sur le disque virtuel **Disque en miroir**, puis cliquez sur **Suivant**.
14. Sur la page **Spécifier la taille du volume**, cliquez sur **Suivant** pour confirmer la sélection par défaut.

15. Sur la page **Affecter à la lettre d'un lecteur ou à un dossier**, dans le menu déroulant **Lettre de lecteur**, assurez-vous que la lettre **H** est sélectionnée, puis cliquez sur **Suivant**.
16. Sur la page **Sélectionner les paramètres du système de fichiers**, dans le menu déroulant **Système de fichiers**, cliquez sur **ReFS**, et dans la zone **Nom de volume**, tapez **Volume en miroir**, puis cliquez sur **Suivant**.
17. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
18. Sur la page **Dernière étape**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

▶ Tâche 3 : Copier un fichier sur le volume et vérifier qu'il est visible dans l'Explorateur de fichiers

1. Cliquez sur l'écran d'accueil, tapez **invite de commandes**, puis appuyez sur Entrée.
2. Dans la fenêtre d'invite de commandes, à l'invite de commandes, tapez la commande suivante, puis appuyez sur Entrée :

```
Copy C:\windows\system32\write.exe H:\
```

3. Fermez la fenêtre d'invite de commandes.
4. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
5. Dans la fenêtre de l'Explorateur de fichiers, cliquez sur **Volume en miroir (H:)**.
6. Vérifiez que **write.exe** figure dans la liste des fichiers.
7. Fermez l'Explorateur de fichiers.

▶ Tâche 4 : Supprimer un disque physique

1. Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V®, dans le volet Ordinateurs virtuels, cliquez avec le bouton droit sur **22410B-LON-SVR1**, puis sur **Paramètres**.
2. Dans les paramètres de 22410B-LON-SVR1, dans le volet de matériel, cliquez sur le disque dur qui commence par **22410B-LON-SVR1-Disk5**.
3. Dans le volet de disque dur, cliquez sur **Retrier** et sur **Appliquer**. Dans la boîte de dialogue des paramètres, cliquez sur Appliquer, sur **Continuer**, puis sur **OK**.

▶ Tâche 5 : Vérifier que le fichier write.exe est toujours accessible

1. Basculez vers LON-SVR1.
2. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
3. Dans la fenêtre de l'Explorateur de fichiers, cliquez sur **Volume en miroir (H:)**.
4. Dans le volet de liste de fichiers, vérifiez que **write.exe** est toujours accessible.
5. Fermez l'Explorateur de fichiers.
6. Dans le Gestionnaire de serveur, dans le volet POOLS DE STOCKAGE, sur la barre de menus, cliquez sur le bouton **Actualiser « Pools de stockage »**. Notez l'avertissement qui s'affiche en regard de Disque en miroir.
7. Dans le volet DISQUE VIRTUEL, cliquez avec le bouton droit sur **Disque en miroir**, puis cliquez sur **Propriétés**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Dans la boîte de dialogue **Propriétés de Disque en miroir**, dans le volet gauche, cliquez sur **Intégrité**. Notez que l'état d'intégrité signale un avertissement. L'état opérationnel doit indiquer **Incomplet**, **Inconnu** ou **Détérioré**.
9. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de Disque en miroir**.

▶ Tâche 6 : Ajouter un disque au pool de stockage et supprimer un disque endommagé

1. Basculez vers LON-SVR1.
2. Dans le Gestionnaire de serveur, dans le volet POOLS DE STOCKAGE, sur la barre de menus, cliquez sur le bouton **Actualiser « Pools de stockage »**.
3. Dans le volet POOLS DE STOCKAGE, cliquez avec le bouton droit sur **StoragePool1**, puis cliquez sur **Ajouter un disque physique**.
4. Dans la fenêtre Ajouter un disque physique, cliquez sur **PhysicalDisk8 (LON-SVR1)**, puis cliquez sur **OK**.
5. Dans le volet DISQUES PHYSIQUES, cliquez avec le bouton droit sur le disque en regard duquel s'affiche un avertissement, puis cliquez sur **Supprimer le disque**.
6. Après avoir cliqué sur Oui, dans la fenêtre contextuelle Supprimer un disque physique, cliquez sur **Oui** à deux reprises.
7. Dans le volet POOLS DE STOCKAGE, sur la barre de menus, cliquez sur le bouton **Actualiser « Pools de stockage »** pour faire disparaître les avertissements.

Résultats : À la fin de cet exercice, vous devez avoir créé un pool de stockage et lui avoir ajouté cinq disques. Vous devez ensuite avoir créé un disque virtuel en miroir triple alloué dynamiquement à partir du pool de stockage. Vous devez également avoir copié un fichier sur le nouveau volume et vérifié qu'il est accessible. Ensuite, après avoir supprimé un disque physique, vous devez avoir vérifié que le disque virtuel était toujours disponible et accessible. Enfin, vous devez avoir ajouté un autre disque physique au pool de stockage.

▶ 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 des ordinateurs virtuels, cliquez avec le bouton droit sur **22410B-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 **22410B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10 : Implémentation des services de fichier et d'impression

Atelier pratique : Implémentation des services de fichier et d'impression

Exercice 1 : Création et configuration d'un partage de fichiers

▶ Tâche 1 : Créer l'arborescence du nouveau partage

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
2. Dans une fenêtre de l'Explorateur de fichiers, dans le volet de navigation, développez Ordinateur, puis cliquez sur **Allfiles (E:)**.
3. Dans la barre d'outils Menu, cliquez sur **Accueil**, cliquez sur **Nouveau dossier**, tapez **Données** et appuyez sur Entrée.
4. Double-cliquez sur le dossier **Données**.
5. Dans la barre d'outils Menu, cliquez sur **Accueil**, cliquez sur **Nouveau dossier**, tapez **Development** et appuyez sur Entrée.
6. Répétez l'étape 5 pour les nouveaux noms de dossiers suivants :
   - **Marketing**
   - **Research**
   - **Sales**

▶ Tâche 2 : Configurer des autorisations NTFS sur l'arborescence

1. Dans l'Explorateur de fichiers, accédez au lecteur **E**, cliquez avec le bouton droit sur le dossier **Données**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : Données**, cliquez sur **Sécurité**, puis sur **Avancé**.
3. Dans la fenêtre Paramètres de sécurité avancés pour Données, cliquez sur **Désactiver l'héritage**.
4. Dans la fenêtre Bloquer l'héritage, cliquez sur **Convertir les autorisations héritées en autorisations explicites sur cet objet**.
5. Cliquez sur **OK** pour fermer la fenêtre Paramètres de sécurité avancés pour Données.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : Données**.
7. Dans l'Explorateur de fichiers, double-cliquez sur le dossier **Données**.
8. Cliquez avec le bouton droit sur le dossier **Development**, puis cliquez sur **Propriétés**.
9. Dans la fenêtre Propriétés de Development, cliquez sur **Sécurité**, puis sur **Avancé**.
10. Dans la fenêtre Paramètres de sécurité avancés pour Development, cliquez sur **Désactiver l'héritage**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la fenêtre Bloquer l'héritage, cliquez sur **Convertir les autorisations héritées en autorisations explicites sur cet objet**.
12. Supprimez les deux entrées d'autorisations pour les utilisateurs (LON-SVR1\Utilisateur), puis cliquez sur **OK**.
13. Dans l'onglet **Sécurité**, cliquez sur **Modifier**.
14. Dans la fenêtre **Autorisations pour Development**, cliquez sur **Ajouter**.
15. Tapez **Development**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
16. Activez la case à cocher pour **Autoriser Modification** dans la section **Autorisations pour Development**.
17. Cliquez sur **OK** pour fermer la fenêtre Autorisations pour Development.
18. Cliquez sur **OK** pour fermer la fenêtre Propriétés de Development.
19. Répétez les étapes 8 à 18 pour les dossiers **Marketing**, **Research** et **Sales**, en attribuant les autorisations Modification aux groupes **Marketing**, **Research** et **Sales** pour leurs dossiers respectifs.

▶ Tâche 3 : Créer le dossier partagé

1. Dans l'Explorateur de fichiers, accédez au lecteur **E**, cliquez avec le bouton droit sur le dossier **Données**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : Données**, cliquez sur l'onglet **Partage**, puis cliquez sur **Partage avancé**.
3. Dans la fenêtre Partage avancé, activez la case à cocher **Partager ce dossier**, puis cliquez sur **Autorisations**.
4. Dans la fenêtre Autorisations pour Données, cliquez sur **Ajouter**.
5. Tapez **Utilisateurs authentifiés**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
6. Dans la fenêtre Autorisations pour Données, cliquez sur **Utilisateurs authentifiés**, puis activez la case à cocher **Autoriser** pour l'autorisation **Modification**.
7. Cliquez sur **OK** pour fermer la fenêtre Autorisations pour Données.
8. Cliquez sur **OK** pour fermer la fenêtre Partage avancé.
9. Cliquez sur **Fermer** pour fermer la boîte de dialogue **Propriétés de : Données**.

▶ Tâche 4 : Tester l'accès au dossier partagé

1. Connectez-vous à **LON-CL1** en tant que **ADATUM\Bernard** avec le mot de passe **Pa$$w0rd**.

Remarque : Bernard est membre du groupe Development.

2. Dans l'écran d'accueil, cliquez sur la vignette **Bureau**.
3. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
4. Dans l'Explorateur de fichiers, dans la barre d'adresses, tapez **\\LON-SVR1\Données** et appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Double-cliquez sur le dossier **Development**.

Remarque : Bernard doit avoir accès au dossier Development.

6. Essayez d'accéder aux dossiers **Marketing**, **Research** et **Sales**. Les autorisations NTFS sur ces dossiers vous en empêcheront.

Remarque : Bernard peut encore voir les autres dossiers, même s'il n'a pas accès à leur contenu.

7. Déconnectez-vous de LON-CL1.

▶ Tâche 5 : Activer l'énumération basée sur l'accès

1. Basculez vers **LON-SVR1**.
2. Dans la barre des tâches, cliquez sur l'icône du **Gestionnaire de serveur**.
3. Dans le Gestionnaire de serveur, dans le volet de navigation, cliquez sur **Services de fichiers et de stockage**.
4. Dans la page **Services de fichiers et de stockage**, dans le volet de navigation, cliquez sur **Partages**.
5. Dans le volet Partages, cliquez avec le bouton droit sur **Données**, puis cliquez sur **Propriétés**.
6. Cliquez sur **Paramètres**, puis activez la case à cocher **Activer l'énumération basée sur l'accès**.
7. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de Données**.
8. Fermez le Gestionnaire de serveur.

▶ Tâche 6 : Tester l'accès au partage

1. Connectez-vous à LON-CL1 en tant que **ADATUM\Bernard** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur la vignette **Bureau**.
3. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
4. Dans l'Explorateur de fichiers, dans la barre d'adresses, tapez **\\LON-SVR1\Données** et appuyez sur Entrée.

Remarque : Bernard peut à présent visualiser uniquement le dossier Development, le dossier pour lequel des autorisations lui ont été attribuées.

5. Double-cliquez sur le dossier **Development**.

Remarque : Bernard doit avoir accès au dossier Development.

6. Déconnectez-vous de LON-CL1.

▶ Tâche 7 : Désactiver les fichiers hors connexion pour le partage

1. Basculez vers **LON-SVR1**.
2. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'Explorateur de fichiers, accédez au lecteur **Allfiles (E:)**, cliquez avec le bouton droit sur le dossier **Données**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de Données**, cliquez sur l'onglet **Partage**, sur **Partage avancé**, puis sur **Mise en cache**.
5. Dans la fenêtre Paramètres hors connexion, cliquez sur **Aucun fichier ou programme du dossier partagé n'est disponible hors connexion**, puis cliquez sur **OK**.
6. Cliquez sur **OK** pour fermer la fenêtre Partage avancé.
7. Cliquez sur **Fermer** pour fermer la boîte de dialogue **Propriétés de Données**.

Résultats : À la fin de cet exercice, vous aurez créé un nouveau dossier partagé à l'usage de plusieurs services.

Exercice 2 : Configuration de clichés instantanés

▶ Tâche 1 : Configurer des clichés instantanés pour le partage de fichiers

1. Basculez vers **LON-SVR1**.
2. Ouvrez l'Explorateur de fichiers.
3. Accédez au lecteur **E**, cliquez avec le bouton droit sur **Allfiles (E:)**, puis cliquez sur **Configurer les clichés instantanés**.
4. Dans la boîte de dialogue **Propriétés de Allfiles (E:)**, dans l'onglet **Clichés instantanés**, cliquez sur le lecteur **E**, puis cliquez sur **Activer**.
5. Dans la boîte de dialogue **Activer les clichés instantanés**, cliquez sur **Oui**.
6. Dans la boîte de dialogue **Propriétés de Allfiles (E:)**, dans l'onglet **Clichés instantanés**, cliquez sur **Paramètres**.
7. Dans la boîte de dialogue**Paramètres**, cliquez sur **Planifier**. La boîte de dialogue du lecteur **E** s'affiche.
8. Dans la boîte de dialogue du lecteur **Allfiles (E:)**, modifiez le paramètre Tâche planifiée en spécifiant **Tous les jours**, spécifiez l'heure de début **12:00**, puis cliquez sur **Avancé**.
9. Dans la boîte de dialogue **Options de planification avancées**, sélectionnez **Répéter la tâche**, puis définissez la fréquence sur **Toutes les 1 heures**.
10. Sélectionnez **Heure** et spécifiez la valeur horaire **23:59**.
11. Cliquez sur **OK** à deux reprises.
12. Cliquez sur **OK** pour fermer la boîte de dialogue **Paramètres**.
13. Laissez ouverte la boîte de dialogue **Propriétés de Allfiles (E:)** ; elle sera ouverte dans l'onglet **Clichés instantanés**.

▶ Tâche 2 : Créer plusieurs clichés instantanés d'un fichier

1. Basculez vers **LON-SVR1**.
2. Ouvrez l'Explorateur de fichiers.
3. Accédez au dossier **E:\Données\Development**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la barre d'outils Menu, cliquez sur **Accueil**, sur **Nouvel élément**, puis sur **Document texte**.
5. Tapez **Report** et appuyez sur Entrée.
6. Revenez à la boîte de dialogue **Propriétés de Allfiles (E:)** ; elle devrait être encore ouverte dans l'onglet **Clichés instantanés**. Cliquez sur **Créer**.

▶ Tâche 3 : Récupérer un fichier supprimé à partir d'un cliché instantané

1. Sur LON-SVR1, revenez à la fenêtre de l'Explorateur de fichiers.
2. Cliquez avec le bouton droit sur **Report.txt**, puis cliquez sur **Supprimer**.
3. Dans l'Explorateur de fichiers, cliquez avec le bouton droit sur le dossier **Development**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de Development**, cliquez sur l'onglet **Versions précédentes**.
5. Cliquez sur la version la plus récente du dossier pour **Development**, puis cliquez sur **Ouvrir**.
6. Confirmez que le fichier Report.txt se trouve dans le dossier, cliquez avec le bouton droit sur **Report.txt**, puis cliquez sur **Copier**.
7. Fermez la fenêtre de l'Explorateur de fichiers qui vient de s'ouvrir.
8. Dans la fenêtre de l'Explorateur de fichiers, cliquez avec le bouton droit sur le dossier **Development**, puis cliquez sur **Coller**.
9. Fermez l'Explorateur de fichiers.
10. Cliquez sur **OK** et fermez toutes les fenêtres ouvertes.

Résultats : À la fin de cet exercice, vous aurez activé des clichés instantanés sur le serveur de fichiers.

Exercice 3 : Création et configuration d'un pool d'imprimantes

▶ Tâche 1 : Installer le rôle serveur Services d'impression et de numérisation de document

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur le raccourci **Gestionnaire de serveur**.
2. Dans le Gestionnaire de serveur, dans la barre d'outils Menu, cliquez sur **Gérer**.
3. Cliquez sur **Ajouter des rôles et fonctionnalités**, puis sur **Suivant**.
4. Cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, cliquez sur le serveur où vous souhaitez installer les services d'impression et de numérisation de document. Le serveur par défaut est le serveur local. Cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services de documente et d'impression**. Dans la fenêtre Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant** dans la fenêtre **Sélectionner des rôles de serveurs**
7. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Dans la page **Services de documente et d'impression**, examinez les remarques destinées à l'administrateur, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans la page **Sélectionner des services de rôle**, cliquez sur **Suivant** jusqu'à ce que la page **Confirmer les sélections d'installation** s'affiche. Cliquez sur **Installer** pour installer les services de rôle requis.
10. Cliquez sur **Fermer**.

▶ Tâche 2 : Installer une imprimante

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestion de l'impression**.
2. Dans Développez **Serveurs d'impression**, développez **LON-SVR1**, cliquez avec le bouton droit sur **Imprimantes**, puis cliquez sur **Ajouter une imprimante**. L'Assistant Installation d'imprimante réseau démarre.
3. Dans la page Assistant Installation d'imprimante réseau, cliquez sur **Ajouter une imprimante TCP/IP ou de services Web par adresse IP ou nom d'hôte**, puis cliquez sur **Suivant**.
4. Modifiez le type de périphérique en spécifiant **Périphérique TCP/IP**.
5. Dans la zone **Nom de l'hôte ou adresse IP**, tapez **172.16.0.200**, désactivez la case à cocher **Détecter automatiquement le pilote d'imprimante à utiliser**, puis cliquez sur **Suivant**.
6. Sous Type de périphérique, cliquez sur **Generic Network Card**, puis cliquez sur **Suivant**.
7. Cliquez sur **Installer un nouveau pilote**, puis sur **Suivant**.
8. Cliquez sur **Microsoft** comme fabricant ; sous Imprimantes, cliquez sur **Microsoft XPS Class Driver**, puis cliquez sur **Suivant**.
9. Modifiez le nom de l'imprimante en spécifiant **Imprimante de filiale**, puis cliquez sur **Suivant**.
10. Cliquez sur **Suivant** deux fois pour accepter le nom d'imprimante et le nom de partage par défaut, et pour installer l'imprimante.
11. Cliquez sur **Terminer** pour fermer l'Assistant Installation d'imprimante réseau.
12. Dans le volet de navigation, cliquez sur **Imprimantes** si nécessaire, et dans la console de gestion de l'impression, cliquez avec le bouton droit sur **Imprimante de filiale**, puis cliquez sur **Activer l'impression directe pour les filiales**.
13. Dans la console de gestion de l'impression, cliquez avec le bouton droit sur **Imprimante de filiale**, puis sélectionnez **Propriétés**.
14. Cliquez sur l'onglet **Partage**, activez la case à cocher **Lister dans l'annuaire**, puis cliquez sur **OK**.

▶ Tâche 3 : Configurer le pool d'imprimantes

1. Dans la console de gestion de l'impression, sous **LON-SVR1**, cliquez avec le bouton droit sur **Ports**, puis cliquez sur **Ajouter un port**.
2. Dans la fenêtre Ports d'imprimante, cliquez sur **Standard TCP/IP Port**, puis cliquez sur **Ajouter un port**.
3. Dans l'Assistant Ajout de port imprimante TCP/IP standard, cliquez sur **Suivant**.
4. Dans le champ **Nom ou adresse IP de l'imprimante**, tapez **172.16.0.201**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Informations supplémentaires requises concernant le port, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Cliquez sur **Terminer** pour fermer l'Assistant Ajout de port imprimante TCP/IP standard.
7. Cliquez sur **Fermer** pour fermer la fenêtre Ports d'imprimante.
8. Dans la console de gestion de l'impression, cliquez sur **Imprimantes**, cliquez avec le bouton droit sur **Imprimante de filiale**, puis cliquez sur **Propriétés**.
9. Dans la page **Propriétés de Imprimante de filiale**, cliquez sur l'onglet **Ports**, activez la case à cocher **Activer le pool d'imprimante**, puis cliquez sur le port **172.16.0.201** pour le sélectionner comme deuxième port.
10. Cliquez sur **OK** pour fermer la page **Propriétés de Imprimante de filiale**.
11. Fermez la console de gestion de l'impression.

▶ Tâche 4 : Installer une imprimante sur un ordinateur client

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur **LON-CL1**, pointez dans l'angle inférieur gauche de l'écran et cliquez sur l'icône **Accueil**.
3. Dans la zone **Accueil**, tapez **Panneau de configuration** et appuyez sur **Entrée**.
4. Dans le Panneau de configuration, sous **Matériel et audio**, cliquez sur **Ajouter un périphérique**.
5. Dans la fenêtre **Ajouter un périphérique**, cliquez sur **Imprimante de filiale sur LON-SVR1**, puis cliquez sur **Suivant**. Le périphérique s'installe automatiquement.

▶ 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 **22410B-LON-SVR1**, 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 **22410B-LON-CL1** et **22410B-LON-DC1**.

Résultats : À la fin de cet exercice, vous aurez installé le rôle serveur Services de documents et d'impression et installé une imprimante avec le pool d'imprimantes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11 : Implémentation d'une stratégie de groupe

Atelier pratique : Implémentation d'une stratégie de groupe

Exercice 1 : Configuration d'un magasin central

▶ Tâche 1 : Afficher l'emplacement des modèles d'administration dans un objet de stratégie de groupe

1. Connectez-vous à LON-DC1 en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
3. Dans la Console de gestion des stratégies de groupe (GPMC), développez **Forêt : Adatum.com**, **Domaines**, **Adatum.com**, puis le dossier **Objets de stratégie de groupe**.
4. Cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
5. Dans l'Éditeur de gestion des stratégies de groupe, développez **Default Domain Policy**, **Configuration utilisateur**, puis **Stratégies** et cliquez sur **Modèles d'administration**.
6. Pointez la souris sur le dossier **Modèles d'administration** et notez que l'emplacement est **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local**.
7. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 2 : Créer un magasin central

1. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
2. Dans la fenêtre de l'Explorateur de fichiers, développez **Disque local (C :)**, **Windows**, **SYSVOL**, **sysvol**, puis **Adatum.com** et double-cliquez sur **Policies**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur une zone vide, cliquez sur **Nouveau**, puis sur **Dossier**.
4. Nommez le dossier **PolicyDefinitions**.

▶ Tâche 3 : Copier les modèles d'administration dans le magasin central

1. Dans l'Explorateur de fichiers, accédez à nouveau à **C:\Windows** et ouvrez le dossier **PolicyDefinitions**.
2. Sélectionnez tout le contenu du dossier **PolicyDefinitions**.

Conseil : cliquez sur le volet d'informations, puis utilisez les touches Ctrl+A pour sélectionner tout le contenu.

3. Cliquez avec le bouton droit sur la sélection, puis cliquez sur **Copier**.
4. Développez **Disque local (C :)**, **Windows**, **SYSVOL**, **sysvol**, puis **Adatum.com** et ouvrez le dossier **PolicyDefinitions**.
5. Cliquez avec le bouton droit sur la zone du dossier vide, puis cliquez sur **Coller**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Vérifier l'emplacement des modèles d'administration dans la console GPMC

1. Dans la console GPMC, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
2. Dans l'Éditeur de gestion des stratégies de groupe, développez **Stratégies**, pointez la souris sur le dossier **Modèles d'administration** et affichez le texte d'information local. Notez qu'il indique maintenant **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central**.
3. Fermez l'Éditeur de gestion des stratégies de groupe.

Résultats : À la fin de cet exercice, vous devez avoir configuré un magasin central.

Exercice 2 : Création d'objets de stratégie de groupe

▶ Tâche 1 : Créer un objet de stratégie de groupe Starter par défaut Restrictions de Windows Internet Explorer®

1. Dans la console GPMC, cliquez avec le bouton droit sur le dossier **Objets GPO Starter**, puis cliquez sur **Nouveau**.
2. Dans la boîte de dialogue **Nouvel objet GPO Starter**, dans le champ **Nom**, tapez **Restrictions d'Internet Explorer** et, dans le champ **Commentaire**, tapez **Cet objet de stratégie de groupe désactive l'onglet Général des Options Internet**, puis cliquez sur **OK**.

▶ Tâche 2 : Configurer l'objet de stratégie de groupe Starter Restrictions d'Internet Explorer

1. Dans la console GPMC, développez le dossier Objets GPO Starter, cliquez avec le bouton droit sur l'objet de stratégie de groupe **Restrictions d'Internet Explorer**, puis cliquez sur **Modifier**.
2. Dans l'Éditeur de gestion des stratégies de groupe, développez **Configuration utilisateur**, **Modèles d'administration**, puis cliquez sur **Tous les paramètres**.
3. Cliquez avec le bouton droit sur **Tous les paramètres**, puis cliquez sur **Options de filtres**.
4. Dans la boîte de dialogue **Options de filtres**, activez la case à cocher **Activer les filtres par mots clés**.
5. Dans le champ **Filtrer par le ou les mots :** tapez **onglet Général**.
6. Dans la liste déroulante, cliquez sur **Exacte**, puis cliquez sur **OK**.
7. Double-cliquez sur le paramètre **Désactiver l'onglet Général**, cliquez sur **Activé**, puis cliquez sur **OK**.
8. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 3 : Créer un objet de stratégie de groupe Restrictions d'Internet Explorer à partir de l'objet de stratégie de groupe Starter Restrictions d'Internet Explorer

1. Dans la console GPMC, cliquez avec le bouton droit sur le domaine, **Adatum.com**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
2. Dans la boîte de dialogue **Nouvel objet GPO**, dans le champ **Nom**, tapez **Restrictions d'IE**.
3. Sous Objets Starter GPO source, cliquez sur la zone déroulante, sélectionnez **Restrictions d'Internet Explorer**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Tester l'objet de stratégie de groupe pour les utilisateurs du domaine

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Brad** avec le mot de passe **Pa$$w0rd**.
2. Pointez la souris sur le coin inférieur droit de l'écran, puis, lorsque la barre latérale s'affiche, cliquez sur l'icône **Rechercher**.
3. Dans la zone de recherche **Applications**, tapez **Panneau de configuration**.
4. Dans les résultats **Applications**, cliquez sur **Panneau de configuration**.
5. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
6. Dans la boîte de dialogue **Réseau et Internet**, cliquez sur **Modifier la page d'accueil**. Une boîte de message s'affiche et vous informe que cette fonctionnalité a été désactivée.
7. Cliquez sur **OK** pour accepter le message.
8. Dans le Panneau de configuration, cliquez sur **Options Internet**. Vous pouvez remarquer que dans la boîte de dialogue **Propriétés Internet**, l'onglet **Général** ne s'affiche pas.
9. Fermez toutes les fenêtres, puis déconnectez-vous.

▶ Tâche 5 : Utiliser le filtrage de sécurité pour exempter le service informatique de la stratégie Restrictions d'Internet Explorer

1. Basculez vers LON-DC1.
2. Dans la console GPMC, développez le dossier **Objets de stratégie de groupe**, puis, dans le volet gauche, cliquez sur la stratégie **Restrictions d'IE**.
3. Dans le volet d'informations, cliquez sur l'onglet **Délégation**.
4. Sous l'onglet **Délégation**, cliquez sur le bouton **Avancé**.
5. Dans la boîte de dialogue **Paramètres de sécurité pour Restrictions d'IE**, cliquez sur **Ajouter**.
6. Dans le champ **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, tapez **IT**, puis cliquez sur **OK**.
7. Dans la boîte de dialogue **Paramètres de sécurité pour Restrictions d'IE**, cliquez sur le groupe **IT (ADATUM\IT)**, en regard de l'autorisation **Appliquer la stratégie de groupe**, activez la case à cocher **Refuser**, puis cliquez sur **OK**.
8. Cliquez sur **Oui** pour valider la boîte de dialogue **Sécurité de Windows**.

▶ Tâche 6 : Tester l'application de l'objet de stratégie de groupe pour les utilisateurs du service informatique

1. Connectez-vous à **LON-CL1** en tant que **Brad** avec le mot de passe **Pa$$w0rd**.
2. Pointez la souris sur le coin inférieur droit de l'écran, puis, lorsque la barre latérale s'affiche, cliquez sur l'icône **Rechercher**.
3. Dans la zone de recherche **Applications**, tapez **Panneau de configuration**.
4. Dans la fenêtre de résultats Applications, cliquez sur **Panneau de configuration**.
5. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
6. Dans la boîte de dialogue **Réseau et Internet**, cliquez sur **Modifier la page d'accueil**. La boîte de dialogue **Propriétés Internet** affiche l'onglet **Général** et tous les paramètres sont disponibles.
7. Fermez toutes les fenêtres, puis déconnectez-vous.

▶ Tâche 7 : Tester l'application de l'objet de stratégie de groupe pour les autres utilisateurs du domaine

1. Connectez-vous à **LON-CL1** en tant que **Boris** avec le mot de passe **Pa$$w0rd**.
2. Pointez la souris sur le coin inférieur droit de l'écran, puis, lorsque la barre latérale s'affiche, cliquez sur l'icône **Rechercher**.
3. Dans la zone de recherche **Applications**, tapez **Panneau de configuration**.
4. Dans la fenêtre de résultats Applications, cliquez sur **Panneau de configuration**.
5. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
6. Dans la boîte de dialogue **Réseau et Internet**, cliquez sur **Modifier la page d'accueil**. Une boîte de message s'affiche et vous informe que cette fonctionnalité a été désactivée.
7. Cliquez sur **OK** pour accepter le message.
8. Cliquez sur **Options Internet**. Dans la boîte de dialogue **Propriétés Internet**, vous pouvez remarquer que l'onglet **Général** ne s'affiche pas.
9. Fermez toutes les fenêtres, puis déconnectez-vous.

Résultats : À la fin de cet atelier pratique, vous devez avoir créé un objet de stratégie de groupe.

▶ 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 des ordinateurs virtuels, cliquez avec le bouton droit sur **22410B-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 **22410B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12 : Sécurisation des serveurs Windows à l'aide d'objets de stratégie de groupe

Atelier pratique A : Renforcement de la sécurité des ressources de serveur

Exercice 1 : Utilisation des stratégies de groupe pour sécuriser les serveurs membres

▶ Tâche 1 : Créer une unité d'organisation de serveurs membres et y placer les serveurs

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, dans le volet de navigation, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
3. Dans la fenêtre Nouvel objet - Unité d'organisation, dans la zone **Nom**, tapez **Unité d'organisation Serveurs membres**, puis cliquez sur **OK**.
4. Dans la console Utilisateurs et ordinateurs Active Directory, dans le volet de navigation, cliquez sur le conteneur **Computers**.
5. Maintenez enfoncée la touche Ctrl. Dans le volet d'informations, cliquez sur **LON-SVR1** et **LON-SVR2**, cliquez avec le bouton droit sur la sélection, puis cliquez sur **Déplacer**.
6. Dans la fenêtre Déplacer, cliquez sur **Unité d'organisation Serveurs membres**, puis cliquez sur **OK**.

▶ Tâche 2 : Créer un groupe Administrateurs de serveur

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, dans le volet de navigation, cliquez avec le bouton droit sur **Unité d'organisation Serveurs membres**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
3. Dans la fenêtre Nouvel objet - Groupe, dans le champ **Nom du groupe**, tapez **Administrateurs de serveur**, puis cliquez sur **OK**.

▶ Tâche 3 : Créer un objet de stratégie de groupe des paramètres de sécurité des serveurs membres et le lier à l'unité d'organisation Serveurs membres

1. Sur LON-DC1, dans la fenêtre **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la console de gestion des stratégies de groupe (GPMC), développez successivement **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez avec le bouton droit sur **Objets de stratégie de groupe** et cliquez sur **Nouveau**.
3. Dans la fenêtre **Nouvel objet GPO**, dans le champ **Nom**, tapez **Paramètres de sécurité des serveurs membres**, puis cliquez sur **OK**.
4. Dans la fenêtre Console de gestion des stratégies de groupe, cliquez avec le bouton droit sur **Unité d'organisation Serveurs membres**, puis cliquez sur **Lier un objet de stratégie de groupe existant**.
5. Dans la fenêtre **Sélectionner un objet GPO**, dans la fenêtre Objets de stratégie de groupe, cliquez sur **Paramètres de sécurité des serveurs membres**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer l'appartenance aux groupes pour les administrateurs locaux afin d'inclure les groupes Administrateurs de serveur et Administrateurs de domaine

1. Sur LON-DC1, dans la console de gestion des stratégies de groupe (GPMC), développez **Forêt : Adatum.com**, **Domaines**, **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
2. Dans la fenêtre Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez **Stratégies**, **Paramètres Windows** et **Paramètres de sécurité**, puis cliquez sur **Groupes restreints**.
3. Cliquez avec le bouton droit sur **Groupes restreints**, puis cliquez sur **Ajouter un groupe**.
4. Dans la boîte de dialogue **Ajouter un groupe**, dans le champ **Groupe**, tapez **Administrateurs**, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Administrateurs Propriétés**, en regard de **Membres de ce groupe**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Ajouter un membre**, tapez **ADATUM\Administrateurs de serveur**, puis cliquez sur **OK**.
7. En regard de **Membres de ce groupe**, cliquez sur **Ajouter**.
8. Dans la boîte de dialogue **Ajouter un membre**, tapez **ADATUM\Admins du domaine**, puis cliquez sur **OK** à deux reprises.
9. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 5 : Vérifier que les administrateurs d'ordinateur ont été ajoutés au groupe Administrateurs local

1. Basculez vers LON-SVR1.
2. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
4. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Gpupdate /force
```

5. Dans la fenêtre du Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestion de l'ordinateur**.
6. Dans la console **Gestion de l'ordinateur**, développez **Utilisateurs et groupes locaux**, cliquez sur **Groupes**, puis, dans le volet de droite, double-cliquez sur **Administrateurs**.
7. Confirmez que le groupe **Administrateurs** contient à la fois **ADATUM\Admins du domaine** et **ADATUM\Administrateurs de serveur** comme membres. Cliquez sur **Annuler**.
8. Fermez la console **Gestion de l'ordinateur**.

▶ Tâche 6 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour supprimer des utilisateurs de l'autorisation Permettre l'ouverture d'une session locale

1. Basculez vers **LON-DC1**.
2. Sur LON-DC1, dans la console GPMC, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez sur **Objets de stratégie de groupe**.
3. Dans le volet de droite, cliquez avec le bouton droit sur **Paramètres de sécurité des serveurs membres**, puis cliquez sur **Modifier**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la fenêtre Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité** et **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**.
5. Dans le volet de droite, cliquez avec le bouton droit sur **Permettre l'ouverture d'une session locale**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de : Permettre l'ouverture d'une session locale**, activez la case à cocher **Définir ces paramètres de stratégie**, puis cliquez sur **Ajouter un utilisateur ou un groupe**.
7. Dans la fenêtre **Ajouter un utilisateur ou un groupe**, tapez **Admins du domaine**, puis cliquez sur **OK**.
8. Cliquez sur **Ajouter un utilisateur ou un groupe**.
9. Dans la fenêtre **Ajouter un utilisateur ou un groupe**, tapez **Administrateurs**, puis cliquez sur **OK** à deux reprises.

▶ Tâche 7 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

1. Sur LON-DC1, dans la fenêtre Éditeur de gestion des stratégies de groupe, sous **Configuration de l'ordinateur**, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité** et **Stratégies locales**, puis cliquez sur **Options de sécurité**.
2. Dans le volet de droite, cliquez avec le bouton droit sur **Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré**, activez la case à cocher **Définir ces paramètres de stratégie**, assurez-vous que la case d'option **Activé** est sélectionnée, puis cliquez sur **OK**.
4. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 8 : Vérifier qu'un utilisateur ne disposant pas de droits d'administration ne peut pas se connecter à un serveur membre

1. Basculez vers **LON-SVR1**.
2. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
3. À l'invite Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Gpupdate /force
```

4. Déconnectez-vous de LON-SVR1.
5. Essayez de vous connecter à **LON-SVR1** en tant qu'**ADATUM\Adam** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Vérifiez que vous ne pouvez pas vous connecter à **LON-SVR1** et qu'un message d'erreur de connexion s'affiche.
7. Pour préparer l'exercice suivant, déconnectez-vous de LON-SVR1 et connectez-vous de nouveau à **LON-SVR1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Résultats : À la fin de cet exercice, vous devrez avoir utilisé les stratégies de groupe pour sécuriser les serveurs membres.

Exercice 2 : Audit de l'accès au système de fichiers

▶ Tâche 1 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer l'audit de l'accès aux objets

1. Basculez vers **LON-DC1**.
2. Connectez-vous à **LON-DC1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans la console GPMC, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez sur **Objets de stratégie de groupe**.
4. Dans le volet de droite, cliquez avec le bouton droit sur **Paramètres de sécurité des serveurs membres**, puis cliquez sur **Modifier**.
5. Dans la fenêtre Éditeur de gestion des stratégies de groupe, sous Configuration ordinateur, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité** et **Stratégies locales**, cliquez sur **Stratégie d'audit**, puis, dans le volet de droite, cliquez avec le bouton droit sur **Auditer l'accès aux objets**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de : Auditer l'accès aux objets**, activez la case à cocher **Définir ces paramètres de stratégie**, activez les deux cases à cocher **Réussite** et **Échec**, puis cliquez sur **OK**.
7. Déconnectez-vous de LON-DC1.

▶ Tâche 2 : Créer et partager un dossier

1. Basculez vers **LON-SVR1**.
2. Connectez-vous à **LON-SVR1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Sur LON-SVR1, dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
4. Dans la fenêtre de l'Explorateur de fichiers, dans le volet de navigation, cliquez sur **Ordinateur**.
5. Dans la fenêtre **Ordinateur**, double-cliquez sur **Disque local (C:)**, cliquez sur **Accueil**, cliquez sur **Nouveau dossier**, puis tapez **Marketing**.
6. Dans la fenêtre **Ordinateur**, cliquez avec le bouton droit sur le dossier **Marketing**, cliquez sur **Partager avec**, puis cliquez sur **Des personnes spécifiques**.
7. Dans la fenêtre Partage de fichiers, tapez **Adam**, puis cliquez sur **Ajouter**.
8. Passez le niveau d'autorisation à **Lecture/écriture**, cliquez sur **Partager**, puis cliquez sur **Terminé**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Activer l'audit sur le dossier Marketing pour les utilisateurs du domaine

1. Sur LON-SVR1, dans la fenêtre Disque local (C:), cliquez avec le bouton droit sur le dossier **Marketing**, puis cliquez sur **Propriétés**.
2. Dans la fenêtre Propriétés de Marketing, cliquez sur l'onglet **Sécurité**, puis sur **Avancé**.
3. Dans la fenêtre Paramètres de sécurité avancés pour Marketing, cliquez sur l'onglet **Audit**, cliquez sur **Continuer**, puis cliquez sur **Ajouter**.
4. Dans la fenêtre Audits pour Marketing, cliquez sur **Sélectionnez un principal**.
5. Dans la fenêtre Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes, dans le champ **Entrez le nom de l'objet à sélectionner**, tapez **Utilisateurs du domaine**, puis cliquez sur **OK**.
6. Dans la fenêtre Audits pour Marketing, dans le menu déroulant **Type**, sélectionnez **Tout**.
7. Dans la fenêtre Audits pour Marketing, sous la liste **Autorisations de base**, activez la case à cocher **Écriture**, puis cliquez sur **OK** trois fois.
8. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
9. À l'invite Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
gpupdate /force
```

10. Fermez la fenêtre Windows PowerShell.

▶ Tâche 4 : Créer un nouveau fichier dans le partage de fichiers à partir de LON-CL1

1. Basculez vers **LON-CL1**.
2. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Pointez dans l'angle inférieur droit de l'écran, cliquez sur l'icône **Rechercher**, puis, dans la zone **Rechercher**, tapez **cmd**.
4. Ouvrez une fenêtre d'invite de commandes et, à l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

5. Fermez la fenêtre d'invite de commandes.
6. Déconnectez-vous de LON-CL1, puis connectez-vous de nouveau en tant qu'**ADATUM\Adam** avec le mot de passe **Pa$$w0rd**.
7. Pointez dans l'angle inférieur droit de l'écran, cliquez sur l'icône **Rechercher**, puis, dans la zone **Rechercher**, tapez **\\LON-SVR1\Marketing**, puis appuyez sur Entrée.
8. Dans la fenêtre Marketing, cliquez sur **Accueil**, sur **Nouvel élément** et sur **Document texte**, puis, dans le champ nom de fichier, tapez **Employés**, puis appuyez sur Entrée.
9. Déconnectez-vous de LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Visualiser les résultats dans le journal de sécurité sur le contrôleur de domaine

1. Basculez vers LON-SVR1.
2. Dans la fenêtre **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Observateur d'événements**.
3. Dans la fenêtre de l'observateur d'événements, développez **Journaux Windows**, puis cliquez sur **Sécurité**.
4. Vérifiez que l'événement et les informations suivants s'affichent :
   - Source : **Microsoft Windows Security Auditing**
   - ID d'événement : **4663**
   - Catégorie de la tâche : **Système de fichiers**
   - Une tentative d'accès à un objet a été effectuée.

Résultats : À la fin de cet exercice, vous devrez avoir activé l'audit des accès au système de fichiers.

Exercice 3 : Audit des connexions au domaine

▶ Tâche 1 : Modifier l'objet GPO Stratégie de domaine par défaut

1. Basculez vers **LON-DC1**.
2. Connectez-vous à **LON-DC1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Sur LON-DC1, dans la barre des tâches, cliquez sur l'icône du **Gestionnaire de serveur**.
4. Dans la fenêtre **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
5. Sur LON-DC1, dans la console GPMC, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez sur **Objets de stratégie de groupe**.
6. Dans le volet de droite, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
7. Dans la fenêtre Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité** et **Stratégies locales**, puis cliquez sur **Stratégie d'audit**. Dans le volet de droite, cliquez avec le bouton droit sur **Auditer les événements de connexion aux comptes**, puis cliquez sur **Propriétés**.
8. Dans la boîte de dialogue **Propriétés de : Auditer les événements de connexion aux comptes**, activez la case à cocher **Définir ces paramètres de stratégie**, activez les deux cases à cocher **Réussite** et **Échec**, puis cliquez sur **OK**.
9. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
11. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

▶ Tâche 2 : Exécuter GPUpdate

1. Basculez vers **LON-CL1**.
2. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
4. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
5. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

6. Fermez la fenêtre d'invite de commandes et déconnectez-vous de LON-CL1.

▶ Tâche 3 : Se connecter à LON-CL1 avec un mot de passe incorrect

- Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Adam** avec le mot de passe **password**.

Remarque : Ce mot de passe est intentionnellement incorrect afin de générer une entrée de journal de sécurité indiquant qu'une tentative de connexion infructueuse a été effectuée.

▶ Tâche 4 : Examiner les journaux des événements sur LON-DC1

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis cliquez sur **Observateur d'événements**.
2. Dans la fenêtre de l'**observateur d'événements**, développez **Journaux Windows**, puis cliquez sur **Sécurité**.
3. Examinez les journaux des événements pour rechercher le message suivant : « **ID d'événement 4771 La pré-authentification Kerberos a échoué. Informations sur le compte : ID de sécurité : ADATUM\Adam**. »

▶ Tâche 5 : Se connecter à LON-CL1 avec le mot de passe correct

- Connectez-vous à LON-CL1 en tant qu'**ADATUM\Adam** avec le mot de passe **Pa$$w0rd**.

Remarque : Ce mot de passe est correct et vous devriez pouvoir vous connecter avec succès en tant qu'**Adam**.

▶ Tâche 6 : Examiner les journaux des événements sur LON-DC1

1. Connectez-vous à **LON-DC1**.
2. Dans la fenêtre Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Observateur d'événements**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la fenêtre de l'**observateur d'événements**, développez **Journaux Windows**, puis cliquez sur **Sécurité**.
4. Examinez les journaux des événements pour rechercher le message suivant : « **ID d'événement 4624 L'ouverture de session d'un compte s'est correctement déroulée. Nouvelle connexion : ID de sécurité : ADATUM\Adam**. »

Résultats : À la fin de cet exercice, vous devrez avoir activé l'audit des connexions au domaine.

▶ Pour préparer l'atelier suivant

- Pour préparer l'atelier pratique suivant, laissez les ordinateurs virtuels s'exécuter.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Configuration d'AppLocker et du Pare-feu Windows

Exercice 1 : Configuration des stratégies AppLocker

▶ Tâche 1 : Créer une unité d'organisation pour les ordinateurs clients

1. Basculez vers **LON-DC1**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans la console Utilisateurs et ordinateurs Active Directory®, dans le volet de navigation, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
4. Dans la fenêtre Nouvel objet - Unité d'organisation, tapez **Unité d'organisation Ordinateurs clients**, puis cliquez sur **OK**.

▶ Tâche 2 : Placer LON-CL1 dans l'unité d'organisation Ordinateurs clients

1. Sur LON-DC1, dans la console Utilisateurs et ordinateurs Active Directory, dans le volet de navigation, cliquez sur le conteneur **Computers**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-CL1**, puis cliquez sur **Déplacer**.
3. Dans la fenêtre Déplacer, cliquez sur **Unité d'organisation Ordinateurs clients**, puis cliquez sur **OK**.

▶ Tâche 3 : Créer un objet GPO de contrôle de logiciels et le lier à l'unité d'organisation Ordinateurs clients

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la console GPMC, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez avec le bouton droit sur **Objets de stratégie de groupe** et cliquez sur **Nouveau**.
3. Dans la fenêtre **Nouvel objet GPO**, dans la zone de texte **Nom**, tapez **Objet GPO Contrôle de logiciels**, puis cliquez sur **OK**.
4. Dans le volet de droite, cliquez avec le bouton droit sur **Objet GPO Contrôle de logiciels**, puis cliquez sur **Modifier**.
5. Dans la fenêtre Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Stratégies de contrôle de l'application**, puis **AppLocker**.
6. Sous **AppLocker**, cliquez avec le bouton droit sur **Règles de l'exécutable**, puis cliquez sur **Créer des règles par défaut**.
7. Répétez l'étape précédente pour les **Règles Windows Installer**, les **Règles de script** et les **Règles d'applications empaquetées**.
8. Dans le volet de navigation, cliquez sur **AppLocker**, puis, dans le volet de droite, cliquez sur **Configurer la mise en application des règles**.
9. Dans la boîte de dialogue **Propriétés de AppLocker**, sous **Règles de l'exécutable**, activez la case à cocher **Configuré**, puis, dans le menu déroulant, sélectionnez **Auditer uniquement**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Répétez l'étape précédente pour les **Règles Windows Installer**, les **Règles de script** et les **Règles d'applications empaquetées**, puis cliquez sur **OK**.
11. Dans l'Éditeur de gestion des stratégies de groupe, développez **Configuration ordinateur**, **Stratégies**, **Paramètres Windows** et **Paramètres de sécurité**, cliquez sur **Services système**, puis double-cliquez sur **Identité de l'application**.
12. Dans la boîte de dialogue **Propriétés de : Identité de l'application**, cliquez sur **Définir ce paramètre de stratégie**, sous **Sélectionnez le mode de démarrage du service**, cliquez sur **Automatique**, puis cliquez sur **OK**.
13. Fermez l'Éditeur de gestion des stratégies de groupe.
14. Dans la console GPMC, cliquez avec le bouton droit sur **Unité d'organisation Ordinateurs clients**, puis cliquez sur **Lier un objet de stratégie de groupe existant**.
15. Dans la fenêtre **Sélectionner un objet GPO**, dans la liste **Objets de stratégie de groupe**, cliquez sur **Objet GPO Contrôle de logiciels**, puis cliquez sur **OK**.

▶ Tâche 4 : Exécuter GPUpdate

1. Basculez vers **LON-CL1**.
2. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
3. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
4. Dans la fenêtre d'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

5. Fermez la fenêtre d'invite de commandes.
6. Pointez dans l'angle inférieur droit de l'écran, cliquez sur l'icône **Paramètres**, sur **Marche/Arrêt**, puis sur **Redémarrer**.

▶ Tâche 5 : Exécuter app1.bat dans le dossier C:\CustomApp

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
3. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
4. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpresult /R
```

   Examinez le résultat de la commande et vérifiez que **Objet GPO Contrôle de logiciels** est affiché sous Paramètres de l'ordinateur, Objets Stratégie de groupe appliqués. Si **Objet GPO Contrôle de logiciels** n'est pas affiché, redémarrez LON-CL1 et répétez les étapes 1 à 4.

5. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
6. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
7. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
C:\CustomApp\app1.bat
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 6 : Afficher les événements AppLocker® dans un journal des événements

1. Sur LON-CL1, pointez dans l'angle inférieur droit de l'écran, cliquez sur l'icône **Rechercher**, puis, dans la zone **Rechercher**, tapez **eventvwr.msc**, puis appuyez sur Entrée.
2. Dans la fenêtre de l'**observateur d'événements**, développez **Journaux des applications et des services**, **Microsoft**, **Windows**, puis **AppLocker**.
3. Cliquez sur **Script** et examinez le journal des événements 8005 qui contient le texte suivant : **L'exécution de %OSDRIVE%\CUSTOMAPP\APP1.BAT a été autorisée**.

Remarque : Si aucun événement ne s'affiche, assurez-vous que le service Identité de l'application a démarré et réessayez.

▶ Tâche 7 : Créer une règle qui autorise l'exécution des logiciels figurant dans un emplacement spécifique

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la fenêtre Gestion des stratégies de groupe, développez le nœud **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **Objet GPO Contrôle de logiciels**, puis cliquez sur **Modifier**.
3. Accédez à l'emplacement de paramétrage suivant : **Configuration ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/Stratégies de contrôle de l'application/AppLocker**.
4. Cliquez avec le bouton droit sur **Règles de script** et cliquez sur **Créer une règle**.
5. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
6. Dans la page **Autorisations**, activez la case d'option **Autoriser**, puis cliquez sur **Suivant**.
7. Dans la page **Conditions**, activez la case d'option **Chemin d'accès**, puis cliquez sur **Suivant**.
8. Dans la page **Chemin d'accès**, dans le champ **Chemin d'accès**, tapez le chemin d'accès **%OSDRIVE%\CustomApp\app1.bat**, puis cliquez sur **Suivant**.
9. Dans la page **Exceptions**, cliquez sur **Suivant**.
10. Dans la page **Nom et description**, dans le champ **Nom**, tapez **Règle d'application personnalisée**, puis cliquez sur **Créer**.

▶ Tâche 8 : Modifier l'objet GPO Contrôle de logiciels pour appliquer des règles

1. Dans la fenêtre Objet GPO Contrôle de logiciels, dans le volet de navigation, cliquez sur **AppLocker**, puis, dans le volet de droite, cliquez sur **Configurer la mise en application des règles**.
2. Dans la boîte de dialogue **Propriétés de AppLocker**, sous **Règles de l'exécutable**, activez la case à cocher **Configuré**, puis, dans le menu déroulant, cliquez sur **Appliquer les règles**.
3. Répétez l'étape précédente pour les **Règles Windows Installer**, les **Règles de script** et les **Règles d'applications empaquetées**, puis cliquez sur **OK**.
4. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 9 : Vérifier qu'une application peut encore être exécutée

1. Basculez vers **LON-CL1**.
2. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
3. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
4. Dans la fenêtre d'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

5. Fermez la fenêtre d'invite de commandes.
6. Pointez dans l'angle inférieur droit de l'écran, cliquez sur l'icône **Paramètres**, sur **Marche/Arrêt**, puis sur **Redémarrer**.
7. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Tony** avec le mot de passe **Pa$$w0rd**.
8. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
9. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
10. Dans la fenêtre d'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
C:\customapp\app1.bat
```

▶ Tâche 10 : Vérifier qu'une application ne peut pas être exécutée

1. Sur LON-CL1, dans la barre des tâches, cliquez sur l'icône de l'**Explorateur des fichiers**.
2. Dans la fenêtre de l'Explorateur de fichiers, dans le volet de navigation, cliquez sur **Ordinateur**.
3. Dans la fenêtre **Ordinateur**, double-cliquez sur **Disque local (C:)**, double-cliquez sur le dossier **CustomApp**, cliquez avec le bouton droit sur **app1.bat**, puis cliquez sur **Copier**.
4. Dans la fenêtre **CustomApp**, dans le volet de navigation, cliquez avec le bouton droit sur le dossier **Documents**, puis cliquez sur **Coller**.
5. Dans une fenêtre d'invite de commandes, tapez **C:\Users\Tony\Documents\app1.bat** et appuyez sur Entrée.
6. Vérifiez que les applications ne peuvent pas être exécutées à partir du dossier **Documents** et que le message suivant s'affiche : « **Ce programme est bloqué par une stratégie de groupe. Pour plus d'informations, contactez votre administrateur système.** »
7. Fermez toutes les fenêtres, puis déconnectez-vous de LON-CL1.

Résultats : À la fin de cet exercice, vous devrez avoir configuré des stratégies AppLocker pour tous les utilisateurs dont les comptes d'ordinateur sont situés dans l'unité d'organisation des ordinateurs clients. Les stratégies que vous avez configurées doivent autoriser ces utilisateurs à exécuter les applications figurant dans les dossiers C:\Windows et C:\Program Files, et à exécuter l'application personnalisée app1.bat dans le dossier C:\CustomApp.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT REQUIREMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration du Pare-feu Windows

▶ Tâche 1 : Créer un groupe nommé Serveurs d'applications

1. Basculez vers **LON-DC1**.
2. Dans la fenêtre Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans la console Utilisateurs et ordinateurs Active Directory, dans le volet de navigation, cliquez avec le bouton droit sur **Unité d'organisation Serveurs membres**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
4. Dans la fenêtre Nouvel objet - Groupe, dans le champ **Nom du groupe**, tapez **Serveurs d'applications**, puis cliquez sur **OK**.

▶ Tâche 2 : Ajouter LON-SVR1 en tant que membre du groupe

1. Dans la console Utilisateurs et ordinateurs Active Directory, dans le volet de navigation, cliquez sur l'**unité d'organisation Serveurs membres**, dans le volet d'informations, cliquez avec le bouton droit sur le groupe **Serveurs d'applications**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : Serveurs d'applications**, cliquez sur l'onglet **Membres**, puis cliquez sur **Ajouter**.
3. Dans Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes, cliquez sur **Types d'objets**, sur **des ordinateurs**, puis sur **OK**.
4. Dans la zone **Entrez les noms des objets à sélectionner**, tapez **LON-SVR1**, puis cliquez sur **OK**.
5. Dans la fenêtre **Propriétés de : Serveurs d'applications**, cliquez sur **OK**.

▶ Tâche 3 : Créer un nouvel objet GPO Serveurs d'applications

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la console GPMC, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez avec le bouton droit sur **Objets de stratégie de groupe** et cliquez sur **Nouveau**.
3. Dans la fenêtre **Nouvel objet GPO**, dans le champ **Nom**, tapez **Objet GPO Serveurs d'applications**, puis cliquez sur **OK**.
4. Dans la console GPMC, cliquez avec le bouton droit sur **Objet GPO Serveurs d'applications**, puis cliquez sur **Modifier**.
5. Dans l'Éditeur de gestion des stratégies de groupe, sous **Configuration de l'ordinateur**, développez successivement **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité** et **Pare-feu Windows avec fonctions avancées de sécurité**, puis cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité - LDAP://CN={GUID}**.
6. Dans l'Éditeur de gestion des stratégies de groupe, cliquez sur **Règles de trafic entrant**.
7. Cliquez avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**.
8. Dans l'Assistant Nouvelle règle de trafic entrant, dans la page **Type de règle**, cliquez sur **Personnalisée**, puis sur **Suivant**.
9. Dans la page **Programme**, cliquez sur **Suivant**.
10. Dans la page **Protocole et ports**, dans la liste **Type de protocole**, cliquez sur **TCP**.

11. Dans la liste **Port local**, cliquez sur **Ports spécifiques**, puis, dans la zone de texte, tapez **8080** et cliquez sur **Suivant**.
12. Dans la page **Étendue**, cliquez sur **Suivant**.
13. Dans la page **Action**, cliquez sur **Autoriser la connexion**, puis cliquez sur **Suivant**.
14. Dans la page **Profil**, désactivez les deux cases à cocher **Privé** et **Public**, puis cliquez sur **Suivant**.
15. Dans la page **Nom**, dans la zone **Nom**, tapez **Règle de pare-feu de service de serveur d'applications**, puis cliquez sur **Terminer**.
16. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 4 : Lier l'objet GPO Serveurs d'applications à l'unité d'organisation Serveurs membres

1. Sur LON-DC1, dans la console GPMC, cliquez avec le bouton droit sur **Unité d'organisation Serveurs membres**, puis cliquez sur **Lier un objet de stratégie de groupe existant**.
2. Dans la fenêtre **Sélectionner un objet GPO**, dans la liste **Objets de stratégie de groupe**, cliquez sur **Objet GPO Serveurs d'applications**, puis cliquez sur **OK**.

▶ Tâche 5 : Utiliser le filtrage de sécurité pour limiter l'objet GPO Serveurs d'applications aux membres du groupe Serveurs d'applications

1. Sur LON-DC1, dans la console GPMC, cliquez sur **Unité d'organisation Serveurs membres**.
2. Développez **Unité d'organisation Serveurs membres**, puis cliquez sur le lien **Objet GPO Serveurs d'applications**.
3. Dans la zone de message **Console de gestion des stratégies de groupe**, cliquez sur **OK**.
4. Dans le volet de droite, sous Filtrage de sécurité, cliquez sur **Utilisateurs authentifiés**, puis sur **Supprimer**.
5. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
6. Dans le volet d'informations, sous Filtrage de sécurité, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs ou des groupes**, tapez **Serveurs d'applications**, puis cliquez sur **OK**.

▶ Tâche 6 : Exécuter GPUpdate sur LON-SVR1

1. Basculez vers **LON-SVR1** et connectez-vous en tant qu'**ADATUM\Administrateur**.
2. Pointez dans l'angle inférieur droit de l'écran, puis cliquez sur l'icône **Rechercher**.
3. Dans la zone **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
4. Dans la fenêtre d'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

5. Fermez la fenêtre d'invite de commandes.
6. Redémarrez **LON-SVR1**, puis connectez-vous à nouveau en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 7 : Afficher les règles de pare-feu sur LON-SVR1

1. Basculez vers **LON-SVR1**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.
3. Dans la fenêtre Pare-feu Windows avec fonctions avancées de sécurité, cliquez sur **Règles de trafic entrant**.
4. Dans le volet de droite, vérifiez que la **règle de pare-feu de service de serveur d'applications** que vous avez créée auparavant à l'aide d'une stratégie de groupe est configurée.
5. Vérifiez que vous ne pouvez pas modifier la **règle de pare-feu de service de serveur d'applications**, car elle est configurée via une stratégie de groupe.

Résultats : À la fin de cet exercice, vous devrez avoir utilisé une stratégie de groupe pour configurer le Pare-feu Windows avec fonctions avancées de sécurité afin de créer des règles pour les serveurs d'applications.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®**.
2. Dans la liste des **ordinateurs virtuels**, cliquez avec le bouton droit sur **22410B-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 **22410B-LON-SVR1** et **22410B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 13 : Implémentation de la virtualisation de serveur avec Hyper-V

Atelier pratique : Implémentation de la virtualisation de serveur avec Hyper-V

Exercice 1 : Installation du rôle Hyper V sur un serveur

▶ Tâche 1 : Installer le rôle Hyper-V sur un serveur

1. Sur LON-HOST1, dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
2. Dans le volet Propriétés, cliquez sur le lien **Adresse IPv4 attribuée par DHCP, compatible IPv6**.
3. Dans la boîte de dialogue **Connexions réseau**, cliquez avec le bouton droit sur l'objet réseau, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés**, cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de : Protocole Internet version 4 (TCP/IPv4)**, sous l'onglet **Général**, cliquez sur **Utiliser l'adresse IP suivante**, puis configurez ce qui suit :
   - Adresse IP : **172.16.0.31**
   - Masque de sous-réseau : **255.255.0.0**
   - Passerelle par défaut : **172.16.0.1**
6. Sous l'onglet **Général**, cliquez sur **Utiliser l'adresse de serveur DNS suivante**, puis configurez comme suit :
   - Serveur DNS préféré : **172.16.0.10**
7. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés**.
8. Dans la boîte de dialogue **Propriétés de Ethernet**, cliquez sur **Fermer**.
9. Fermez la boîte de dialogue **Connexions réseau**.
10. Dans la console du Gestionnaire de serveur, à partir du menu **Gérer**, cliquez sur **Ajouter des rôles et fonctionnalités**.
11. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
12. Dans la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
13. Dans la page **Sélectionner le serveur de destination**, vérifiez que LON-HOST1 est sélectionné, puis cliquez sur **Suivant**.
14. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez **Hyper-V**.
15. Dans la fenêtre Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Ajouter des fonctionnalités**.
16. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
17. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
18. Dans la page **Hyper-V**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

19. Dans la page **Créer des commutateurs virtuels**, vérifiez qu'aucune sélection n'a été faite, puis cliquez sur **Suivant**.
20. Dans la page **Migration d'ordinateur virtuel**, cliquez sur **Suivant**.
21. Dans la page **Emplacements par défaut**, vérifiez l'emplacement des **Emplacements par défaut**, puis cliquez sur **Suivant**.
22. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Redémarrer automatiquement le serveur de destination, si nécessaire**.
23. Dans la boîte de dialogue Assistant Ajout de rôles et de fonctionnalités, consultez le message relatif aux redémarrages automatiques, puis cliquez sur **Oui**.
24. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
25. Au bout de quelques minutes, le serveur redémarre automatiquement. Assurez-vous de redémarrer l'ordinateur à partir du menu de démarrage comme **22410B-LON-HOST1**. L'ordinateur redémarrera plusieurs fois.

▶ Tâche 2 : Terminer l'installation du rôle Hyper-V et vérifier les paramètres

1. Connectez-vous à **LON-HOST1** à l'aide du compte **Administrateur** avec mot de passe **Pa$$word**.
2. Une fois l'installation de **Hyper-V** terminée, cliquez sur **Fermer** pour fermer l'Assistant Ajout de rôles et de fonctionnalités.
3. Sur le bureau, cliquez sur l'icône du Gestionnaire de serveur dans la barre des tâches.
4. Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Gestionnaire Hyper-V**.
5. Dans la console du Gestionnaire Hyper-V, cliquez sur **LON-HOST1**.
6. Dans la console du Gestionnaire Hyper-V, dans le volet Actions, avec **LON-HOST1** sélectionné, cliquez sur **Paramètres Hyper-V**.
7. Dans la boîte de dialogue **Paramètres Hyper-V de LON-HOST1**, cliquez sur l'élément **Clavier**. Vérifiez que le Clavier est défini sur l'option **Utiliser sur l'ordinateur virtuel**.
8. Dans la boîte de dialogue **Paramètres Hyper-V pour LON-HOST1**, cliquez sur l'élément **Disques durs virtuels**. Vérifiez que l'emplacement du dossier par défaut pour le stockage des fichiers-de disque dur virtuel est **C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks**, puis cliquez sur **OK**.

Résultats : À la fin de cet exercice, vous aurez installé le rôle Hyper-V sur un serveur physique.

Exercice 2 : Configuration d'un réseau virtuel

▶ Tâche 1 : Configurer le réseau externe

1. Dans la console du Gestionnaire Hyper-V, cliquez sur **LON-HOST1**.
2. Dans le menu **Actions**, cliquez sur **Gestionnaire de commutateur virtuel**.
3. Dans la boîte de dialogue **Gestionnaire de commutateur virtuel pour LON-HOST1**, cliquez sur **Nouveau commutateur réseau virtuel**. Vérifiez que l'option **Externe** est sélectionnée, puis cliquez sur **Créer le commutateur virtuel**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la zone Propriétés du commutateur virtuel, entrez les informations suivantes, puis cliquez sur **OK** :
   - Nom : **Commutateur pour la carte externe**
   - Réseau externe : mappé à la carte réseau physique de l'ordinateur hôte. (Varie selon l'ordinateur hôte)
5. Dans la boîte de dialogue **Appliquer les modifications réseau**, lisez l'avertissement, puis cliquez sur **Oui**.

▶ Tâche 2 : Créer un réseau privé

1. Dans le Gestionnaire de serveur, dans le menu **Outils**, ouvrez le **Gestionnaire Hyper-V**, puis cliquez sur **LON-HOST1**.
2. Dans le menu **Actions**, cliquez sur **Gestionnaire de commutateur virtuel**.
3. Sous Commutateurs virtuels, cliquez sur **Nouveau commutateur réseau virtuel**.
4. Sous Créer le commutateur virtuel, cliquez sur **Privé**, puis sur **Créer le commutateur virtuel**.
5. Dans la section Propriétés du commutateur virtuel de la boîte de dialogue Gestionnaire de commutateur virtuel, configurez les paramètres suivants, puis cliquez sur **OK** :
   - Nom : **Réseau privé**
   - Type de connexion : **Réseau privé**

▶ Tâche 3 : Créer un réseau interne

1. Dans le Gestionnaire de serveur, dans le menu **Outils**, ouvrez le **Gestionnaire Hyper-V**, puis cliquez sur **LON-HOST1**.
2. Dans le menu **Actions**, cliquez sur **Gestionnaire de commutateur virtuel**.
3. Sous Commutateurs virtuels, cliquez sur **Nouveau commutateur réseau virtuel**.
4. Sous Créer un commutateur virtuel, cliquez sur **Interne**, puis sur **Créer le commutateur virtuel**.
5. Dans la section Propriétés du commutateur virtuel de la boîte de dialogue **Gestionnaire de commutateur virtuel**, configurez les paramètres suivants, puis cliquez sur **OK** :
   - Nom : **Réseau interne**
   - Type de connexion : **Réseau interne**

▶ Tâche 4 : Configurer la plage d'adresses MAC (Media Access Control)

1. Dans le Gestionnaire de serveur, dans le menu **Outils**, ouvrez le **Gestionnaire Hyper-V**, puis cliquez sur **LON-HOST1**.
2. Dans le menu **Actions**, cliquez sur **Gestionnaire de commutateur virtuel**.
3. Sous Paramètres du réseau global, cliquez sur **Plage d'adresses MAC**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans les paramètres de la plage d'adresse MAC, configurez les valeurs suivantes, puis cliquez sur **OK** :
   - Minimum : **00-15-5D-0F-AB-A0**
   - Maximum : **00-15-5D-0F-AB-EF**
5. Fermez la console du **Gestionnaire Hyper-V**.

Résultats : À la fin de cet exercice, vous aurez configuré des options de commutateur virtuel sur un serveur Windows Server 2012 physiquement déployé qui exécute le rôle Hyper-V.

Exercice 3 : Création et configuration d'un ordinateur virtuel

▶ Tâche 1 : Créer des disques VHD de différenciation

1. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
2. Cliquez sur **Ordinateur**, développez le lecteur **E**, développez **Program Files**, développez **Microsoft Learning**, puis **Base**.

Remarque : La lettre du lecteur peut être différente selon le nombre de lecteurs sur l'ordinateur hôte physique.

3. Dans le dossier **Base**, vérifiez que le fichier image **Base12A-WS12-TMP_FR.vhd** du disque dur est présent.
4. Cliquez sur l'onglet **Démarrer**, puis cliquez deux fois sur l'icône **Nouveau dossier** pour créer deux nouveaux dossiers. Cliquez avec le bouton droit sur chaque dossier, et renommez les dossiers comme suit :
   - **LON-GUEST1**
   - **LON-GUEST2**
5. Fermez l'Explorateur de fichiers.
6. Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Gestionnaire Hyper-V**.
7. Dans le volet Actions de la console du Gestionnaire Hyper-V, cliquez sur **Nouveau**, puis sur **Disque dur**.
8. Dans l'Assistant Nouveau disque dur virtuel, sur la page **Avant de commencer**, cliquez sur **Suivant**.
9. Dans la page **Choisir le format de disque**, cliquez sur **VHD**, puis sur **Suivant**.
10. Dans la page **Choisir le type de disque**, cliquez sur **Différenciation**, puis sur **Suivant**.
11. Dans la page **Spécifier le nom et l'emplacement**, indiquez les informations suivantes, puis cliquez sur **Suivant** :
    - Nom : **LON-GUEST1.vhd**
    - Emplacement : **E:\Program Files\Microsoft Learning\Base\LON-GUEST1**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

12. Dans la page **Configurer un disque**, tapez l'emplacement : **E:\Program Files\Microsoft Learning\Base\Base12A-WS12-TMP_FR.vhd**, puis cliquez sur **Terminer**.
13. Sur le bureau, dans la barre des tâches, cliquez sur l'icône Windows PowerShell®.
14. À l'invite de commande Windows PowerShell, tapez la commande suivante pour importer le module Hyper-V, puis appuyez sur Entrée :

```
Import-Module Hyper-V
```

15. À l'invite de Windows PowerShell, saisissez la commande suivante pour créer un nouveau disque VHD de différenciation à utiliser avec LON-GUEST2, puis appuyez sur Entrée :

```
New-VHD "E:\Program Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd"
-ParentPath "E:\Program Files\Microsoft Learning\Base\Base12A-WS12-TMP_FR.vhd"
```

16. Fermez Windows PowerShell.
17. Dans le volet Actions de la console du Gestionnaire Hyper-V, cliquez sur **Inspecter le disque**.
18. Dans la boîte de dialogue **Ouvrir**, accédez à **E:\Program Files\Microsoft Learning\Base\LON-GUEST2**, cliquez sur **LON-GUEST2.vhd**, puis sur **Ouvrir**.
19. Dans la boîte de dialogue **Propriétés du disque dur virtuel**, vérifiez que **LON-GUEST2.vhd** est configuré comme disque VHD de différenciation avec **E:\Program Files\Microsoft Learning\Base\Base12A-WS12TMP_FR.vhd** comme parent, puis cliquez sur **Fermer**.

▶ Tâche 2 : Créer des ordinateurs virtuels

1. Dans le Gestionnaire de serveur, dans le menu **Outils**, ouvrez le **Gestionnaire Hyper-V**, puis cliquez sur **LON-HOST1**.
2. Dans le volet Actions de la console du Gestionnaire Hyper-V, cliquez sur **Nouveau**, puis sur **Ordinateur virtuel**.
3. Dans l'Assistant Nouvel ordinateur virtuel, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Spécifier le nom et l'emplacement**, cliquez sur **Stocker l'ordinateur virtuel à un autre emplacement**, entrez les valeurs suivantes, puis cliquez sur **Suivant** :
   - Nom : **LON-GUEST1**
   - Emplacement : **E:\Program Files\Microsoft Learning\Base\LON-GUEST1**
5. Dans la page **Affecter la mémoire**, entrez la valeur **1024 Mo**, sélectionnez l'option **Utiliser la mémoire dynamique pour cet ordinateur virtuel**, puis cliquez sur **Suivant**.
6. Dans la page **Configurer la mise en réseau**, pour la connexion, cliquez sur **Réseau privé**, puis sur **Suivant**.
7. Dans la page **Connecter un disque dur virtuel**, cliquez sur **Utiliser un disque dur virtuel existant**. Cliquez sur **Parcourir**, accédez à **E:\Program Files\Microsoft Learning\Base\LON-GUEST1\LON-GUEST1.vhd**, cliquez sur **Ouvrir**, puis sur **Terminer**.
8. Sur le bureau, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
9. À l'invite de commande Windows PowerShell, tapez la commande suivante et appuyez sur Entrée pour importer le module Hyper-V :

```
Import-Module Hyper-V
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. À l'invite de commande Windows PowerShell, tapez la commande suivante pour créer un nouvel ordinateur virtuel nommé **LON-GUEST2** :

```
New-VM -Name LON-GUEST2 -MemoryStartupBytes 1024MB -VHDPath "E:\Program
Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd" -SwitchName "Réseau privé"
```

11. Fermez Windows PowerShell.
12. Dans la console Gestionnaire Hyper-V, cliquez sur **LON-GUEST2**.
13. Dans le volet Actions, sous **LON-GUEST2**, cliquez sur **Paramètres**.
14. Dans la boîte de dialogue **Paramètres pour LON-GUEST2 sur LON-HOST1**, cliquez sur **Action de démarrage automatique**, et définissez l'action de démarrage automatique sur **Rien**.
15. Dans la boîte de dialogue **Paramètres pour LON-GUEST2 sur LON-HOST1**, cliquez sur **Action d'arrêt automatique**, et définissez l'action d'arrêt automatique sur **Arrêter le système d'exploitation invité**.
16. Cliquez sur **OK** pour fermer la boîte de dialogue **Paramètres pour LON-GUEST2 sur LON-HOST1**.

▶ Tâche 3 : Activer le contrôle des ressources

1. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. À l'invite de commande Windows PowerShell, entrez la commande suivante pour importer le module Hyper-V et appuyez sur Entrée :

```
Import-Module Hyper-V
```

3. À l'invite Windows PowerShell, entrez les commandes suivantes pour activer le contrôle des ressource sur les ordinateurs virtuels, en appuyant sur Entrée à la fin de chaque ligne :

```
Enable-VMResourceMetering LON-GUEST1
Enable-VMResourceMetering LON-GUEST2
```

Résultats : À la fin de cet exercice, vous aurez déployé deux ordinateurs virtuels distincts en utilisant un fichier VHD préparé avec sysprepped comme disque parent pour deux disques VHD de différenciation.

Exercice 4 : Utilisation d'instantanés d'ordinateur virtuel

▶ Tâche 1 : Déployer Windows Server 2012 sur un ordinateur virtuel

1. Dans la console Gestionnaire Hyper-V, cliquez sur **LON-GUEST1**.
2. Dans le volet Actions, cliquez sur **Démarrer**.
3. Double-cliquez sur **LON-GUEST1** pour ouvrir la fenêtre Connexion à un ordinateur virtuel.
4. Dans LON-GUEST1 sur LON-HOST1, fenêtre Connexion à un ordinateur virtuel, procédez comme suit :
   - Dans la page **Paramètres**, activez la case à cocher **J'accepte les termes du contrat de licence pour l'utilisation de Windows**, puis cliquez sur **Accepter**.
   - Dans la page **Paramètres**, cliquez sur **Suivant** pour accepter les paramètres Région et langue.
   - Dans la page **Paramètres**, tapez le mot de passe **Pa$$w0rd** deux fois, puis cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans LON-GUEST1 sur LON-HOST1, fenêtre Connexion à un ordinateur virtuel, menu Actions, cliquez sur **Ctrl+Alt+Suppr**.
6. Ouvrez une session sur l'ordinateur virtuel avec le compte **Administrateur** et le mot de passe **Pa$$w0rd**.
7. Sur l'ordinateur virtuel, dans la console du Gestionnaire de serveur, cliquez sur **Serveur local**, puis cliquez sur le nom attribué de manière aléatoire en regard du nom de l'ordinateur.
8. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier**.
9. Dans le champ **Nom de l'ordinateur**, saisissez **LON-GUEST1**, puis cliquez sur **OK**.
10. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, cliquez sur **OK**.
11. Cliquez sur **Fermer** pour fermer la boîte de dialogue **Propriétés système**.
12. Dans la boîte de dialogue **Microsoft Windows**, cliquez sur **Redémarrer maintenant**.

▶ Tâche 2 : Créer un instantané d'ordinateur virtuel

1. Ouvrez une session sur l'ordinateur virtuel **LON-GUEST1** avec le compte **Administrateur** et le mot de passe **Pa$$w0rd**.
2. Dans la console Gestionnaire de serveur, cliquez sur le nœud **Serveur local**, puis vérifiez que le nom de l'ordinateur est défini sur **LON-GUEST1**.
3. Dans la fenêtre Connexion à un ordinateur virtuel, dans le menu **Action**, cliquez sur **Capture instantanée**.
4. Dans la boîte de dialogue **Nom de la capture instantanée**, tapez le nom **Before Change**, puis cliquez sur **Oui**.

▶ Tâche 3 : Modifier l'ordinateur virtuel

1. Dans la console du Gestionnaire de serveur, cliquez sur **Serveur local**, puis en regard de **Nom de l'ordinateur**, cliquez sur **LON-GUEST1**.
2. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier**.
3. Dans le champ **Nom de l'ordinateur**, tapez **LON-Computer1**, puis cliquez sur **OK**.
4. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, cliquez sur **OK**.
5. Fermez la boîte de dialogue **Propriétés système**.
6. Dans la boîte de dialogue **Microsoft Windows**, cliquez sur **Redémarrer maintenant**.
7. Reconnectez-vous à l'ordinateur virtuel **LON-GUEST1** avec le compte **Administrateur** et le mot de passe **Pa$$w0rd**.
8. Dans la console Gestionnaire de serveur, cliquez sur le nœud **Serveur local**, puis vérifiez que le nom de serveur est défini sur **LON-Computer1**.

▶ Tâche 4 : Rétablir l'instantané d'ordinateur virtuel existant

1. Dans la fenêtre Connexion à un ordinateur virtuel, dans le menu **Action**, cliquez sur **Rétablir**.
2. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
3. Dans la console Gestionnaire de serveur, dans le nœud Serveur local, dans la liste **Ordinateurs virtuels**, vérifiez que le **Nom de l'ordinateur** est maintenant défini sur **LON-GUEST1**.

▶ Tâche 5 : Afficher les données de contrôle des ressources

1. Sur LON-HOST1, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. À l'invite de commande Windows PowerShell, entrez la commande suivante et appuyez sur Entrée pour importer le module Hyper-V :

```
Import-Module Hyper-V
```

3. À l'invite de commande Windows PowerShell, entrez la commande suivante et appuyez sur Entrée pour extraire les informations de contrôle des ressources :

```
Measure-VM LON-GUEST1
```

4. Notez les chiffres relatifs à l'UC moyenne, à la mémoire vive moyenne et à l'utilisation totale de disque.
5. Fermez la fenêtre Windows PowerShell.

▶ Tâche 6 : Rétablir les ordinateurs virtuels

À la fin de cet atelier, redémarrez l'ordinateur dans Windows Server 2008 R2.

1. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. Dans la fenêtre Windows PowerShell, entrez la commande suivante et appuyez sur Entrée :

```
Shutdown /r /t 5
```

3. À partir du Gestionnaire de démarrage Windows, cliquez sur **Windows Server 2008 R2**.

Résultats : À la fin de cet exercice, vous aurez utilisé des instantanés d'ordinateur virtuel pour effectuer une récupération à la suite d'une erreur de configuration d'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT