

VITAL Louis

Audit de la gestion des comptes utilisateurs AD sur le contrôleur de domaine

Ouvrez la gestion des stratégies de groupe et sélectionnez la GPO « Default Domain Controllers Policy ».



Activez l'audit de la gestion des comptes utilisateurs en la modifiant pour cocher la case "Succès".



Dans l'Observateur d'événements, vérifiez que l'utilisateur a été correctement créé avec l'ID 4720.

Source	Date et heure	ID de l'événement	Catégorie de la tâche
Succès de l'audit	16/05/2024 16:40:00	4738	User Account Management
Succès de l'audit	16/05/2024 16:40:00	4720	User Account Management
Succès de l'audit	16/05/2024 16:38:25	4719	Audit Policy Change

Événement 4720, Microsoft Windows security auditing.

Général Détails

Un compte d'utilisateur a été créé.

Sujet :

- ID de sécurité : LEARN\Administrateur
- Nom du compte : Administrateur
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x20E10B

Nouveau compte :

- ID de sécurité : LEARN\testaudit
- Nom du compte : testaudit
- Domaine du compte : LEARN

Attributs :

- Nom du compte SAM : testaudit
- Nom complet : testaudit
- Nom principal de l'utilisateur : testaudit@learn.local

Journal : Sécurité

Source : Microsoft Windows security

Connecté : 16/05/2024 16:40:08

Événement : 4720

Catégorie : User Account Management

Niveau : Information

Mots-clés : Succès de l'audit

Mots-clés	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Succès de l'audit	16/05/2024 17:03:06	Microsoft Windows security audit...	4724	User Account Management
Succès de l'audit	16/05/2024 17:03:06	Microsoft Windows security audit...	4738	User Account Management
Succès de l'audit	16/05/2024 16:51:05	Microsoft Windows security audit...	5379	User Account Management
Succès de l'audit	16/05/2024 16:51:05	Microsoft Windows security audit...	5379	User Account Management
Succès de l'audit	16/05/2024 16:51:05	Microsoft Windows security audit...	5379	User Account Management
Succès de l'audit	16/05/2024 16:50:54	Microsoft Windows security audit...	5379	User Account Management
Succès de l'audit	16/05/2024 16:50:54	Microsoft Windows security audit...	5379	User Account Management
Succès de l'audit	16/05/2024 16:50:54	Microsoft Windows security audit...	5379	User Account Management

Événement 4724, Microsoft Windows security auditing.

Général Détails

Une tentative de réinitialisation de mot de passe d'un compte a été effectuée.

Sujet :

- ID de sécurité : LEARN\Administrateur
- Nom du compte : Administrateur
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x9F3C48

Compte cible :

- ID de sécurité : LEARN\testaudit
- Nom du compte : testaudit
- Domaine du compte : LEARN