Travaux pratiques - Configuration de la stratégie de sécurité locale de Windows

Introduction

Au cours de ces travaux pratiques, vous configurerez la stratégie de sécurité locale de Windows. La stratégie de sécurité locale de Windows permet de configurer de nombreux éléments de sécurité pour les ordinateurs autonomes qui ne font pas partie d'un domaine Active Directory. Vous modifierez les exigences relatives aux mots de passe, activerez l'audit, configurerez des droits d'utilisateur et définirez certaines options de sécurité. Vous utiliserez ensuite le Gestionnaire d'événements pour voir les informations enregistrées.

Matériel conseillé

- Un ordinateur avec Windows installé

Remarque : l'accès à l'outil de stratégie de sécurité locale peut être légèrement différent en fonction des versions de Windows. Mais au sein de l'outil, les procédures de configuration sont les mêmes pour les étapes présentées dans ces travaux pratiques.

Instructions

Étape 1 : Examinez les exigences en matière de sécurité.

Un client a besoin de six ordinateurs Windows autonomes dans une de ses filiales. Ils doivent être configurés conformément à la stratégie de sécurité de l'entreprise. Ces ordinateurs ne font pas partie d'un domaine Active Directory. Les stratégies doivent être configurées manuellement sur chaque ordinateur.

La stratégie de sécurité est la suivante :

- Les mots de passe doivent contenir au moins 8 caractères.
- Les mots de passe doivent être changés tous les 90 jours.
- Les utilisateurs peuvent changer de mot de passe une fois par jour.
- Les utilisateurs peuvent réutiliser un mot de passe unique après l'utilisation de 8 autres.
- Les mots de passe doivent comprendre trois des quatre éléments suivants :
  - Au moins un caractère alphanumérique en minuscules.
  - Au moins un caractère alphanumérique en majuscules.
  - Au moins un caractère numérique.
  - Au moins un symbole.
- Les utilisateurs ne peuvent plus accéder à leur ordinateur après 5 tentatives erronées de saisie du mot de passe. Les utilisateurs doivent patienter 5 minutes avant que le compteur se réinitialise et permette à nouveau de saisir un mot de passe.
- Chaque paramètre de sécurité de la stratégie d'audit doit être activé.
- Après 30 minutes d'inactivité, l'utilisateur est automatiquement déconnecté. (Systèmes d'exploitation Windows 8.1 et 8.0 uniquement)
- Les utilisateurs doivent se connecter avant de retirer l'ordinateur portable d'une station d'accueil.
- Lors de la connexion, le titre et le texte suivants doivent s'afficher :

- Titre : **Attention :**
- Texte : **Votre activité est surveillée. Cet ordinateur est conçu pour une utilisation professionnelle uniquement.**

- Les utilisateurs reçoivent un rappel les avertissant qu'ils doivent changer de mot de passe 7 jours avant son expiration.

L'outil Stratégie de sécurité locale de Windows offre beaucoup plus de paramètres, qui vont au-delà du cadre de ce cours.

Étape 2 : Ouvrez l'outil Stratégie de sécurité locale de Windows.

a. Pour accéder à la Stratégie de sécurité locale dans Windows 10, vous pouvez utiliser les deux chemins d'accès suivants :

Outils d'administration > Stratégie de sécurité locale

Ou **Rechercher > secpol.msc**, puis cliquer sur **secpol**.

b. La fenêtre **Stratégie de sécurité locale** s'ouvre. Ces travaux pratiques mettent l'accent sur les **Stratégies de compte** et les **Stratégies locales** surlignées dans l'illustration ci-dessous. Les autres **Paramètres** de sécurité sortent du cadre de ce cours.

Étape 3 : Configurez les paramètres de sécurité Stratégie de mot de passe.

Les six premières exigences de la stratégie de sécurité de l'entreprise sont configurées dans la section **Stratégies de compte** de l'outil **Stratégie de sécurité locale**.

a. Cliquez sur la flèche en regard de **Stratégies de compte** pour développer cette section, puis cliquez sur **Stratégie de mot de passe**. Six stratégies sont affichées dans le panneau de droite avec les paramètres de sécurité associés par défaut.

b. La première stratégie, **Appliquer l'historique des mots de passe**, est utilisée pour définir le nombre de mots de passe uniques que vous devez créer avant d'être autorisé à réutiliser un mot de passe. Selon la stratégie de sécurité de l'entreprise définie à l'étape 1, le paramètre de sécurité de cette stratégie doit être **8**. Double-cliquez sur **Appliquer l'historique des mots de passe** pour ouvrir la fenêtre des **propriétés** correspondante. Définissez la valeur sur **8**.

c. En vous basant sur les exigences de la stratégie de sécurité de l'étape 1, entrez les valeurs que vous devez définir dans **Stratégie de sécurité locale** pour les paramètres de sécurité restants de **Stratégie de mot de passe**.

Politique	Paramètre de sécurité
Appliquer l'historique des mots de passe	8
Durée de vie maximale du mot de passe	
Durée de vie minimale du mot de passe	
Longueur minimale du mot de passe	
Le mot de passe doit respecter des exigences de complexité	
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé

Remarque : le paramètre de sécurité **Enregistrer les mots de passe en utilisant un chiffrement réversible** doit toujours être désactivé. Le fait d'enregistrer les mots de passe en utilisant un chiffrement réversible est pratiquement identique à l'enregistrement des mots de passe en clair. Pour cette raison, cette stratégie ne doit jamais être activée à moins que les besoins des applications soient plus importants que la nécessité de protéger les informations.

d. Double-cliquez sur chacune des stratégies et définissez les valeurs en fonction des entrées du tableau ci-dessus.

Étape 4 : Configurez les paramètres de sécurité Stratégie de verrouillage du compte.

a. Selon la stratégie de sécurité définie à l'étape 1, combien de fois l'utilisateur est-il autorisé à tenter d'ouvrir une session avant le verrouillage du compte ?

Saisissez vos réponses ici

b. Combien de temps l'utilisateur doit-il attendre avant d'essayer de se reconnecter ?

Saisissez vos réponses ici

c. Utilisez les paramètres de sécurité **Stratégie de verrouillage du compte** dans **Stratégie de sécurité locale** pour configurer les exigences de la stratégie.

Conseil : vous devez d'abord configurer le **Seuil de verrouillage de compte**.

Étape 5 : Configurez les paramètres de sécurité de la stratégie d'audit.

a. Dans la Stratégie de sécurité locale, développez le menu Stratégies locales, puis cliquez sur Stratégie d'audit.

b. Double-cliquez sur **Auditer les événements de connexion aux comptes** pour ouvrir la fenêtre **Propriétés**. Cliquez sur l'onglet **Expliquer** pour en savoir plus sur ce paramètre de sécurité.

c. Cliquez sur l'onglet **Paramètre local de sécurité**, puis activez les options **Réussite** et **Échec**. Cliquez sur **OK** pour fermer la fenêtre **Propriétés** et appliquer les paramètres de sécurité.

d. Continuez à modifier les autres paramètres de sécurité de **Stratégie d'audit**. Cliquez sur l'onglet **Expliquer** de chacun des paramètres et lisez ce qu'ils font. Cliquez sur les cases à cocher **Réussite** et **Échec** dans chaque fenêtre **Propriétés**.

Étape 6 : Configurez les paramètres de sécurité Stratégies locales.

a. Dans Stratégie de sécurité locale, cliquez sur Attribution des droits utilisateur dans Stratégies locales pour afficher les paramètres de sécurité.

b. Bien qu'aucun des paramètres de sécurité ne doive être modifié pour répondre aux exigences en matière de sécurité, passez un peu de temps à étudier les paramètres par défaut.

Question :

Selon vous, certains de ces paramètres doivent-ils être modifiés ? Pourquoi ?

Saisissez vos réponses ici

c. Dans Stratégie de sécurité locale, cliquez sur Options de sécurité dans Stratégies locales pour afficher les paramètres de sécurité.

d. Pour les exigences de stratégie de sécurité restantes de l'étape 1, dressez dans le tableau ci-dessous la liste des stratégies et des paramètres de sécurité que vous devez modifier dans **Options de sécurité**. La première stratégie est déjà indiquée pour vous.

Politique	Paramètre de sécurité
Ouverture de session interactive : Limite d'inactivité de la machine	1800 secondes

Étape 7 : Testez les paramètres de sécurité Stratégie de mot de passe.

Testez vos paramètres de sécurité Stratégie de mot de passe en essayant de changer de mot de passe. Essayez un nouveau mot de passe qui ne répond pas aux exigences de longueur ou de complexité.

Panneau de configuration > Comptes d'utilisateurs > Apporter des modifications à mon compte dans les paramètres de l'ordinateur > Options de connexion, puis cliquez sur **Modifier** sous **Mot de passe**.

Vous devriez voir un message indiquant que le nouveau mot de passe ne répond pas aux exigences de la stratégie de mot de passe.

Étape 8 : Exportez et importez les paramètres de la stratégie de sécurité.

Le client dispose encore de 5 autres ordinateurs autonomes qui doivent répondre aux mêmes exigences en matière de sécurité. Plutôt que de configurer manuellement les paramètres de chaque ordinateur, exportez les paramètres de cet ordinateur.

a. Dans la barre de menus de Stratégie de sécurité locale, cliquez sur Action > Exporter la stratégie.

b. Donnez un nom au fichier **.inf** et enregistrez-le dans l'emplacement de votre choix.

c. Copiez le fichier de stratégie de sécurité **.inf** sur un lecteur Flash. Branchez celui-ci sur un autre ordinateur. Ouvrez **Stratégie de sécurité locale**, puis cliquez sur **Action > Importer la stratégie.** Recherchez le fichier **.inf** sur le lecteur Flash et ouvrez-le pour appliquer la stratégie de sécurité au nouvel ordinateur.