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.

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 :
 - o 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 ouvrir une session avant de retirer l'ordinateur portable de la 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 7 et Windows Vista, suivez le chemin suivant :

Démarrer > Outils d'administration > Stratégie de sécurité locale

b. Pour accéder à la Stratégie de sécurité locale dans Windows 8 et 8.1, sélectionnez :

Rechercher > secpol.msc, puis cliquez sur secpol.

c. 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.

Remarque : les captures d'écran de Windows 8.1 sont utilisées tout au long des présents travaux pratiques.



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**.

 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 Appliquer l'historique des mots de passe. Définissez la valeur sur 8.

Stratégie de sécurité locale – 🗆 🗙				
Fichier Action Affichage ? Fichier Action Affichage ? Image: Stratégies Image: Stratégies Image: Stratégies Image: Stratégies Image: Stratégies Image: Stratégies Image: Stratégies Image: Stratégies	Stratégie Stratégie Conserver l'hist Durée de vie ma Enregistrer les n Le mot de passe Longueur minir	e de sécurité locale – × Propriétés de : Conserver l'historique des mots de ? × Paramètre de sécurité locale Expliquer Conserver l'historique des mots de passe Conserver l'historique du mot de passe pendant : 8		
		OK Annuler Appliquer		
	L	143		

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
Antériorité maximale du mot de passe	
Antériorité 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 cidessus. Lorsque vous avez terminé, la configuration doit être similaire à celle-ci :

🚡 Stratégie de sécurité locale – 🗖 🗙			
Fichier Action Affichage ?			
🗢 🔿 🙍 📰 🗟 🖬			
 Paramètres de sécurité Stratégies de comptes Stratégie de verrouillage du comp Stratégies locales Pare-feu Windows avec fonctions ava Stratégies de cép ublique Stratégies de cép ublique Stratégies de contrôle de l'application Stratégies de sécurité IP sur Ordinateu Configuration avancée de la stratégie 	Stratégie	Paramètre de sécurité 8 mots de passe mémori 90 jours 1 jours Désactivé Activé 8 caractère(s)	

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

c. Utilisez les paramètres de sécurité Stratégie de verrouillage du compte dans Stratégie de sécurité locale pour configurer les exigences de la stratégie. Lorsque vous avez terminé, la configuration doit être similaire à celle-ci.

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

Fichier Action Affichage ? Image: Stratégies de comptes Image: Stratégies de comtoins ava Image: Stratégies de comtoine de lists de lost de lost de lost de lost de lastratégie Image: Stratégies de contrôle de l'application Image: Stratégies de sécurité IP sur Ordinateu Image: Stratégies de sécurité IP sur Ordinateu Image: Stratégies de lastratégie Image: Stratégies de lastratégie Image: Stratégies de lastratégie Image: Stratégies de contrôle de lastratégie	🚡 Stratégie de sécurité locale – 🗖 🗙				
Image: Stratégies de comptes Stratégies de comptes Stratégies de comptes Stratégies de verrouillage du compte Stratégies de verrouillage du compte Stratégies de verrouillage du compte Image: Stratégies du gestionnaire de listes de la Stratégies de contrôle de l'application Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Image: Stratégies de sécurité de la stratégie Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Image: Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Image: Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Image: Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Image: Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate. Stratégies de sécurité l'P sur Ordinate.	Fichier Action Affichage ?				
Paramètres de sécurité Stratégies de comptes Stratégie de mot de passe Stratégie de verrouillage du compte Stratégies locales Stratégies de clé publique Stratégies de clé publique Stratégies de clé publique Stratégies de clé publique Stratégies de sécurité IP sur Ordinateu Stratégies de sécurité IP sur Ordinateu Configuration avancée de la stratégie Stratégies Stratégies Stratégies	🗢 🔿 🙍 📰 🗟 👔				
	Paramètres de sécurité Stratégies de comptes Stratégie de mot de passe Stratégies locales Pare-feu Windows avec fonctions ava Stratégies de certroillage du comp Stratégies de gestionnaire de listes de Stratégies de clé publique Stratégies de clé publique Stratégies de contrôle de l'application Stratégies de sécurité IP sur Ordinated Configuration avancée de la stratégies	Stratégie Durée de verrouillage des comptes Réinitialiser le compteur de verrouillages du compte après Seuil de verrouillage du compte	Paramètre de sécurité 5 minutes 5 minutes 5 tentatives d'ouvertures		

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 de sécurité**, puis activez les cases à cocher **Réussite** et **Échec**. Cliquez sur **OK** pour fermer la fenêtre **Propriétés** et appliquer les paramètres de sécurité.

	Stratégi	e de sécurité locale – 🗖 🗡
Image: Stratégies de comptes Image: Stratégies de verrouillage du comp Image: Stratégies de vertrition logicielle Image: Stratégies de vertrition logicielle Image: Stratégies de sécurité IP sur Ordinatei Image: Stratégies de sécurité IP sur Ordinatei	Stratégie Stratégie Auditer l'accès : Auditer l'accès : Auditer l'accès : Auditer la gestic Auditer le sévér Auditer les évér Auditer les évér Auditer les moc	e de sécurité locale – Propriétés de : Auditer l'accès au service d'annuaire ? Paramètre de sécurité locale Expliquer Auditer les consulter l'accès au service d'annuaire Auditer les tentatives des types suivants : Auditer les tentatives des types suivants : Réussite Échec Munice stratégie est configurée pour avoir la priorité sur la stratégie d'audit au niveau de la catégorie. Pour obtenir davantage d'informations, consultez <u>Auditer l'accès au</u> service d'annuaire. (Q921468)
۲		OK Annuler Appliquer

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. Lorsque vous avez terminé, la configuration Stratégie d'audit doit être similaire à celle-ci :



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.

3	Stratégie de sécurité locale	_ 🗆	×
Fichier Action Affichage ?			
🗢 🤿 🖄 📰 🗙 🗟 🛛 🖬			
Paramètres de sécurité Stratégies de comptes	Stratégie	Paramètre de sécurité	1
 Garages de comptes Garages locales Garages d'audit Attribution des droits utilisateur 	 Accéder à cet ordinateur à partir du réseau Accéder au gestionnaire d'informations d'identification en t Agir en tant que partie du système d'exploitation Ajouter des stations de travail au domaine 	Tout le monde,Administ	
Legitions de securite Legitions de securite Legitions de securite Legitions de securite Legitions de legitions ava Legitions de legitier de legitions de legitions de legitier de legi	Ajuster les quotas de mémoire pour un processus Arrêter le système Murgementer la griocité de planification	SERVICE LOCAL, SERVICE Administrateurs, Utilisate	
 Stratégies de clé publique Stratégies de restriction logicielle Stratégies de contrôle de l'application 	Augmenter la profite de planification Augmenter une plage de travail de processus Autoriser l'ouverture de session par les services Bureau à dist	Utilisateurs, Window Ma Administrateurs, Utilisate	
 Stratégies de sécurité IP sur Ordinateu Configuration avancée de la stratégie 	Changer le fuseau horaire Charger et décharger les pilotes de périphériques Contourner la vérification de parcours	SERVICE LOCAL,Admini Administrateurs Tout le monde,SERVICE	1
	Créer des liens symboliques Créer des objets globaux	Administrateurs SERVICE LOCAL,SERVICE	
	Créer un fichier d'échange	Administrateurs	
	Déboguer les programmes Effectuer les tâches de maintenance de volume Effectuer l'identifé d'un client ance l'authentification	Administrateurs Administrateurs	
	Forcer l'arrêt à partir d'un système distant Générer des audits de sécurité	Administrateurs SERVICE LOCAL, SERVICE	
< >>	B Gérer le journal d'audit et de sécurité	∆dministrateurs	1

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. Selon vous, certains de ces paramètres doivent-ils être modifiés ? Pourquoi ? c. Dans **Stratégie de sécurité locale**, cliquez sur **Options de sécurité** dans **Stratégies locales** pour afficher les paramètres de sécurité.

🚡 Stratégie de sécurité locale – 🗖 🗡			
Fichier Action Affichage ?			
🗧 🔿 📶 🗙 🗟 🛛 🖬			
 Paramètres de sécurité Stratégies de comptes Stratégies locales Stratégie d'audit Attribution des droits utilisateur Options de sécurité Pare-feu Vindows avec fonctions ava Stratégies du estionnaire de listes de Stratégies de clé publique Stratégies de contrôle de l'application Stratégies de sécurité IP sur Ordinate. Configuration avancée de la stratégie 	Stratégie Stratégie Accès réseau : chemins et sous-chemins de Registre accessi Accès réseau : les autorisations spécifiques des utilisateurs a Accès réseau : les canaux nommés qui sont accessibles de Accès réseau : les chemins de Registre accessibles de manière a Accès réseau : les partages qui sont accessibles de manière a Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser l'énumération anonyme des Accès réseau : ne pas autoriser le stockage de mots de passe Accès réseau : ne pas autoriser le stockage de mots de passe Accès réseau : ne pas autoriser le stockage de mots de passe Audit : germet au système d'être arrêté sans avoir à se conne Audit : auditer l'accès des objets système globaux Audit : auditer l'utilisation des privilèges de sauvegarde et d Audit : force les paramètres de sous-catégorie de stratégie d Client réseau Microsoft : communications signées numériq Client réseau Microsoft : communications signées numériq	Paramètre de sécurité System\CurrentControlS Désactivé System\CurrentControlS Non défini Classique - les utilisateu Désactivé Activé Désactivé Désactivé Désactivé Désactivé Désactivé Désactivé Non défini Désactivé Non défini Désactivé Désactivé Désactivé	
< >	Comptes : renommer le compte administrateur Compter : renommer le compte la vité	Administrateur	

 À l'aide des 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 (Windows 8.1 et 8.0 uniquement)	1800 secondes

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

a. 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.

Sous Windows 7 et Windows Vista, sélectionnez :

Panneau de configuration > Comptes utilisateur > Modifier votre mot de passe

Sous Windows 8,1, procédez comme suit :

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

Sous Windows 8,0, procédez comme suit :

Panneau de configuration > Comptes utilisateur > Apporter des modifications à mon compte dans les paramètres de l'ordinateur, puis cliquez sur Modifier votre mot de passe.

b. Vous devriez voir un message indiquant que le nouveau mot de passe ne répond pas aux exigences de la stratégie de mot de passe, par exemple, dans Windows 8.1 :



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.

1	🕹 Stratégie de sécurité locale – 🗖 🗙			
Fichier Action Affich	hage ?			
Fichier Action Affich Importer Ouvrir Parar Importer Importer Exporter Importer <td>hage ? une stratégie ne stratégie a liste a liste a liste ionnaire de listes de ublique iction logicielle rôle de l'application rité IP sur Ordinateu ncée de la stratégie</td> <td>m Stratégies de comptes Stratégies locales Pare-feu Windows avec fonctions avancé Stratégies du gestionnaire de listes de rés Stratégies de clé publique Stratégies de cestriction logicielle Stratégies de contrôle de l'application Stratégies de sécurité IP sur Ordinateur Io Configuration avancée de la stratégie d'a</td> <td>Description Stratégies de mot de passe et de verrouillage d Stratégies des options d'audit, de droits d'utilis Stratégies de soptions d'audit, de droits d'utilis Stratégies de groupes relatives au nom, à l'icôn Stratégies de contrôle de l'application Administration de la sécurité du protocole Inter Configuration avancée de la stratégie d'audit</td>	hage ? une stratégie ne stratégie a liste a liste a liste ionnaire de listes de ublique iction logicielle rôle de l'application rité IP sur Ordinateu ncée de la stratégie	m Stratégies de comptes Stratégies locales Pare-feu Windows avec fonctions avancé Stratégies du gestionnaire de listes de rés Stratégies de clé publique Stratégies de cestriction logicielle Stratégies de contrôle de l'application Stratégies de sécurité IP sur Ordinateur Io Configuration avancée de la stratégie d'a	Description Stratégies de mot de passe et de verrouillage d Stratégies des options d'audit, de droits d'utilis Stratégies de soptions d'audit, de droits d'utilis Stratégies de groupes relatives au nom, à l'icôn Stratégies de contrôle de l'application Administration de la sécurité du protocole Inter Configuration avancée de la stratégie d'audit	
< Exporte le modèle à partir d	> de cet objet Stratégie vei	rs un fichier.		

- 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.