Sécurisation des serveurs à l'aide des GPO

Windows 2012 Server

1.La sécurité des systèmes d'exploitation Windows

- Windows Server 2012 comprend de nombreuses fonctionnalités qui fournissent différentes méthodes d'implémentation de la sécurité.
- *La défense en profondeur* utilise une approche en couches de la sécurité:

- Réduit les chances de succès d'un intrus
- Augmente les chances de détecter un intrus

1.La sécurité des systèmes d'exploitation Windows

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

1.La sécurité des systèmes d'exploitation Windows

Meilleures pratiques pour accroître la sécurité

Appliquer rapidement toutes les mises à jour de sécurité disponibles: Microsoft diffuse publiquement les détails de toutes les vulnérabilités connues après la publication d'une mise à jour.

Appliquer 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.

Restreindre la connexion de console: Cela est dû au fait que certains programmes malveillants peuvent infecter un ordinateur uniquement en utilisant une session utilisateur sur cet ordinateur.

Limiter l'accès physique

2.Configuration des paramètres de sécurité

- Configuration de modèles de sécurité
- Configuration des droits des utilisateurs
- Configuration des options de sécurité
- Configuration du contrôle de compte d'utilisateur
- Configuration de l'audit de sécurité
- Configuration des groupes restreints
- Configuration des paramètres de stratégie de compte

2.Configuration des paramètres de sécurité

Les 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.
- les modèles de sécurité sont divisés en sections logiques:
- *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*
- *Groupes restreints*. Appartenance à des groupes dotés de droits et autorisations spéciaux.
- *Services système*. Démarrage et autorisations pour les services système
- *Registre*.
- *Système de fichiers*. Autorisations pour les dossiers et les fichiers.

2.Configuration des paramètres de sécurité

Les modèles de sécurité

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.

2.Configuration des paramètres de sécurité

Les droits des utilisateurs

- *L'attribution des droits utilisateur* se rapporte à la capacité d'exécuter des actions sur le système d'exploitation. La plupart des droits sont accordés au système local ou à l'administrateur.
- Types de droits des utilisateurs:
- Les *privilèges* définissent l'accès aux ressources de l'ordinateur et du domaine, Comme Les droits de sauvegarder des fichiers et des répertoires.
- Les *droits de connexion* définissent les personnes autorisées à se connecter à un ordinateur et la manière dont elles peuvent se connecter.
- Vous pouvez configurer des droits via une stratégie de groupe à Configuration de l'ordinateur\Stratégies\Paramètres windows\Paramètres de sécurité\Stratégies locales\Attribution des droits utilisateurs dans **GPMC**.

2.Configuration des paramètres de sécurité

Les droits des utilisateurs

Exemples

- Ajouter des stations de travail à un domaine
- Permettre l'ouverture d'une session locale
- Sauvegarder les fichiers et les répertoires
- Modifier l'heure système
- Forcer l'arrêt à partir d'un ordinateur distant
- Arrêter le système

2.Configuration des paramètres de sécurité

Les options de sécurité

- 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

2.Configuration des paramètres de sécurité

Les options de sécurité

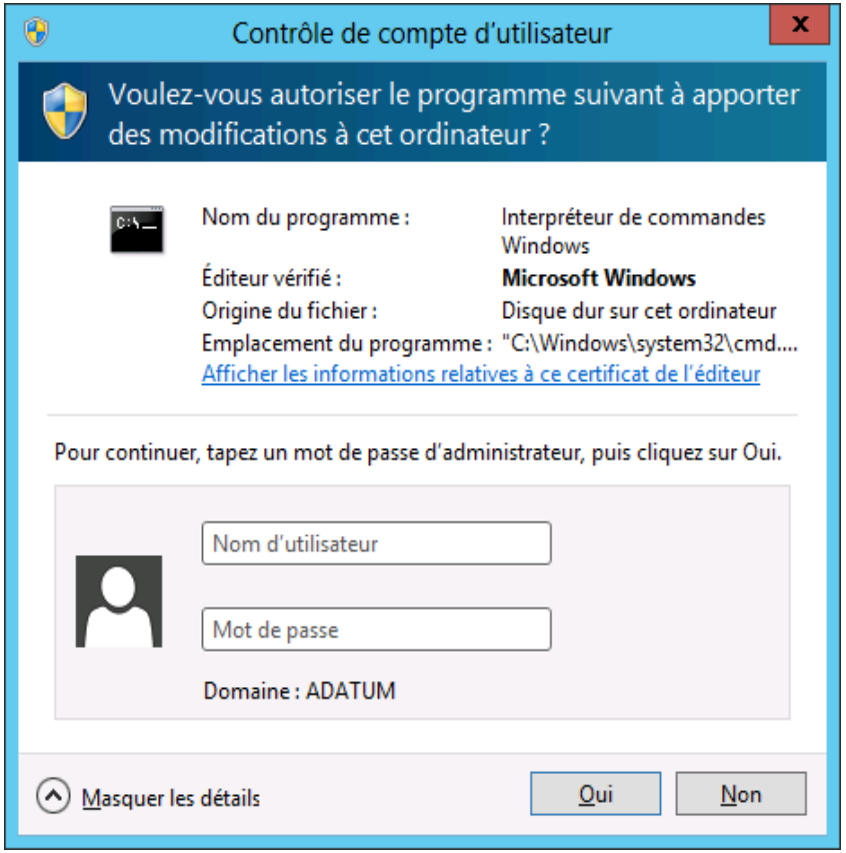
Exemples

- Prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire
- Ne pas afficher le dernier nom d'utilisateur
- Renommer le compte administrateur
- Autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session localement

2.Configuration des paramètres de sécurité

Contrôle de compte utilisateur

- Le Contrôle de compte d'utilisateur (UAC) est une fonctionnalité de sécurité qui invite l'utilisateur à fournir les informations d'identification d'un administrateur si la tâche requiert des autorisations d'administration.
- Le Contrôle de compte permet aux utilisateurs d'effectuer des tâches quotidiennes courantes en tant que non-administrateurs.



2.Configuration des paramètres de sécurité

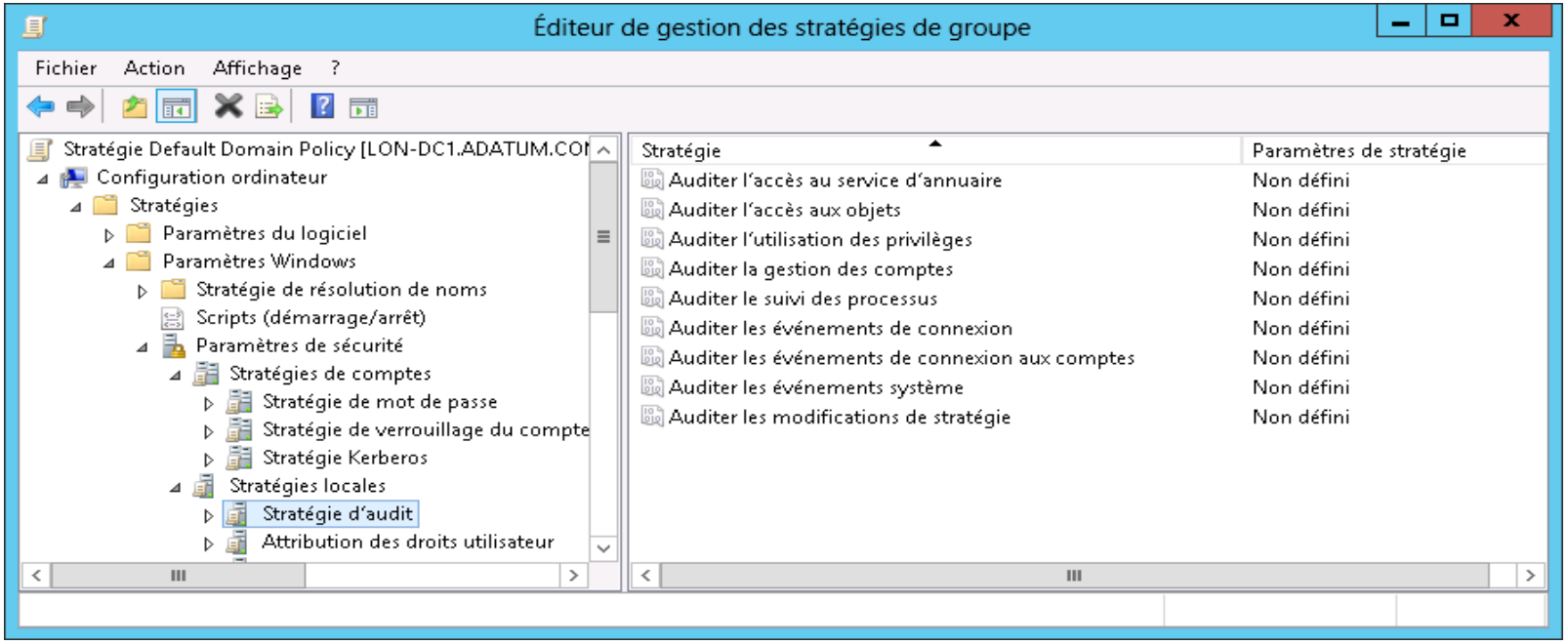
Contrôle de compte utilisateur

- 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.*
- 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. Une fois la tâche terminée, les autorisations redeviennent celles d'un utilisateur standard.

2.Configuration des paramètres de sécurité

Audit de sécurité

- L'audit de sécurité génère des journaux d'événements de sécurité que les administrateurs peuvent consulter dans l'observateur d'événements, dans le journal des événements de sécurité.



2.Configuration des paramètres de sécurité

Groupes restreints

- Vous pouvez utiliser la stratégie Groupes restreints pour contrôler l'appartenance aux groupes en spécifiant les membres qui sont placés dans un groupe.
- La stratégie de groupe peut contrôler l'appartenance aux groupes:
  - Pour tout groupe sur un ordinateur local, en appliquant un objet Stratégie de groupe à l'Unité d'organisation contenant le compte d'ordinateur
  - Pour tout groupe des services de domaine Active Directory, en appliquant un objet Stratégie de groupe à l'unité d'organisation du contrôleur de domaine

2.Configuration des paramètres de sécurité

Paramètres de stratégie de compte

Les stratégies de compte atténuent la menace des attaques en force brute 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

3.Restriction de l’accès aux logiciels

- Que sont les stratégies de restriction logicielle ?
- Qu'est-ce qu'AppLocker ?
- Règles AppLocker

3.Restriction de l'accès aux logiciels

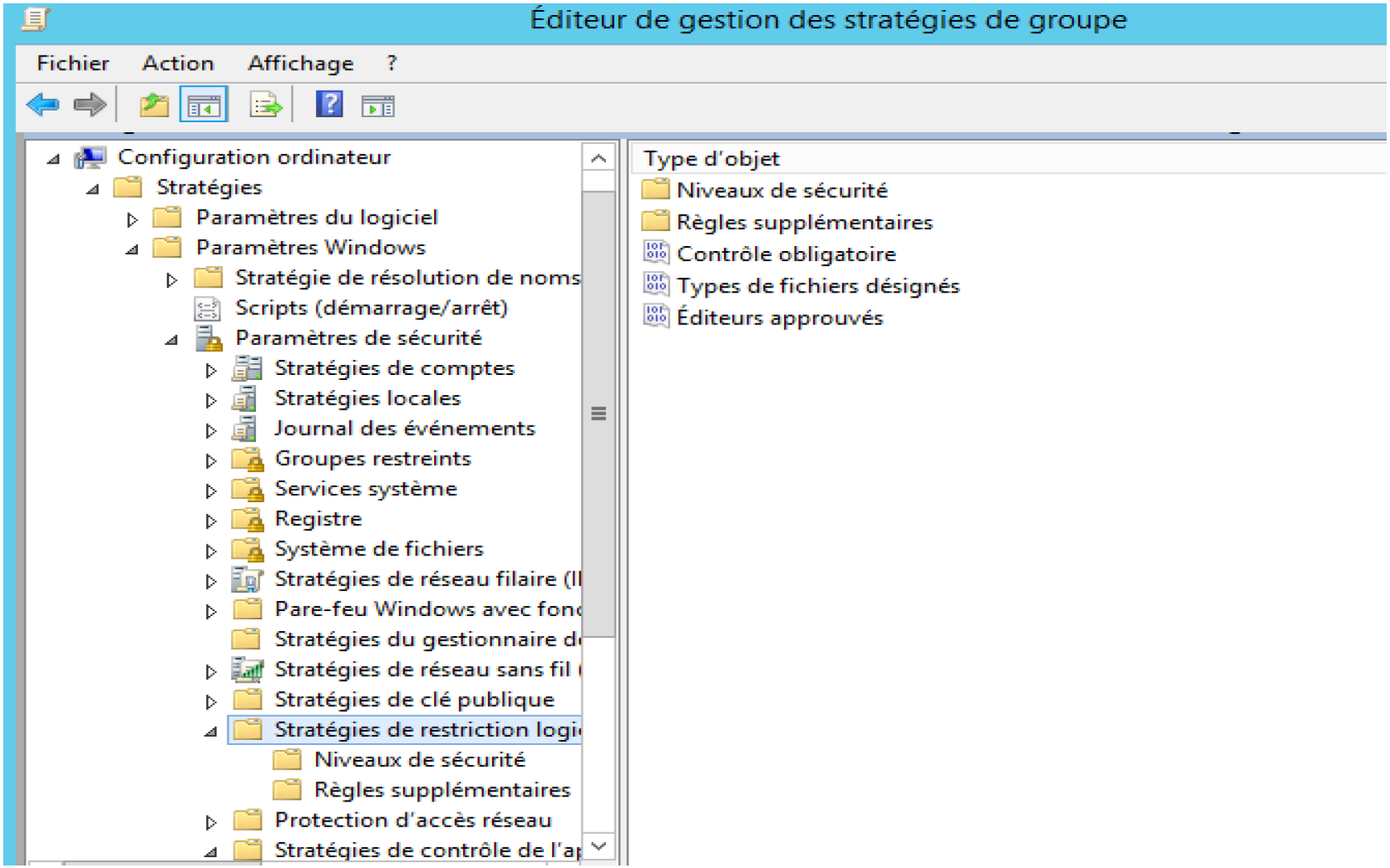
- Les stratégies de restriction logicielle permettent aux administrateurs d'identifier les applications qui sont autorisées à s'exécuter sur les ordinateurs client.
- Vous configurez et déployez les paramètres de stratégie de restriction logicielle sur les clients à l'aide des stratégies de groupe.
- Une stratégie de restriction logicielle définie se compose de règles et de niveaux de sécurité.
- 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
  - Zone: zone internet

3.Restriction de l'accès aux logiciels

- 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 :

- **Non autorisé.** 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 selon les droits d'accès de l'utilisateur. C'est le niveau par défaut.

3.Restriction de l’accès aux logiciels



3.Restriction de l'accès aux logiciels

- Applocker est une fonctionnalité liée aux paramètres de sécurité, qui contrôle quelles applications les utilisateurs sont autorisés à exécuter.
- AppLocker comporte des fonctions et des extensions qui:

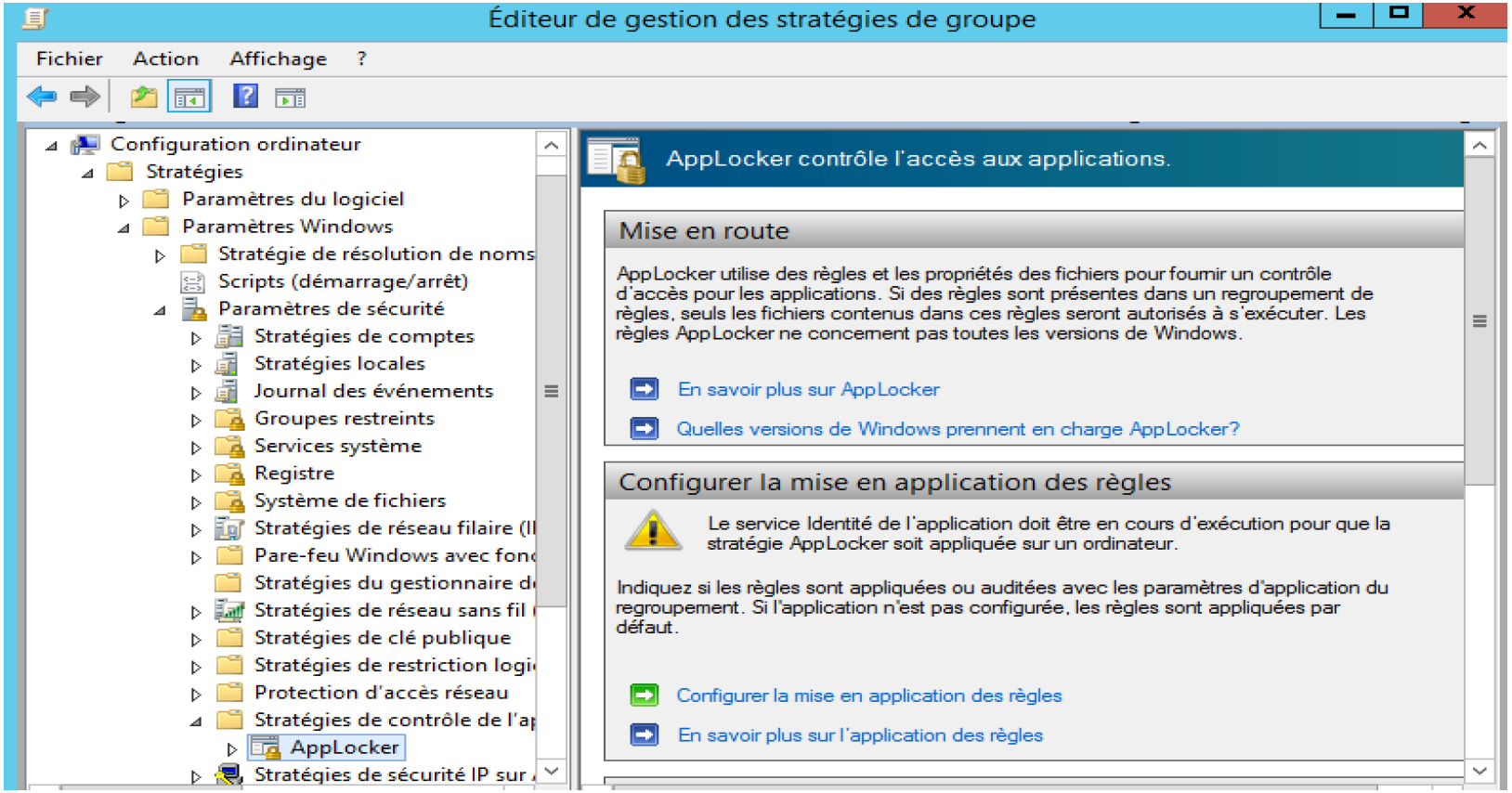
- Réduisent la charge d'administration
- Permettent aux administrateurs de contrôler le mode d'accès et d'utilisation des fichiers suivants par les utilisateurs:
  - fichiers .exe
  - scripts
  - Fichiers du programme d'installation de Windows (fichiers .msi et .msp)
  - DLL

- Avantages d'AppLocker:

- Contrôle la façon dont les utilisateurs peuvent accéder à tous les types d'applications et les exécuter
- Permet la définition de règles basées sur une grande variété de variables
- Permet d'importer et d'exporter l'intégralité de stratégies AppLocker

3.Restriction de l'accès aux logiciels

- 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.



3.Restriction de l’accès aux logiciels

- AppLocker définit des règles basées sur des attributs de fichier tels que:
  - Nom de l'éditeur
  - Nom du produit
  - Nom de fichier
  - Version de fichier

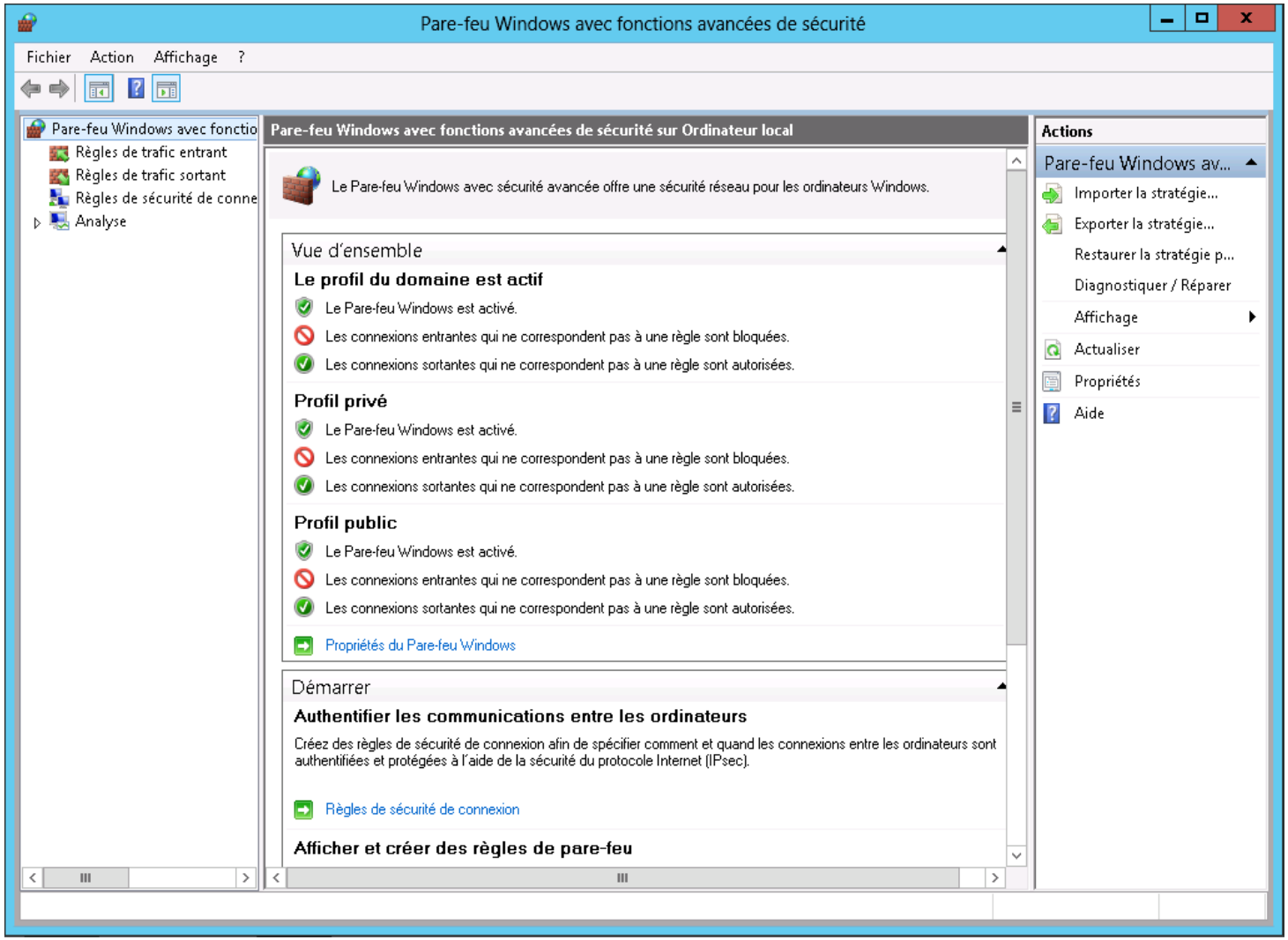
- Actions de règle:
  - Conditions Autoriser ou Refuser
  - Stratégies Appliquer ou Auditer uniquement

4.Configuration du pare-feu Windows

- Qu'est-ce que le Pare-feu Windows avec fonctions avancées de sécurité ?
- Profils de pare-feu
- Règles de sécurité de connexion
- Déploiement des règles de pare-feu

4.Configuration du pare-feu Windows

Le Pare-feu Windows est un pare-feu hôte avec état qui autorise ou bloque le trafic réseau selon la configuration.



4.Configuration du pare-feu Windows

- 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.
- 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.

4.Configuration du pare-feu Windows

- Les profils de pare-feu sont un ensemble de paramètres de configuration qui s'appliquent à un type particulier de réseau.
- Ces profils sont les suivants:
  - Domaine: À utiliser quand votre ordinateur fait partie d'un domaine de système d'exploitation Windows.
  - Public: À utiliser quand vous êtes connecté à un réseau public non approuvé.
  - Privé: À utiliser quand vous êtes connecté derrière un pare-feu.
- Dans Windows Server 2012, il est possible d'avoir plusieurs profils actifs de pare-feu simultanément.

4.Configuration du pare-feu Windows

- 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.
- Lien entre les règles de pare-feu et les règles de connexion:

- Les règles de Pare-feu autorisent le trafic à passer, mais ne sécurisent pas ce trafic.
- Les règles de sécurité de connexion peuvent sécuriser le trafic, mais seulement si une règle de pare-feu a été préalablement configurée.

4.Configuration du pare-feu Windows

Vous pouvez déployer des règles de Pare-feu Windows:

- À l'aide du Pare-feu Windows avec fonctions avancées de sécurité
- À l'aide d'une stratégie de groupe
- En exportant et en important des règles de pare-feu