WINDOWS SERVER AUDITS AD

Windows Server

Margaux TANET CPI

2024-2025

Introduction : Dans ce document, nous allons mettre en place un audit via une GPO pour la gestion de comptes d'AD. Des tests seront réalisés via le journal d'évènement.

I- Création d'une GPO pour activer l'audit

Se rendre dans Gestion de stratégie de groupe > créer une GPO sur le contrôleur de domaine > clic droit Modifier :

 Fichier Action Affichage Fenetre ? Fichier Action Af	Gestion de stratégie de groupe					
 Image: Section de stratégie de groupe Gestion de stratégie de groupe Comaines Default Domain Policy Default Domain Policy Default Domain Controllers Domain Controllers Domain Controllers Doles GPO Starter Sites Modélisation de stratégie de groupe Résultats de stratégie de groupe Résultats de stratégie de groupe Apoleu Dotes GPO Starter Sites Modélisation de stratégie de groupe Miliadeurs authentifiés Divertifiés 	📓 Fichier Action Affichage Fenétre ?					- 8
Gestion de stratégie de groupe ✓ Bronti: Learn.local ✓ Default Domain Policy ✓ Default Domain Policy ✓ Partage2 ✓ Default Domain Controllers ✓ Objets de stratégie de groupe > ④ Objets GPO Starter > ⑤ Objets GPO Starter > ⑤ Sites Ø Modélisation de stratégie de groupe ④ Resultats de stratégie de groupe ④ Modélisation de stratégie de groupe ④ Objets GPO Starter > ⑥ Objets GPO Starter > ⑤ Objets GPO Starter > ⑥ Objets GPO Starter > Ø Objets GPO Starter > Ø Objets GPO Starter ● Ø Objets	🗢 🔿 🚾 🔍 🖓 🖬					
(aucun> ∨ Ouvrir	Image: Section de stratégie de groupe Image: Section de stratégie de groupe <t< td=""><td>Default Domain Controllers Polic Ètendue Détais Paramètres Délégation Laisons Afficher les liaisons à cet emplacement : lea Les sites, domaines et unités d'organisation su Emplacement : lea Emplacement Implacement : lea Emplacement Implacement : lea Emplacement Implacement : lea Emplacement Implacement : lea Implacement Implacement : lea Implacement</td></t<> <td>y m Jocal ivants sort liés à ce Appliqué Non quement aux groupe Propriétés e WMI suivant : ~</td> <td>t objet GPO : Lien activé Oui es, utilisateurs et d</td> <td>Chemin d'accès leam local/Domain Controllers</td> <td>> ></td>	Default Domain Controllers Polic Ètendue Détais Paramètres Délégation Laisons Afficher les liaisons à cet emplacement : lea Les sites, domaines et unités d'organisation su Emplacement : lea Emplacement Implacement : lea Emplacement Implacement : lea Emplacement Implacement : lea Emplacement Implacement : lea Implacement Implacement : lea Implacement	y m Jocal ivants sort liés à ce Appliqué Non quement aux groupe Propriétés e WMI suivant : ~	t objet GPO : Lien activé Oui es, utilisateurs et d	Chemin d'accès leam local/Domain Controllers	> >

Dans l'éditeur de gestion des stratégies de groupe > Configuration ordinateur
 Paramètres Windows > Paramètre sécurité > Stratégies locales> Stratégie
 d'audit> Auditer la gestion des comptes :



 Dans les paramètres de stratégie de sécurité, cocher Définir ces paramètres de stratégie et cocher Réussite et Echec :



II- Test : journal d'évènement

Créer un utilisateur dans l'AD. Lors de cette création, grâce à la stratégie mise en place, il est possible de voir la création dans l'observateur d'évènement.

Se rendre dans l'observateur d'évènement et rechercher un évènement 4720 le plus souvent.

Un compte	d'utilisateur a été créé.			
Sujet : ID N Di ID	de sécurité : om du compte : omaine du compte : d'ouverture de session :	LEARN\Administrateur Administrateur LEARN 0x6381F		
Nouveau c ID N D	ompte : I de sécurité : om du compte : omaine du compte :	LEARN\testaudit testaudit LEARN		
Attributs : N N N	om du compte SAM : om complet : om principal de l'utilisati	testaudit test_audit eur : testaudit@	learn.local	
Journal :	Sécurité			
Source :	Microsoft Windows	security Connecté :	18/12/2024 11:24:46	
Événement	4720	Catégorie :	User Account Management	
Niveau :	Information	Mots-clés :	Succès de l'audit	
Utilisateur :	N/A	Ordinateur	DC1.learn.local	
Opcode :	Informations			

III- Audit de modification de mot de passe

Il n'est pas nécessaire de créer une nouvelle GPO puisque dans la configuration de la GPO précédente, l'option de modification de mot de passe est comprise dans l'audit de gestion de compte utilisateur.

> Changer le mot de passe de l'utilisateur :

S lyon.prod	Utilisateur Groupe de séc		
と test_audit	Utilisateur		
	Services de domaine Active Directory X		
	Le mot de passe pour test_audit a été changé.		
	OK		

IV- Test: journal d'évènement

Dans le journal d'évènement, dans le **journal Windows** > **sécurité**, l'évènement 4724 indique qu'une tentative de réinitialisation de mot de passe a été faite :

Sécurité Nombre d'événements : 19 615 (!) No	ouveaux événements di	sponibles		
Niveau	Date et heure	Source	ID de l'événement	Catégorie de la
Q Information	18/12/2024 11:43:33	Microsoft Wi	4634	Logoff
Information	18/12/2024 11:43:33	Microsoft Wi	4724	User Account
Information	18/12/2024 11:43:33	Microsoft Wi	4/38	User Account
Information	18/12/2024 11:43:33	Microsoft Wi	4672	Special Logon
Information	18/12/2024 11:43:33	Microsoft Wi	4769	Kerberos Servi
Information	18/12/2024 11:43:10	Microsoft Wi	5379	User Account
Information	18/12/2024 11:43:10	Microsoft Wi	5379	User Account
Information	18/12/2024 11:43:10	Microsoft Wi	5379	User Account
Information	18/12/2024 11:43:07	Microsoft Wi	5379	User Account
Information	18/12/2024 11:43:07	Microsoft Wi	5379	User Account
Information	18/12/2024 11:43:07	Microsoft Wi	5379	User Account
Événement 4724, Microsoft Windows security au	uditing.			
Général Détails				
Une tentative de réinitialisation de mot de pa	asse d'un compte a été	effectuée.		^
Cuint .				
ID de sécurité : LEARN	Administrateur			
Nom du compte : Admini	strateur			~
Journal : Sécurité				
Source : Microsoft Windows security	Connecté : 18/12/20	024 11:43:33		
Événement : 4724	Catégorie : User Acc	count Management		
Niveau : Information	Mots-clés : Succès d	le l'audit		
Utilisateur : N/A	Ordinateur : DC1.lear	n.local		
Opcode : Informations				
Informations : Aide sur le Journal				

Conclusion : Nous avons mis en place un audit activé via GPO qui a permis d'avoir des informations dans le journal d'événement, lors de la création d'un utilisateur ou d'un changement de mot de passe.