Microsoft® Official Course

Module 8

Installation, configuration et résolution des problèmes du rôle de serveur NPS

Microsoft

Vue d'ensemble du module

- Installation et configuration d'un serveur NPS
- Configuration de clients et de serveurs RADIUS
- Méthodes d'authentification NPS
- Analyse et résolution des problèmes d'un serveur NPS

Leçon 1: Installation et configuration d'un serveur NPS

- Qu'est-ce qu'un serveur NPS ?
- Démonstration : Installation du rôle Serveur NPS (Network Policy Server)
- Outils de configuration d'un serveur NPS
- Démonstration : Configuration des paramètres NPS généraux

Qu'est-ce qu'un serveur NPS ?

- Un serveur NPS Windows Server 2012 fournit les fonctions suivantes :
  - Serveur RADIUS. Le serveur NPS centralise l'authentification, l'autorisation et la gestion de comptes pour les connexions d'accès à distance et VPN, ainsi que pour les connexions sans fil et reposant sur des commutateurs d'authentification
  - Proxy RADIUS. Vous configurez des stratégies de demande de connexion qui spécifient, d'une part, les demandes de connexion transmises par le serveur NPS à d'autres serveurs RADIUS et, d'autre part, les serveurs RADIUS auxquels vous souhaitez transmettre les demandes de connexion
  - Serveur de stratégie NAP. Le serveur NPS évalue les déclarations d'intégrité (SoH) envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau qui souhaitent se connecter au réseau

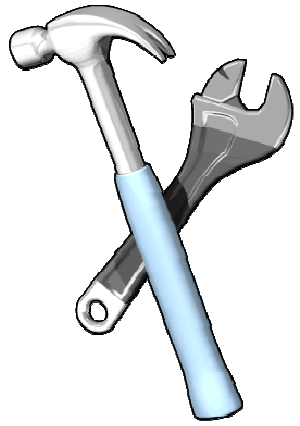
Démonstration : Installation du rôle Serveur NPS (Network Policy Server)

Dans cette démonstration, vous allez apprendre à :

- Installer le rôle NPS
- Inscrire NPS dans AD DS

Outils de configuration d'un serveur NPS

- Outils disponibles pour la gestion d'un serveur NPS :
  - Composant logiciel enfichable MMS (Microsoft Management Console) Serveur NPS
  - Outil en ligne de commande netsh :
    - Commandes de serveur NPS
    - Commandes de client RADIUS
    - Commandes de stratégie de demande de connexion
    - Commandes de groupe de serveurs RADIUS distants
    - Commandes de stratégie réseau
    - Commandes de protection d'accès réseau
    - Commandes de comptes
  - Windows PowerShell



Démonstration : Configuration des paramètres NPS généraux

Dans cette démonstration, vous allez apprendre à :

- Configurer un serveur RADIUS pour des connexions VPN
- Enregistrer la configuration

Leçon 2: Configuration de clients et de serveurs RADIUS

- Qu'est-ce qu'un client RADIUS ?
- Qu'est-ce qu'un proxy RADIUS ?
- Démonstration : Configuration d'un client RADIUS
- Qu'est-ce qu'une stratégie de demande de connexion ?
- Configuration du traitement des demandes de connexion
- Démonstration : Création d'une stratégie de demande de connexion

Qu'est-ce qu'un client RADIUS ?

Le serveur NPS est un serveur RADIUS

- Les clients RADIUS sont des serveurs d'accès réseau, par exemple :
  - Points d'accès sans fil
  - Commutateurs d'authentification 802.1x
  - Serveurs VPN
  - Serveurs d'accès à distance
- Les clients RADIUS envoient des demandes de connexion et des messages de comptes aux serveurs RADIUS pour l'authentification, l'autorisation et la gestion de comptes

Qu'est-ce qu'un proxy RADIUS ?

- Un proxy RADIUS reçoit des tentatives de connexion des clients RADIUS et les transmet au serveur RADIUS approprié ou à un autre proxy RADIUS pour d'autres opérations de routage
- Un proxy RADIUS est requis pour :
  - Sous-traiter des services d'accès réseau à distance, VPN ou sans fil par des fournisseurs de services
  - Authentifier et autoriser les comptes d'utilisateurs qui ne sont pas des membres Active Directory
  - Authentifier et autoriser les utilisateurs en utilisant une base de données qui n'est pas une base de données de comptes Windows
  - Équilibrer la charge des demandes de connexion entre plusieurs serveurs RADIUS
  - Fournir le service RADIUS aux fournisseurs de services sous-traités et limiter les types de trafic par le biais du pare-feu

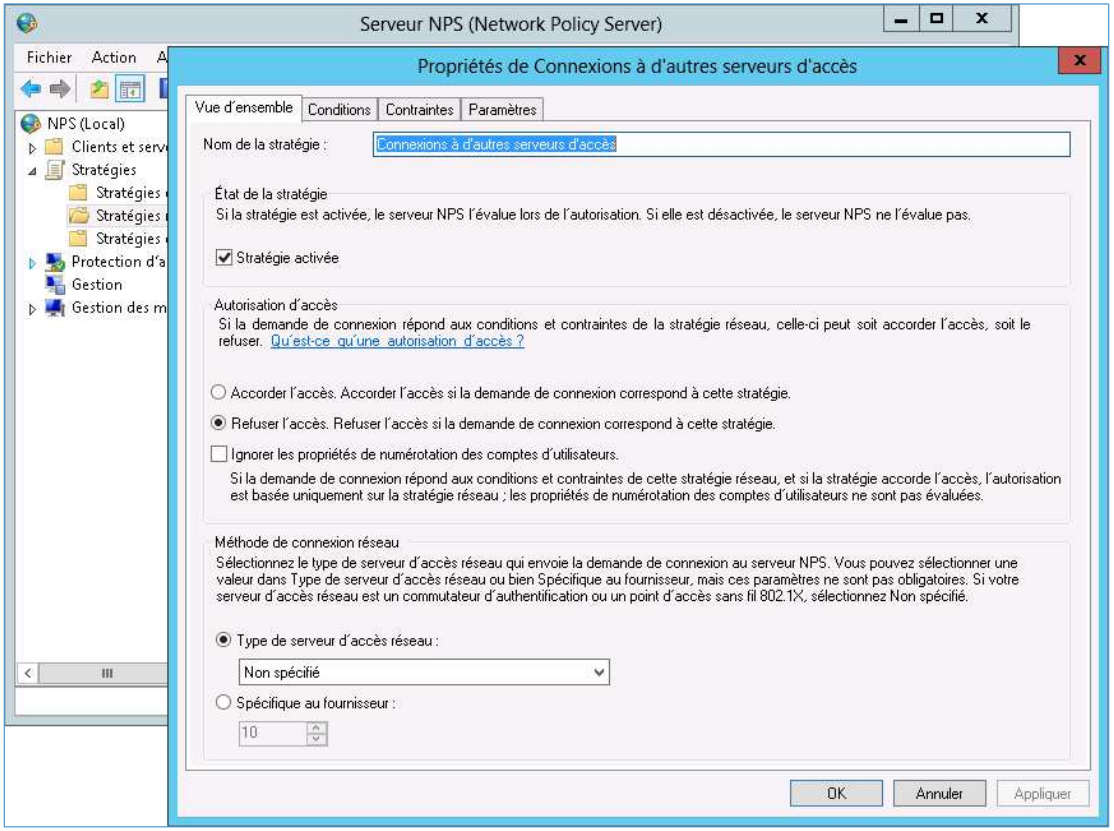
Démonstration : Configuration d'un client RADIUS

- Au cours de cette démonstration, vous allez apprendre à configurer un client RADIUS

Qu'est-ce qu'une stratégie de demande de connexion ?

- Les stratégies de demande de connexion sont des jeux de conditions et de paramètres qui désignent les serveurs RADIUS qui authentifient et autorisent les demandes de connexion que le serveur NPS reçoit des clients RADIUS

- Stratégies de demande de connexion disponibles :
  - Des conditions, telles que :
    - Protocole de trames
    - Type de service
    - Type de tunnel
    - Restrictions relatives aux jours et aux heures
  - Des paramètres, tels que :
    - Authentification
    - Gestion de comptes
    - Manipulation d'attribut
    - Paramètres avancés



Configuration du traitement des demandes de connexion

Configuration	Description
Authentification locale / RADIUS	• L'authentification locale est effectuée par rapport à la base de données des comptes de sécurité locale ou Active Directory. Des stratégies de connexion existent sur ce serveur • L'authentification RADIUS transmet la demande de connexion à un serveur RADIUS à des fins d'authentification par rapport à une base de données de sécurité. Le serveur RADIUS gère un magasin central de toutes les stratégies de connexion
Groupes de serveurs RADIUS	Utilisés lorsqu'un ou plusieurs serveurs RADIUS sont capables de gérer des demandes de connexion. La charge des demandes de connexion est équilibrée selon des critères spécifiés lors de la création du groupe de serveurs RADIUS si plusieurs serveurs RADIUS figurent dans le groupe
Ports par défaut pour la gestion de comptes et l'authentification avec RADIUS	Les ports requis pour les demandes de comptes et d'authentification qui sont transmises à un serveur RADIUS sont UDP 1812/1645 et UDP 1813/1646

Démonstration : Création d'une stratégie de demande de connexion

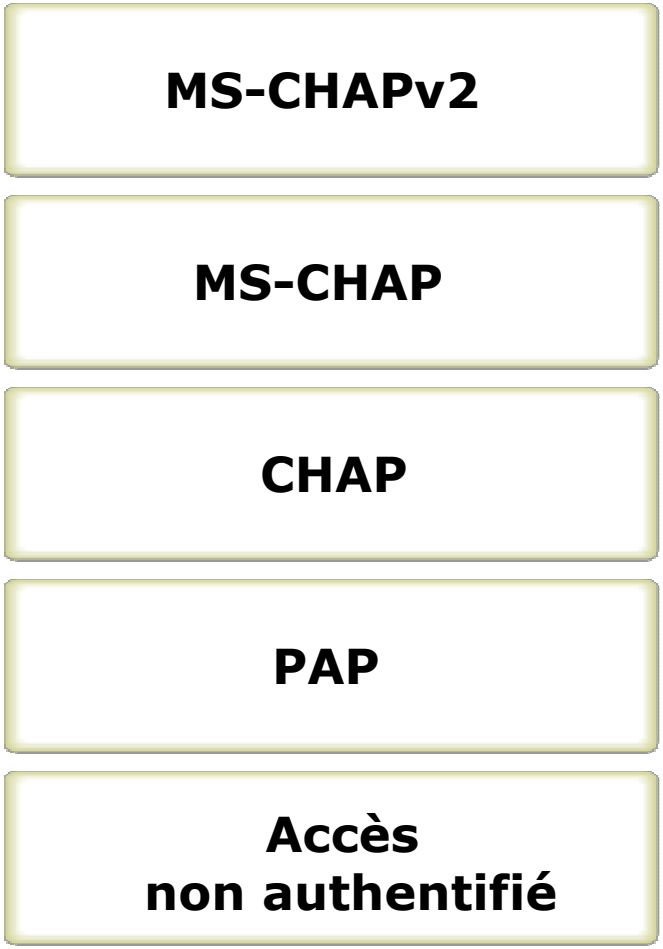
- Dans cette démonstration, vous allez apprendre à créer une stratégie de demande de connexion VPN

Leçon 3: Méthodes d'authentification NPS

- Méthodes d'authentification par mot de passe
- Utilisation de certificats pour l'authentification
- Certificats requis pour l'authentification
- Déploiement de certificats pour l'authentification PEAP et EAP

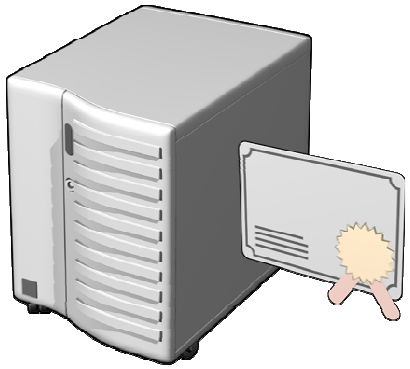
Méthodes d'authentification par mot de passe

- Méthodes d'authentification d'un serveur NPS allant de la plus sécurisée à la moins sécurisée :



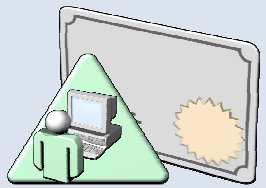
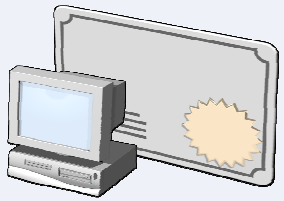
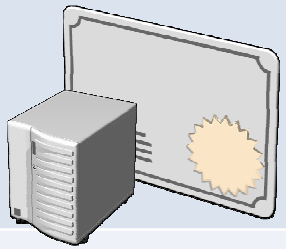
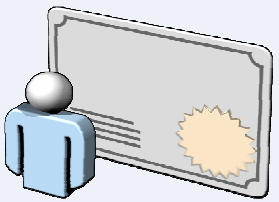
Utilisation de certificats pour l'authentification

- Le serveur NPS vous permet d'utiliser des certificats pour l'authentification de l'accès réseau car ils :
  - Offrent une sécurité renforcée
  - Éliminent la nécessité d'une authentification par mot de passe moins sécurisée



Certificats requis pour l'authentification

Les certificats suivants sont requis pour déployer l'authentification basée sur les certificats dans le serveur NPS :

Description	du certificat
	Certificat d'autorité de certification dans le magasin de certificats Autorités de certification racine approuvées pour l'ordinateur local et l'utilisateur actuel
	Certificat d'ordinateur client dans le magasin de certificats du client
	Certificat de serveur dans le magasin de certificats du serveur NPS
	Certificat utilisateur sur une carte à puce

Déploiement de certificats pour l'authentification PEAP et EAP

- Pour les comptes d'ordinateurs et d'utilisateurs de domaine, utilisez la fonctionnalité d'inscription automatique dans la Stratégie de groupe
- Pour l'inscription de membres n'appartenant pas au domaine, un administrateur doit demander un certificat d'utilisateur ou d'ordinateur à l'aide de l'outil Inscription de l'autorité de certification via le Web
- L'administrateur doit enregistrer le certificat d'utilisateur ou d'ordinateur sur une disquette ou tout autre support amovible, puis installer manuellement le certificat sur l'ordinateur n'appartenant pas au domaine
- L'administrateur peut distribuer des certificats utilisateur sur une carte à puce

Leçon 4: Analyse et résolution des problèmes d'un serveur NPS

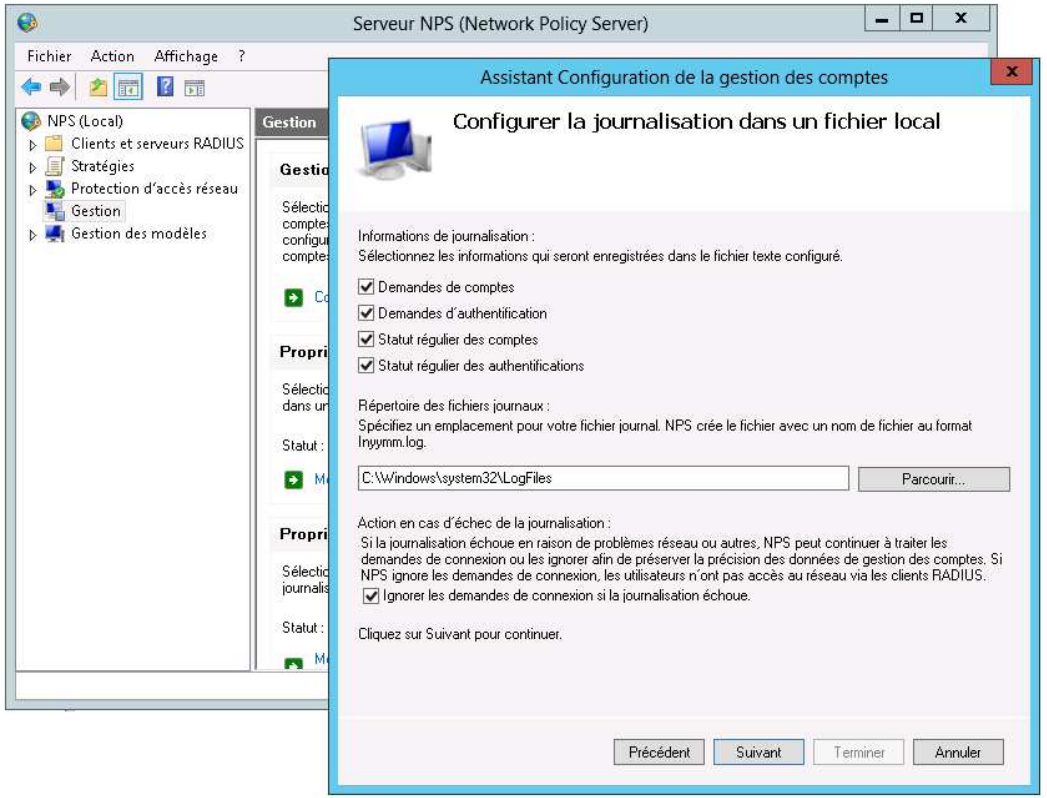
- Méthodes d'analyse du serveur NPS
- Enregistrement de la gestion des comptes NPS
- Configuration de la journalisation SQL Server
- Configuration des événements NPS à enregistrer dans l'Observateur d'événements

Méthodes d'analyse du serveur NPS

- Méthodes d'analyse du serveur NPS disponibles :
  - Journalisation des événements
    - Cette méthode est le processus de journalisation des événements NPS dans le journal des événements système
    - Cette méthode est utile pour auditer et résoudre les problèmes de tentatives de connexion
  - Journalisation des demandes d'authentification et de comptes d'utilisateurs
    - Cette méthode est utile pour l'analyse des connexions et la facturation
    - Cette méthode peut être au format texte
    - Cette méthode peut être dans un format de base de données dans une instance SQL

Enregistrement de la gestion des comptes NPS

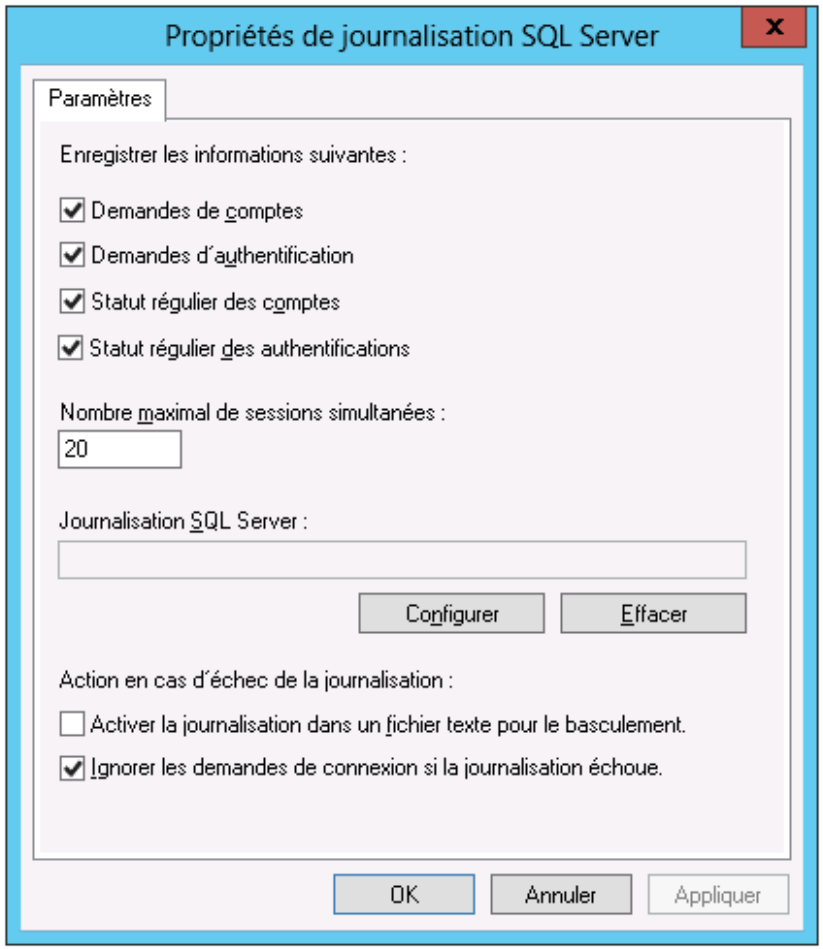
- Utilisez la console NPS pour configurer la journalisation :
  1. Dans le menu **Outils d'administration**, ouvrez le **serveur NPS**
  2. Dans l'arborescence de la console, cliquez sur **Gestion des comptes**
  3. Dans le volet d'informations, cliquez sur **Modifier les propriétés du fichier journal**
- Les fichiers journaux doivent être stockés sur une partition séparée de la partition système



Configuration de la journalisation SQL Server

Vous pouvez utiliser SQL pour journaliser les données de gestion de comptes RADIUS :

- La base de données SQL Server doit avoir une procédure stockée nommée report_event
- Le serveur NPS met en forme les données de comptes en tant que document XML
- La base de données SQL Server peut se trouver sur un ordinateur local ou sur un serveur distant



Configuration des événements NPS à enregistrer dans l'Observateur d'événements

- Comment configurer l'enregistrement d'événements NPS dans l'Observateur d'événements ?
  - Le serveur NPS est configuré par défaut pour enregistrer les échecs de connexion et les connexions réussies dans le journal des événements
    - Vous pouvez modifier ce comportement sous l'onglet Général de la page Propriétés de la stratégie réseau
  - Les événements courants d'échec de demande se composent des demandes refusées ou ignorées par le serveur NPS ; les événements ayant réussi ou échoué sont enregistrés
- Qu'est-ce que la journalisation Schannel et comment la configurer ?
  - Schannel est un fournisseur SSP (Security Support Provider) qui prend en charge un jeu de protocoles de sécurité Internet
  - Vous pouvez configurer la journalisation Schannel dans la clé de Registre suivante :
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging

Atelier pratique : Installation et configuration d'un serveur NPS

- Exercice 1 : Installation et configuration de NPS pour prendre en charge RADIUS
- Exercice 2 : Configuration et test d'un client RADIUS

Informations d'ouverture de session

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-RTR 22411B-LON-CL2
Nom d'utilisateur	**ADATUM\Administrateur**
Mot de passe	**Pa$$w0rd**

Durée approximative : 60 minutes

Scénario d'atelier pratique

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à London pour assister le bureau de Londres et d’autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012

A. Datum développe sa solution d'accès distant dans toute l'organisation. Cette opération nécessite la mise en place de plusieurs serveurs VPN situés à différents endroits pour assurer la connectivité des employés. Vous êtes chargé de mettre en place les tâches nécessaires pour prendre en charge ces connexions VPN

Révision de l'atelier pratique

- Quel est le rôle d'un proxy RADIUS ?
- Qu'est-ce qu'un client RADIUS ? Donnez des exemples de clients RADIUS

Contrôle des acquis et éléments à retenir

- Questions de contrôle des acquis
- Outils