Microsoft® Official Course

Module 9

Implémentation de la protection d'accès réseau

Vue d'ensemble du module

- Vue d'ensemble de la protection d'accès réseau
- Vue d'ensemble des processus de contrainte de mise en conformité NAP
- Configuration de NAP
- Analyse et résolution des problèmes du système NAP

Leçon 1: Vue d'ensemble de la protection d'accès réseau

- Qu'est-ce que la protection d'accès réseau ?
- Scénarios de protection d'accès réseau
- Méthodes de contrainte de mise en conformité NAP
- Architecture de la plateforme NAP

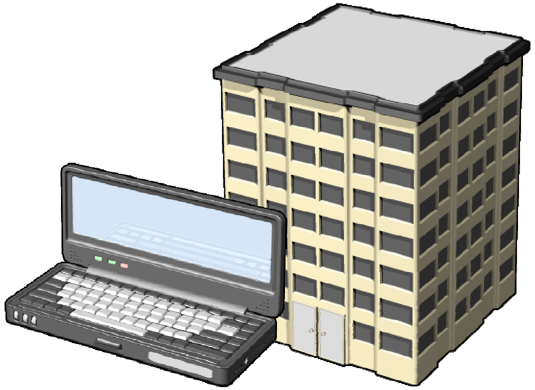
Qu'est-ce que la protection d'accès réseau ?

- La protection d'accès réseau permet de :
  - Mettre en vigueur des stratégies de spécification d'intégrité sur les ordinateurs clients
  - Vérifier que les ordinateurs clients sont conformes aux stratégies
  - Assurer la mise à jour des ordinateurs qui ne répondent pas aux spécifications d'intégrité
- La protection d'accès réseau ne permet pas de :
  - Empêcher des utilisateurs autorisés équipés d'ordinateurs conformes d'effectuer des opérations malveillantes sur le réseau
  - Restreindre l'accès réseau des ordinateurs exécutant des versions de Windows antérieures à Windows XP SP2 lorsque des règles d'exception sont configurées pour ces ordinateurs

Scénarios de protection d'accès réseau

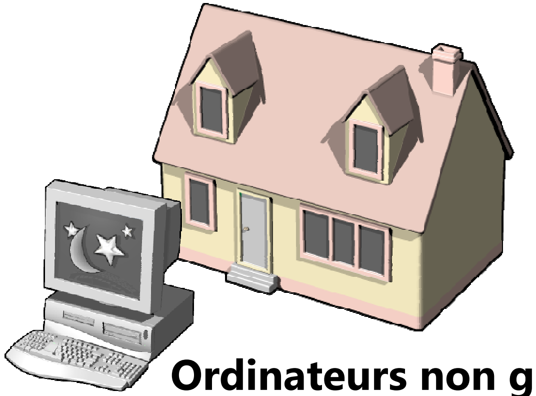
La protection d'accès réseau vous aide à vérifier l'état d'intégrité des éléments suivants :

Ordinateurs portables des employés itinérants



Ordinateurs portables des visiteurs

Ordinateurs de bureau

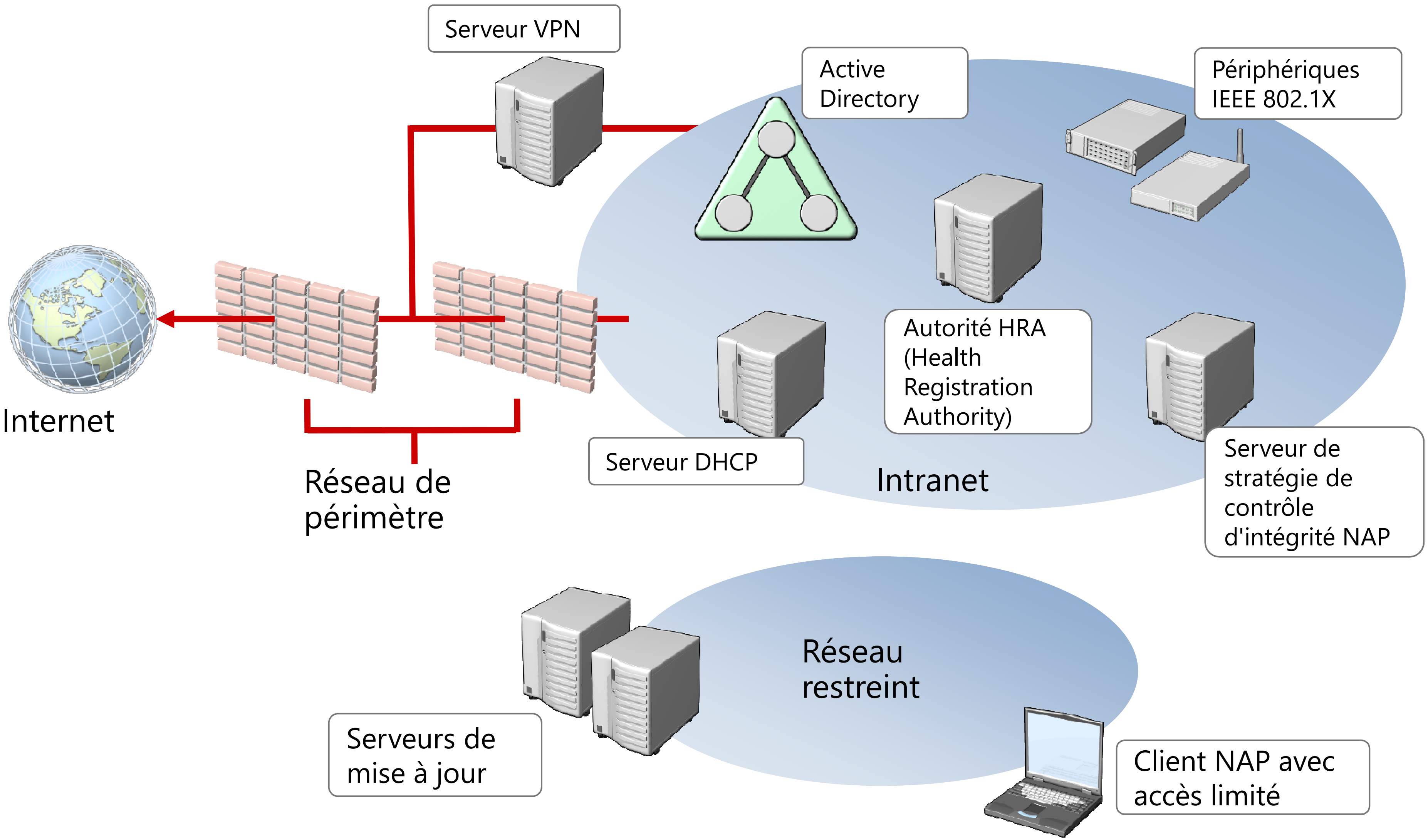


Ordinateurs non gérés destinés à un usage privé

Méthodes de contrainte de mise en conformité NAP

Méthode	Points clés
Contrainte de mise en conformité IPsec pour les communications protégées par IPsec	• L'ordinateur doit être conforme pour pouvoir communiquer avec d'autres ordinateurs conformes • Il s'agit du type de contrainte de mise en conformité NAP le plus puissant, qui peut être appliqué en fonction d'une adresse IP ou d'un numéro de port de protocole
Contrainte de mise en conformité 802.1X pour les connexions câblées ou sans fil authentifiées par le protocole IEEE 802.1X	• L'ordinateur doit être conforme pour pouvoir obtenir un accès illimité via une connexion 802.1X (commutateur d'authentification ou point d'accès)
Contrainte de mise en conformité VPN pour les connexions d'accès à distance	• L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité via une connexion de service d'accès à distance
DirectAccess	• L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité • Pour les ordinateurs non conformes, l'accès est restreint à un groupe défini de serveurs d'infrastructure
Contrainte de mise en conformité par DHCP pour la configuration d'adresse basée sur DHCP	• L'ordinateur doit être conforme pour pouvoir recevoir une configuration d'adresse IPv4 à accès illimité de DHCP • Il s'agit de la forme de contrainte de mise en conformité NAP la plus faible

Architecture de la plateforme NAP



Serveur VPN

Active Directory

Périphériques IEEE 802.1X

Internet

Autorité HRA (Health Registration Authority)

Serveur DHCP

Réseau de périmètre

Intranet

Serveur de stratégie de contrôle d'intégrité NAP

Réseau restreint

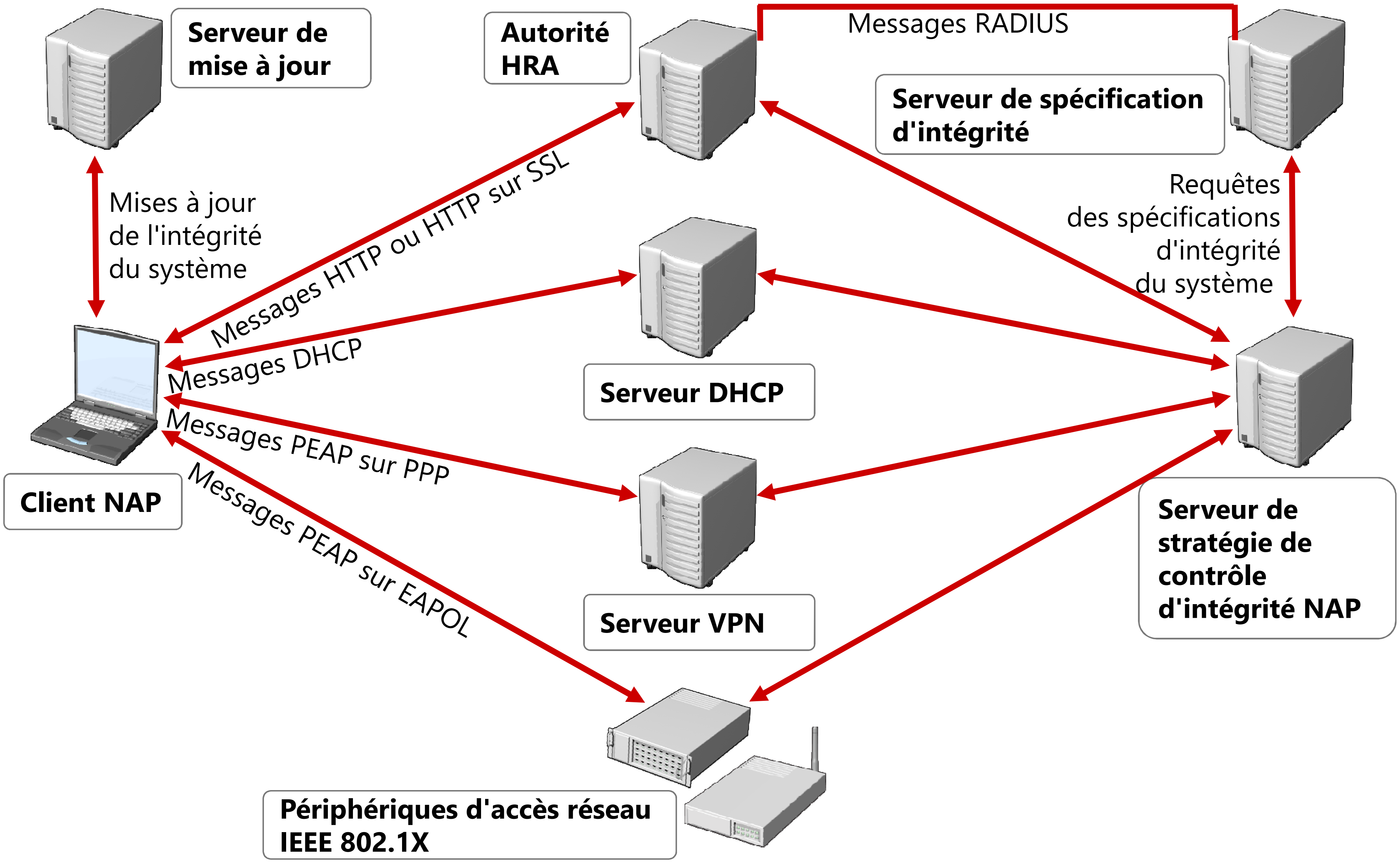
Serveurs de mise à jour

Client NAP avec accès limité

Leçon 2: Vue d'ensemble des processus de contrainte de mise en conformité NAP

- Processus de contrainte de mise en conformité NAP
- Contrainte de mise en conformité IPsec
- Contrainte de mise en conformité 802.1X
- Contrainte de mise en conformité VPN
- Contrainte de mise en conformité DHCP

Processus de contrainte de mise en conformité NAP



Serveur de mise à jour

Autorité HRA

Messages RADIUS

Serveur de spécification d'intégrité

Mises à jour de l'intégrité du système

Messages HTTP ou HTTP sur SSL

Requêtes des spécifications d'intégrité du système

Messages DHCP

Serveur DHCP

Client NAP

Messages PEAP sur PPP

Messages PEAP sur EAPOL

Serveur VPN

Serveur de stratégie de contrôle d'intégrité NAP

Périphériques d'accès réseau IEEE 802.1X

Contrainte de mise en conformité IPsec

- Points clés de la contrainte de mise en conformité NAP IPsec :
  - La contrainte de mise en conformité NAP IPsec comprend un serveur de certificats d'intégrité et un client de contrainte de mise en conformité NAP IPsec
    - Le serveur de certificats d'intégrité délivre des certificats X.509 aux clients en quarantaine lorsque ces derniers prouvent qu'ils sont conformes. Les certificats sont ensuite utilisés pour authentifier les clients NAP lorsqu'ils établissent des communications protégées par IPsec avec d'autres clients NAP sur un intranet.
  - La contrainte de mise en conformité IPsec restreint la communication sur un réseau aux nœuds considérés comme conformes
  - Vous pouvez définir des spécifications pour les communications sécurisées avec des clients conformes en fonction d'une adresse IP ou d'un numéro de port TCP/UDP

Contrainte de mise en conformité 802.1X

- Points clés de la contrainte de mise en conformité NAP pour les connexions 802.1X câblées ou sans fil :
  - L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité via une connexion réseau authentifiée par le protocole 802.1X
  - L'accès des ordinateurs non conformes est limité au moyen d'un profil d'accès restreint que le commutateur Ethernet ou le point d'accès sans fil place sur la connexion
  - Les profils d'accès restreint peuvent spécifier des filtres de paquets IP ou un identificateur de réseau local virtuel (VLAN) qui correspond au réseau restreint
  - La contrainte de mise en conformité 802.1X analyse activement l'état d'intégrité du client NAP connecté et applique le profil d'accès restreint à la connexion si le client devient non conforme

Contrainte de mise en conformité VPN

- Points clés de la contrainte de mise en conformité NAP VPN :
  - L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité via une connexion VPN d'accès à distance
  - Les ordinateurs non conformes ont un accès réseau limité au moyen d'un jeu de filtres de paquets IP que le serveur VPN applique à la connexion VPN
  - La contrainte de mise en conformité VPN analyse activement l'état d'intégrité du client NAP et applique les filtres de paquets IP du réseau restreint à la connexion VPN si le client devient non conforme

Contrainte de mise en conformité DHCP

- Points clés de la contrainte de mise en conformité NAP DHCP :
  - Les ordinateurs doivent être conformes pour pouvoir obtenir une configuration d'adresse IPv4 pour un accès illimité d'un serveur DHCP
  - Les ordinateurs non conformes ont une configuration d'adresse IPv4, ce qui autorise l'accès au réseau restreint uniquement
  - La contrainte de mise en conformité par DHCP analyse activement l'état d'intégrité du client NAP et renouvelle la configuration d'adresse IPv4 pour l'accès au réseau restreint uniquement, si le client devient non conforme

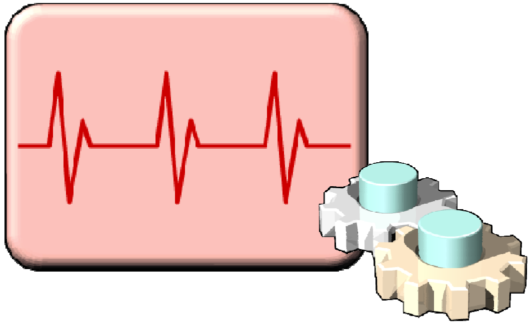
Leçon 3: Configuration de NAP

- Qu'est-ce que les programmes de validation d'intégrité système ?
- Qu'est-ce qu'une stratégie de contrôle d'intégrité ?
- Qu'est-ce que les groupes de serveurs de mise à jour ?
- Configuration du client NAP
- Démonstration : Configuration de NAP

Qu'est-ce que les programmes de validation d'intégrité système ?

Les programmes de validation d'intégrité système sont les équivalents côté serveur des agents d'intégrité système

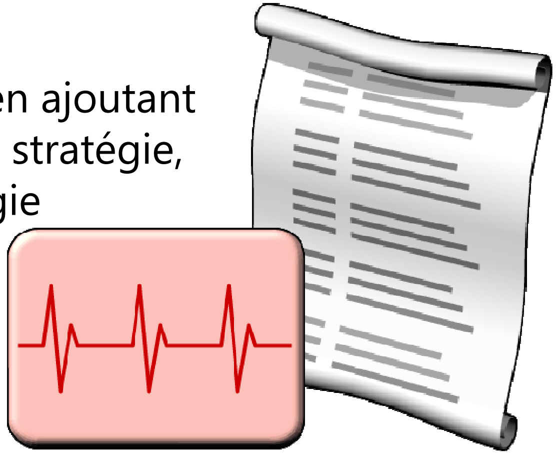
- Chaque agent d'intégrité système sur le client possède un programme de validation d'intégrité système correspondant dans le service NPS
- Les programmes de validation d'intégrité système permettent au service NPS de vérifier la déclaration d'intégrité produite par l'agent d'intégrité système correspondant sur le client
- Les programmes de validation d'intégrité système contiennent les paramètres de configuration requis sur les ordinateurs clients
- Le programme de validation d'intégrité système de la sécurité Windows correspond à l'agent d'intégrité système Microsoft sur les ordinateurs clients



Qu'est-ce qu'une stratégie de contrôle d'intégrité ?

Pour pouvoir exploiter le programme de validation d'intégrité de la sécurité Windows, vous devez configurer une stratégie de contrôle d'intégrité et lui affecter le programme de validation d'intégrité système

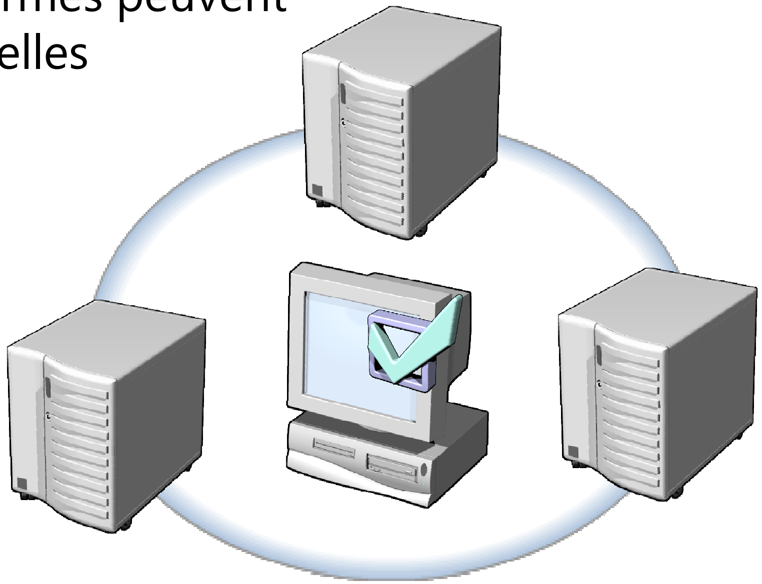
- Les stratégies de contrôle d'intégrité sont composées d'un ou de plusieurs programmes de validation d'intégrité système, ainsi que d'autres paramètres, qui vous permettent de définir les critères de configuration des ordinateurs compatibles avec la protection d'accès réseau qui tentent de se connecter à votre réseau
- Vous pouvez définir des stratégies de contrôle d'intégrité des clients dans le service NPS en ajoutant un ou plusieurs programmes de validation d'intégrité système à la stratégie de contrôle d'intégrité
- La contrainte de mise en conformité NAP est accomplie par le serveur NPS et les stratégies sont spécifiques à un réseau
- Une fois que vous avez créé une stratégie de contrôle d'intégrité en ajoutant un ou plusieurs programmes de validation d'intégrité système à la stratégie, vous pouvez ajouter la stratégie de contrôle d'intégrité à la stratégie réseau et activer la contrainte de mise en conformité NAP dans la stratégie



Qu'est-ce que les groupes de serveurs de mise à jour ?

Lorsque la contrainte de mise en conformité NAP est mise en œuvre, vous devez spécifier des groupes de serveurs de mise à jour afin que les clients aient accès aux ressources qui assurent la mise en conformité des clients non conformes compatibles avec la protection d'accès réseau

- Un serveur de mise à jour héberge les mises à jour que l'agent NAP peut utiliser pour que les ordinateurs clients non conformes deviennent conformes à la stratégie de contrôle d'intégrité définie par le serveur NPS
- Un groupe de serveurs de mise à jour est une liste de serveurs sur le réseau restreint auxquels les clients NAP non conformes peuvent accéder pour obtenir des mises à jour logicielles



Configuration du client NAP

- Certains déploiements NAP qui utilisent le programme de validation d'intégrité de la sécurité Windows requièrent l'activation du Centre de sécurité

- Le service de protection d'accès réseau est requis lorsque vous déployez la protection d'accès réseau sur des ordinateurs clients compatibles avec la protection d'accès réseau

- Vous devez également configurer les clients de contrainte de mise en conformité NAP sur les ordinateurs compatibles avec la protection d'accès réseau

- La plupart des paramètres clients NAP peuvent être configurés à l'aide des objets de stratégie de groupe

Démonstration : Configuration de NAP

Dans cette démonstration, vous allez apprendre à :

- Installer le rôle de serveur NPS
- Configurer le serveur NPS en tant que serveur de stratégie de contrôle d'intégrité NAP
- Configurer les stratégies de contrôle d'intégrité
- Configurer des stratégies réseau pour les ordinateurs conformes
- Configurer des stratégies réseau pour les ordinateurs non conformes
- Configurer le rôle de serveur DHCP pour la protection d'accès réseau
- Configurer les paramètres NAP du client
- Tester la protection d'accès réseau

Leçon 4: Analyse et résolution des problèmes du système NAP

- Qu'est-ce que le suivi NAP ?
- Démonstration : Configuration du suivi NAP
- Résolution des problèmes de la protection d'accès réseau
- Résolution des problèmes de la protection d'accès réseau avec les journaux d'événements

Qu'est-ce que le suivi NAP ?

- Le suivi de la protection d'accès réseau identifie des événements NAP et les enregistre dans un fichier journal en fonction de l'un des niveaux de suivi ci-après :
  - De base
  - Avancée
  - Débogage

- Vous pouvez utiliser les journaux de suivi pour :
  - Évaluer l'intégrité et la sécurité de votre réseau
  - Résoudre les problèmes et effectuer des opérations de maintenance

- Le suivi de la protection d'accès réseau est désactivé par défaut, ce qui signifie qu'aucun événement NAP n'est enregistré dans les journaux de suivi

Démonstration : Configuration du suivi NAP

Dans cette démonstration, vous allez apprendre à :

- Configurer le suivi à partir de l'interface utilisateur graphique
- Configurer le suivi à partir de la ligne de commande

Résolution des problèmes de la protection d'accès réseau

Vous pouvez utiliser la commande netsh NAP suivante pour vous aider à résoudre les problèmes liés à la protection d'accès réseau :

- netsh NAP client show state
- netsh NAP client show config
- netsh NAP client show group

Résolution des problèmes de la protection d'accès réseau avec les journaux d'événements

ID d'événement	Signification
6272	L'authentification a réussi
6273	L'authentification n'a pas réussi
6274	Un problème de configuration existe
6276	Le client NAP est mis en quarantaine
6277	Le client NAP est en période d'essai
6278	Le client NAP bénéficie d'un accès complet

Atelier pratique : Implémentation de la protection d'accès réseau

- Exercice 1 : Configuration des composants NAP
- Exercice 2 : Configuration de l'accès VPN
- Exercice 3 : Configuration des paramètres clients pour prendre en charge la protection d'accès réseau (NAP)

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 situés à Londres pour s’occuper du siège social et d’autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012

Pour améliorer la sécurité et les exigences de conformité, A. Datum doit étendre sa solution VPN pour inclure la protection d'accès réseau (NAP). Vous devez trouver une manière de le vérifier et, s'il y a lieu, mettre automatiquement les ordinateurs client en conformité chaque fois qu'ils se connectent à distance à l'aide de la connexion VPN. Vous allez réaliser cet objectif à l'aide de NPS pour créer des paramètres de validation d'intégrité système, des stratégies réseau et de contrôle d'intégrité et configurer la protection d'accès réseau (NAP) pour vérifier l'intégrité des clients et y remédier

Révision de l'atelier pratique

- La méthode de contrainte de mise en conformité NAP par DHCP est la méthode la plus faible dans Windows Server 2012. Pourquoi est-elle moins intéressante que les autres méthodes disponibles ?
- Est-ce que vous pourriez utiliser la solution NAP pour l'accès à distance avec la solution NAP pour IPsec ? Quel serait l'avantage de ce scénario ?
- Est-ce que vous auriez pu utiliser la contrainte de mise en conformité NAP par DHCP pour le client ? Expliquez pourquoi

Contrôle des acquis et éléments à retenir

- Questions de contrôle des acquis
- Outils