Guide de l'utilisateur Tenable Identity Exposure SaaS

Dernière révision : 5 juin 2025

Copyright © 2025 Tenable, Inc. Tous droits réservés. Tenable, Tenable Nessus, Tenable Lumin, Assure et le logo Tenable sont des marques déposées de Tenable, Inc. ou de ses filiales. Tous les autres produits ou services sont des marques commerciales de leurs propriétaires respectifs.

Table des matières

Bienvenue dans le Guide de l'utilisateur Tenable Identity Exposure SaaS **12**

À propos de ce guide 12

Prise en main de Tenable Identity Exposure SaaS **13**

Vérifier les conditions préalables 14

Installer 14

Configurer 15

Utiliser 15

Intégrer Tenable Identity Exposure à Tenable One 15

Conditions requises pour Secure Relay 17

Secure Relay pour Tenable Identity Exposure 24

Conditions requises pour Secure Relay 33

Configurer le Relay 39

Installer le Secure Relay (CLI) 40

Installer le Secure Relay (Agent Tenable) 42

Résolution des problèmes liés à l'installation de Secure Relay 44

Commencer à utiliser Tenable Identity Exposure 53

Bases de Tenable Identity Exposure **79**

Se connecter à Tenable Identity Exposure 79

Portail utilisateur Tenable Identity Exposure 85

Page d'informations de Tenable Identity Exposure 88

En-tête 90

Navigation dans les sections 90

Sélection d'un domaine ou d'une organisation 91

Section « Priorisation et remédiation » 91
Section « Démographie » 93
Pour afficher des informations détaillées : 94
Section « Tendances des détections » 95
Création de rapports 96
Accéder à l'espace de travail 98
Menu Espace de travail 99
Page Espace de travail 100
Préférences utilisateur 103
Notifications 106
Dashboards 108
Widgets 110
Centre d'exposition 114
Conditions préalables 115
Voir aussi 115
Vue d'ensemble de la cyber-exposition 115
Informations d'en-tête 116
Liste des faiblesses 116
Options de recherche, de filtrage, d'exportation et d'affichage des colonnes 117
Voir aussi 122
Instances d'exposition 122
Informations générales 123
Informations détaillées 123
Analyse des détections 125

Détails des détections 127
Options de recherche, de filtrage et d'exportation 130
Pour filtrer la liste des faiblesses : 131
Voir aussi 132
Exclusions d'instances d'exposition 132
Personnalisez vos scans de sécurité grâce aux exclusions d'assets 132
Identités 360 – Gestion complète du risque d'identité 137
Collecte d'identités 140
Tenant, domaine et organisation IDP 140
Données multi-produits (sources de données) 141
Principaux éléments 144
Voir aussi 145
Détails sur l'identité 145
Pour accéder à la page : 145
En-tête et section supérieure 146
Onglets d'en-tête 147
155
Fondamentaux d'« Identités 360 » 159
Pour appliquer un filtre : 160
Pour exporter des données : 162
Pour personnaliser l'affichage des colonnes : 163
Affichage par défaut des colonnes 165
Pour rétablir l'affichage par défaut des colonnes : 165
Comprendre l'appartenance à un tenant 165

Lier des assets à un tenant ... 166
Identification du tenant ... 166
Exemple ... 166
Cas spéciaux : compréhension des liens de domaines racines de forêt ... 166
Que sont les domaines racines de forêt ? ... 166
Comment les cas spéciaux se produisent-ils ? ... 167
Exemple ... 167
Exemple ... 167
Pourquoi c'est important ... 168
Pourquoi Tenable Identity Explorer a choisi « tenant » comme nom de conteneur racine 168
Trail Flow ... 168
Tableau Trail Flow ... 170
Lancer une recherche dans Trail Flow à l'aide de l'assistant ... 172
Recherche manuelle dans Trail Flow ... 174
Personnaliser les requêtes Trail Flow ... 175
Ajouter des requêtes aux favoris ... 178
Historique des requêtes ... 181
Afficher les événements déviants ... 183
Détails d'un événement ... 184
Changements d'attribut ... 187
Cas d'utilisation du Trail Flow ... 190
Indicateurs d'exposition ... 194
Date de résolution et de détection de la déviance ... 196
Détails d'un indicateur d'exposition ... 197

Objets déviants 200
Rechercher des objets déviants 202
Ignorer un objet déviant ou une raison (Déviance) 206
Attributs incriminants 210
Indicateurs d'exposition basé sur un RSoP 212
Améliorations 213
Avantages 214
Aspects techniques 214
Remédier à des déviances liées à des indicateurs d'exposition 214
Attribut adminCount appliqué à des utilisateurs non administrateurs 215
Délégation Kerberos dangereuse 218
S'assurer de la cohérence de SDProp 224
Indicateurs d'attaque 228
Détails d'un indicateur d'attaque 231
Incidents liés aux indicateurs d'attaque 233
Topologie 239
Relations d'approbation 240
Relations d'approbation dangereuses 243
Chemin d'attaque 244
Relations d'attaque 249
Ajouter des identifiants de clé 250
Ajouter un membre 252
Autorisé à agir 254
Autorisé à déléguer 256

Appartient à la GPO 260
DCSync 261
Attribuer autorisé à agir 263
A un historique SID 265
Prise de contrôle implicite 268
Hérite de GPO 269
GPO liée 271
Membre de 273
Détient 274
Réinitialiser mot de passe 276
Gestion RODC 278
Modifier DACL 280
Modifier propriétaire 282
Identification des assets Tier 0 283
Comptes avec des chemins d'attaque 285
Types de nœuds du chemin d'attaque 287
Journaux d'activité 290
Définitions des entités privilégiées 292
Active Directory 292
Entra ID 293
Configuration et administration de Tenable Identity Exposure 294
Activation de la prise en charge de « Identités 360 », « Centre d'exposition » et « Microsoft Entra ID » 294
Configuration d'Active Directory 296
Accès aux objets ou conteneurs AD 296

Accès pour l'analyse privilégiée 297
Déploiement des indicateurs d'attaque 304
Installer des indicateurs d'attaque 307
Script d'installation des indicateurs d'attaque 315
Modifications techniques et impact potentiel 324
Scénarios d'attaque (< v. 3.36) 325
Programme d'installation de Microsoft Sysmon 330
Désinstaller les indicateurs d'attaque 335
Suppression manuelle des dossiers de GPO obsolètes de SYSVOL 337
Indicateurs d'attaque désactivés 337
Statut de l'icône de la première ligne 338
Statut de l'icône des autres lignes 338
Dépanner les indicateurs d'attaque 340
Détection antivirus 340
Précédence des configurations avancées de stratégie d'audit 342
Validation de l'observateur des journaux d'événements 344
Fichiers journaux Tenable Identity Exposure 346
Atténuation des problèmes liés à la réplication DFS 352
Rétention du journal des événements Windows 354
Entrées de type « Inconnu » dans les alertes d'indicateurs d'attaque 354
Indicateurs d'attaque opérationnels 358
Délais de détection des indicateurs d'attaque 359
Authentification 360
Authentification à l'aide de Tenable One 360

Authentification à l'aide d'un compte Tenable Identity Exposure 361
Authentification à l'aide de LDAP 364
Authentification à l'aide de SAML 370
Comptes utilisateur 373
Profils de sécurité 377
Personnaliser un indicateur 378
Affiner la personnalisation sur un indicateur 381
Rôles utilisateur 382
Gérer les rôles 383
Définir les autorisations d'un rôle 384
Définir des autorisations sur les entités de type Interface utilisateur (exemple) 389
Forêts 391
Gestion des forêts 391
Protection des comptes de service 392
Domaines 393
Forcer l'actualisation des données sur un domaine 397
Honey Accounts 397
Authentification Kerberos 400
Alertes 407
Configuration de serveur SMTP 408
Différences dans l'architecture de déploiement 408
Configuration du serveur SMTP pour les environnements Secure Relay 408
Configuration du serveur SMTP pour les environnements VPN 410
Alertes par e-mail 411

Alertes Syslog 415
Détails des alertes Syslog et par e-mail 419
Encadrement des messages Syslog 423
Vérifications de l'état du système 426
Liste des vérifications de l'état du système 431
Centre de rapports 435
Prise en charge de Microsoft Entra ID 437
Actualiser les identifiants Entra ID 446
Pour actualiser vos identifiants et restaurer la synchronisation : 446
Collecte de données via Tenable Cloud 451
Analyse privilégiée 452
Journaux d'activité 453
API publique Tenable Identity Exposure 456
Gestion des données 458
Régions de déploiement 459
Licences Tenable Identity Exposure 460
Gérer votre licence 462
Prévention des incohérences de l'UUID de conteneur 463
Versions LTS (Long-Term Support) et normales : avantages et différences clés 466
Que sont les versions LTS ? 467
Que sont les versions normales ? 467
Différences clés entre les versions LTS et normales : 467
Pourquoi choisir les versions LTS ? 467
Pourquoi choisir les versions normales ? 468

Résolution des problèmes touchant Tenable Identity Exposure 468
Interférence du durcissement SYSVOL avec Tenable Identity Exposure 468
Utilitaire système (handle.exe) 478

Bienvenue dans le Guide de l'utilisateur Tenable Identity Exposure SaaS

Dernière mise à jour : 30 juin 2025

Tenable Identity Exposure permet de sécuriser votre infrastructure en anticipant les menaces, en détectant les violations et en répondant aux incidents et aux attaques. Grâce à un dashboard intuitif qui permet de surveiller Active Directory en temps réel, vous pouvez identifier d'un coup d'œil les vulnérabilités les plus critiques et les mesures de remédiation recommandées. Les indicateurs d'attaque et les indicateurs d'exposition de Tenable Identity Exposure permettent de découvrir les problèmes sous-jacents qui affectent votre Active Directory, d'identifier les relations d'approbation dangereuses et d'analyser en profondeur les détails des attaques.

Pour commencer, voir Commencer à utiliser Tenable Identity Exposure.

À propos de ce guide

Ce Guide de l'utilisateur Tenable Identity Exposure SaaS traite des sujets suivants :

- L'installation d'un Secure Relay
- Les tâches à effectuer avant d'activer la surveillance de la sécurité
- La configuration et l'utilisation de Tenable Identity Exposure

Les fonctionnalités Indicateurs d'attaque et Indicateurs d'exposition sont disponibles en fonction de la licence que vous avez acquise.

Remarque : Tenable Identity Exposure est disponible seul ou dans le cadre de la suite Tenable One. Pour plus d'informations, voir Tenable One.

Conseil : le *Guide de l'utilisateur Tenable Identity Exposure* est disponible en anglais, en français, en allemand, en japonais, en coréen, en chinois simplifié, en espagnol et en chinois traditionnel. L'interface utilisateur de *Tenable Identity Exposure* est disponible en anglais, en français, en allemand, en japonais, en coréen, en chinois simplifié, en espagnol et en chinois traditionnel. Pour modifier la langue de l'interface utilisateur, voir Préférences utilisateur (Préférences utilisateur).

Pour plus d'informations sur Tenable Identity Exposure, consultez les supports de formation client suivants :

- Guide d'intégration autonome Tenable Identity Exposure (en anglais)
- Introduction à Tenable Identity Exposure (Tenable University)

Plateforme de gestion de l'exposition Tenable One

Tenable One est une plateforme de gestion de l'exposition qui permet aux organisations de gagner en visibilité sur la surface d'attaque moderne, de concentrer leurs efforts pour prévenir les attaques probables et de communiquer avec précision sur le cyber-risque, afin d'assurer des performances opérationnelles optimales.

La plateforme offre la protection la plus large contre les vulnérabilités puisqu'elle couvre les assets informatiques, les ressources cloud, les conteneurs, les applications web et les systèmes d'identité, s'appuie sur la rapidité et l'étendue de la couverture des vulnérabilités de Tenable Research et ajoute des analyses complètes pour prioriser les actions et communiquer sur le cyber-risque. Grâce à Tenable One, les entreprises :

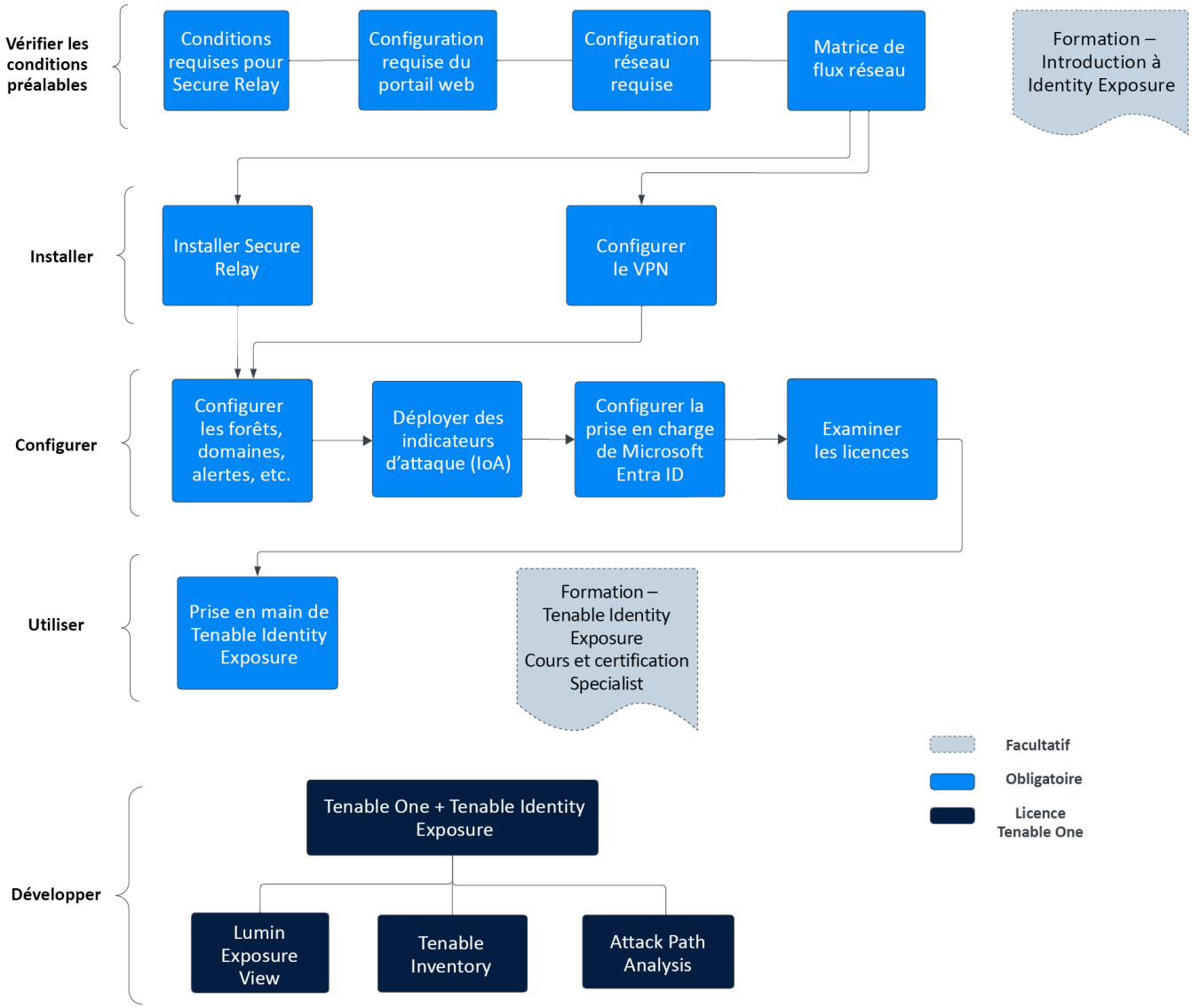
- bénéficient d'une visibilité complète sur l'ensemble de la surface d'attaque moderne ;
- anticipent les menaces et priorisent leurs efforts pour prévenir les attaques ;
- communiquent sur le cyber-risque pour prendre de meilleures décisions.

Tenable Identity Exposure existe en tant que produit autonome ou peut être acheté dans le cadre de la plateforme de gestion de l'exposition Tenable One.

Conseil : pour plus d'informations sur la prise en main des produits Tenable One, voir le Guide de déploiement de Tenable One (en anglais).

Prise en main de Tenable Identity Exposure SaaS

Utilisez le workflow suivant pour procéder au déploiement de Tenable Identity Exposure.



Vérifier les conditions préalables

1. **Consultez** les notes de version.
2. **Examinez attentivement le rôle de Secure Relay** au sein de la plateforme Tenable Identity Exposure – À partir de la version **3.59**, la fonction obligatoire Secure Relay vous permet de configurer les domaines à partir desquels le Relay transfère les données au composant Directory Listener chargé de collecter les objets AD. Voir Conditions requises pour Secure Relay.

Installer

1. **Installez** le Secure Relay pour Tenable Identity Exposure .

Configurer

1. **Consultez** Licences Tenable Identity Exposure.

Utiliser

- Commencer à utiliser Tenable Identity Exposure

Intégrer Tenable Identity Exposure à Tenable One

> **Remarque** : cela nécessite une licence Tenable One. Pour plus d'informations sur l'essai de Tenable One, voir Tenable One.

Intégrez Tenable Identity Exposure à Tenable One et exploitez les fonctionnalités suivantes :

- Dans Lumin Exposure View, obtenez des informations essentielles sur le contexte métier grâce au score CES (Cyber Exposure Score) unifié pour les services, processus et fonctions métier critiques, et suivez le respect des SLA. Suivez le risque global lié aux identités pour comprendre la contribution du risque des applications web à votre score CES (Cyber Exposure Score) global.
    - Examinez la fiche d'exposition **Global Exposure Card** (Fiche d'exposition globale) pour comprendre votre score holistique. Cliquez sur **Per exposure** (Par exposition) pour comprendre quels facteurs déterminent votre score et dans quelle mesure.
    - Consultez la fiche d'exposition **Active Directory** (Fiche Active Directory).
    - Configurez les paramètres de la vue de l'exposition (Exposure View Settings) pour définir une **cible de fiche** personnalisée et paramétrer les options **Remediation SLA** (SLA de remédiation) et **SLA Efficiency Target** (Efficacité du SLA) en fonction de la politique de votre entreprise.
    - Créez une fiche d'exposition personnalisée (Custom Exposure Card) en fonction du contexte de l'entreprise (par exemple, domaines, admins de domaine, criticité des assets, utilisateurs critiques/assets critiques ou comptes de service).

- Dans Tenable Inventory, améliorez les renseignements sur les assets en accédant à des informations plus approfondies à leur sujet, notamment les chemins d'attaque associés, les tags, les fiches d'exposition, les utilisateurs, les relations, etc. Améliorez l'évaluation du score de risque en acquérant une vue plus complète de l'exposition des assets grâce au score AES (Asset Exposure Score) qui évalue le risque total et la criticité des assets pour les identités.
    - Examinez vos assets AD pour comprendre la nature stratégique de l'interface. Cela devrait vous aider à choisir les fonctionnalités à utiliser dans Tenable Inventory et dans quelles circonstances les utiliser.
    - Passez en revue les requêtes **Tenable** (Tenable Queries) que vous pouvez utiliser, modifier et ajouter aux favoris.
    - Familiarisez-vous avec le générateur de requêtes de recherche globale, ainsi qu'avec ses objets et propriétés. Ajoutez des requêtes personnalisées aux favoris pour les réutiliser ultérieurement.

      > **Conseil :** pour obtenir un aperçu des propriétés disponibles :
      >
      > - Dans le générateur de requêtes, saisissez *has*. La liste des propriétés d'asset suggérées s'affiche.
      > - Personnalisez la liste en ajoutant une colonne. La liste des colonnes/propriétés disponibles s'affiche.

    - Explorez la page des détails de l'asset pour consulter les propriétés de l'asset et toutes les vues contextuelles associées.
    - (Facultatif) Créez un tag qui combine différentes classes d'assets.
- Dans Attack Path Analysis, optimisez la priorisation des risques en exposant les chemins d'attaque à risque qui traversent la surface d'attaque, y compris les applications web, IT, OT, IoT, les identités et ASM, pour éviter tout impact significatif. Simplifiez l'atténuation en identifiant des points d'étranglement afin de perturber les chemins d'attaque en suivant des conseils d'atténuation, et approfondissez votre expertise grâce aux informations exploitables de l'IA.
    - Affichez le dashboard **Attack Path Analysis** (Analyse du chemin d'attaque) pour obtenir une vue de haut niveau sur les assets vulnérables avec le nombre de chemins d'attaque menant à ces assets critiques, le nombre de détections ouvertes et leur sévérité, une

matrice affichant les chemins avec différents scores d'exposition de nœud source et des combinaisons de valeurs cibles ACR, ainsi qu'une liste de tendances concernant les chemins d'attaque.

- Examinez la **Top Attack Path Matrix** (matrice des principaux chemins d'attaque) et cliquez sur la tuile **Top Attack Paths** (Chemins d'attaque principaux) pour afficher des informations supplémentaires sur les chemins menant à vos assets les plus précieux.

Vous pouvez les ajuster si nécessaire pour visualiser les données et les détections les plus critiques concernant les chemins d'attaque.

- Sur la page **Findings** (Détections), affichez toutes les techniques d'attaque présentes dans un ou plusieurs chemins d'attaque qui mènent à un ou plusieurs assets critiques en associant vos données à des analyses graphiques avancées et au cadre MITRE ATT&CK®. Vous pourrez ainsi créer des détections qui vous aideront à comprendre et à traiter les inconnues qui favorisent et amplifient l'impact des menaces sur vos assets et vos informations.
- Sur la page **Discover** (Découvrir), générez des requêtes de chemin d'attaque pour afficher vos assets dans le cadre de chemins d'attaque potentiels :
  - Generate an Attack Path using a Built-in Query (Générer un chemin d'attaque à l'aide d'une requête intégrée)
  - Generate an Asset Query using the Asset Query Builder (Générer une requête d'asset à l'aide du générateur de requêtes d'asset)
  - Generate an Attack Path Query using the Attack Path Query Builder (Générer une requête de chemin d'attaque à l'aide du générateur de requêtes de chemin d'attaque)

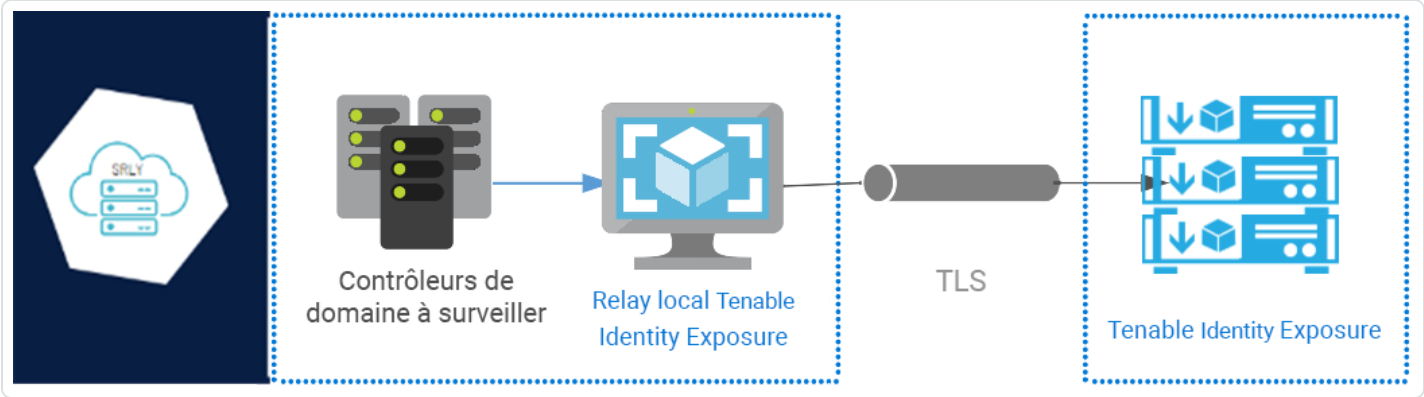
  Vous pouvez ensuite afficher les données des requêtes de chemin d'attaque (Attack Path Queries) et des requêtes d'asset (Asset Queries) et interagir avec elles via la liste des résultats des requêtes et le graphe interactif.

Conditions requises pour Secure Relay

Secure Relay est un mode de transfert de vos données Active Directory de votre réseau vers Tenable Identity Exposure qui utilise le protocole TLS (Transport Layer Security) au lieu d'un VPN,

comme illustré dans ce diagramme. La fonctionnalité Relay prend aussi en charge le proxy HTTP avec ou sans authentification si votre réseau nécessite un serveur proxy pour accéder à Internet.

Tenable Identity Exposure peut prendre en charge plusieurs Secure Relays que vous pouvez mapper aux domaines en fonction de vos besoins.



Exigences TLS

Pour utiliser TLS 1.2, votre serveur Relay doit prendre en charge au moins l'une des suites de chiffrement suivantes à partir du 24 janvier 2024 :

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

Assurez-vous également que votre configuration Windows correspond aux suites de chiffrement spécifiées pour assurer la compatibilité avec la fonctionnalité Relay.

Pour vérifier les suites de chiffrement :

1. Dans PowerShell, exécutez la commande suivante :

   ```
   @("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
   ```

2. Vérifiez la sortie : `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`.

```
PS C:\Users> @("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
, "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }


KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 128
BaseCipherSuite       : 49199
CipherSuite           : 49199
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Protocols             : {771, 65277}

KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 256
BaseCipherSuite       : 49200
CipherSuite           : 49200
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocols             : {771, 65277}
```

3. Une sortie vide indique qu'aucune des suites de chiffrement requises pour la connexion TLS du Relay n'est activée. Activez au moins une suite de chiffrement.
4. Vérifiez la courbe Elliptic Curve Cryptography (ECC) à partir du serveur du Relay. Cette vérification est obligatoire pour utiliser les suites de chiffrement Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Dans PowerShell, exécutez la commande suivante :

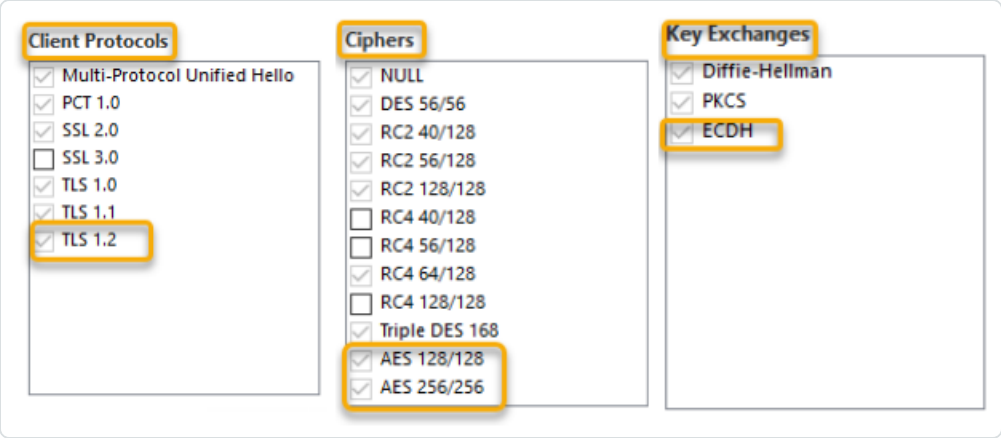
```
Get-TlsEccCurve
```

5. Vérifiez que vous disposez de la courbe **25519**. Si ce n'est pas le cas, activez-la.

```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

Pour vérifier les paramètres de chiffrement Windows :

1. Dans un outil IIS Crypto, vérifiez que les options suivantes sont activées :
    - Protocoles client : **TLS 1.2**
    - Chiffrements : **AES 128/128** et **AES 256/256**
    - Échanges de clés : **ECDH**

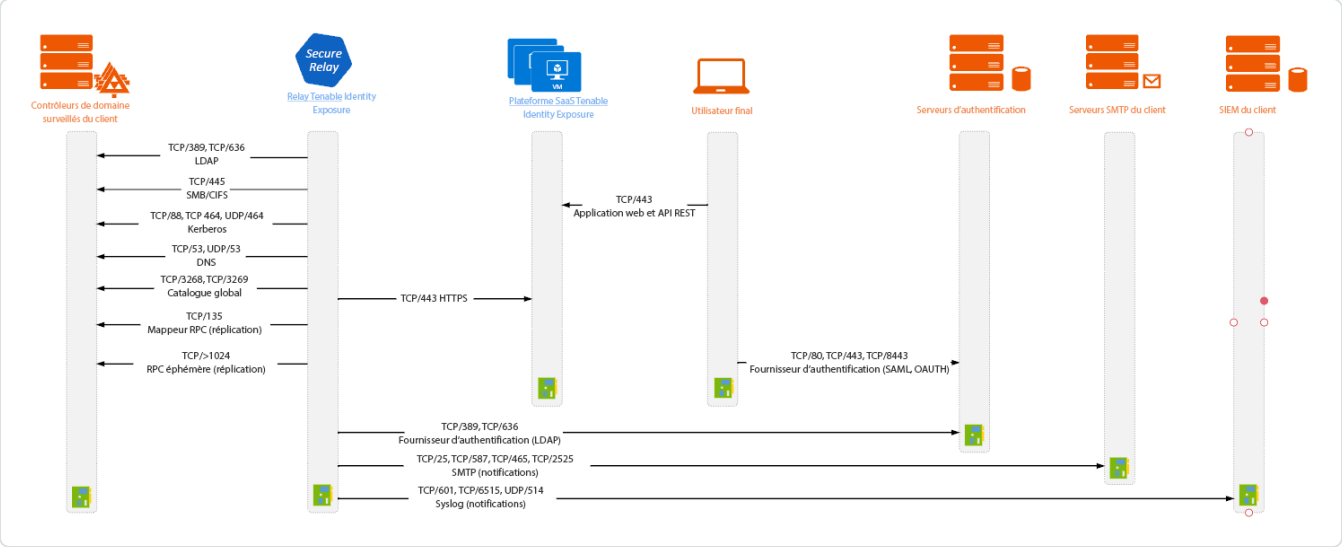


2. Après avoir modifié les paramètres de chiffrement, redémarrez la machine.

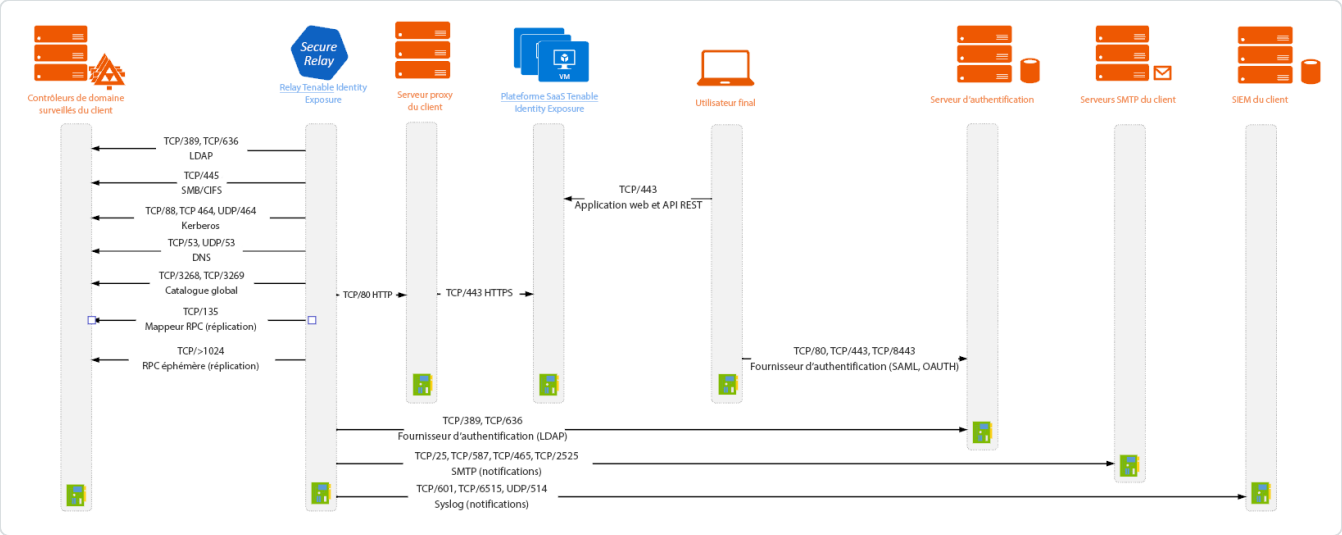
> **Remarque** : la modification des paramètres de chiffrement Windows affecte toutes les applications exécutées sur la machine et utilisant la bibliothèque TLS de Windows, connue sous le nom de « Schannel ». Par conséquent, assurez-vous que tout ajustement que vous effectuez n'entraîne pas d'effets secondaires non souhaités. Vérifiez que les configurations choisies sont compatibles avec les objectifs généraux de durcissement ou les mandats de conformité de l'organisation.

Ports requis

- Pour une configuration classique **sans serveur proxy**, le Relay nécessite les ports suivants :



Pour une configuration **avec un serveur proxy**, le Relay nécessite les ports suivants :



Remarque : les flux réseau fonctionnent de la même manière pour les plateformes sur site et SaaS.

Conditions préalables pour les machines virtuelles

La machine virtuelle (VM) hébergeant le Secure Relay doit présenter les caractéristiques suivantes :

Taille du client	Services Tenable	Instance	Mémoire (par	vCPU (par	Topologie de	Espace disque

	Identity Exposure	requise	instance)	instance)	disque	disponible (par instance)
N'importe quelle taille	• tenable_Relay • tenable_envoy	1	8 Go de RAM	2 vCPU	Partition pour les journaux distincte de la partition système	30 GB

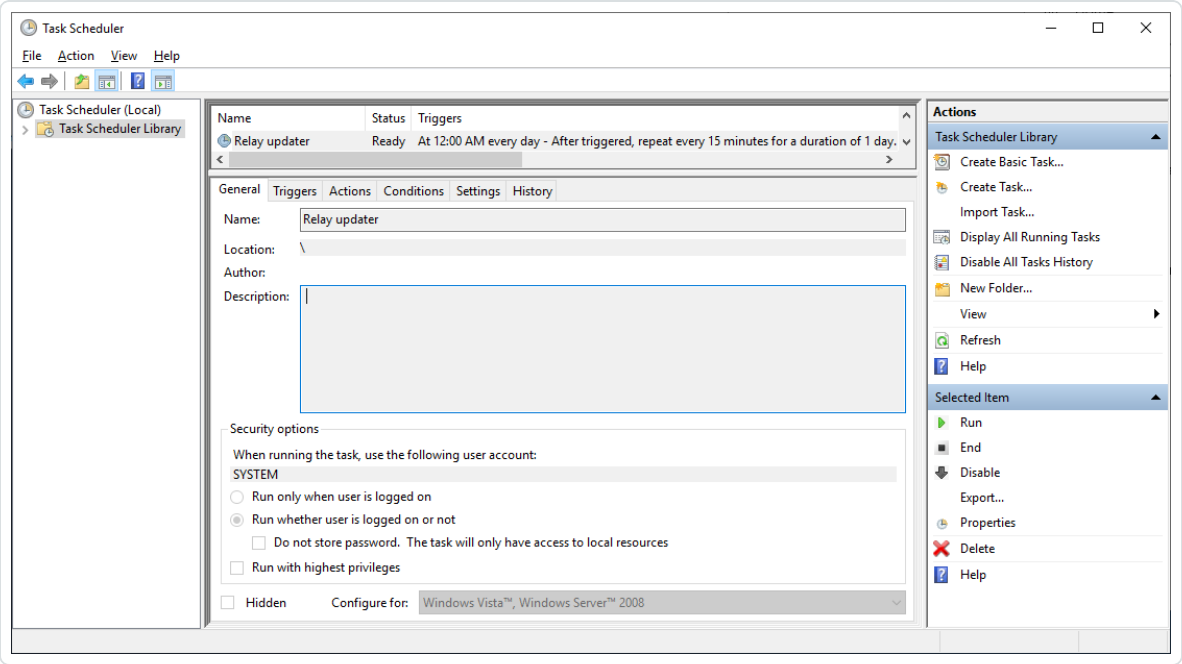
Remarque : si vous installez le Secure Relay et le Directory Listener sur la même machine virtuelle, vous devez combiner leurs exigences de dimensionnement. Voir Resource Sizing.

Conseil : pour l'installation initiale, il est préférable que la VM ne soit pas jointe au domaine, afin d'éviter d'hériter de politiques de GPO existantes susceptibles d'interférer avec le processus d'installation. Une fois l'installation terminée, vous pouvez joindre la VM au domaine.

La VM doit également présenter les caractéristiques suivantes :

- Trafic HTTPS – Supprimez, désactivez, contournez ou ajoutez à la liste d'autorisations tout client capable de diriger le trafic HTTP/HTTPS vers la machine Secure Relay. Cette action bloque l'installation du Secure Relay et interrompt ou ralentit le trafic entrant dans la plateforme Tenable.
- Un système d'exploitation Windows Server 2016+ (pas Linux)
- Une résolution des requêtes DNS orientées Internet et un accès à Internet pour au moins `cloud.tenable.com` et `*.tenable.ad` (TLS 1.2).
- Des privilèges d'administrateur local
- Une configuration EDR, antivirus et GPO :
    - Quantité de processeur suffisante disponible sur la VM – Par exemple, la fonctionnalité temps réel de Windows Defender consomme une quantité considérable de processeur et peut saturer la machine.

- Mises à jour automatiques :
  - Autorisez les appels vers `*.tenable.ad`, afin que la fonctionnalité de mise à jour automatique puisse télécharger un fichier exécutable Relay.
  - Vérifiez qu'aucune stratégie de groupe (GPO) ne bloque la fonction de mise à jour automatique.
  - Ne supprimez ni ne modifiez la tâche planifiée « Relay updater » :



Fichiers et processus autorisés

Pour que le Relay fonctionne correctement, vous devez autoriser certains fichiers et processus auprès des outils de sécurité tiers, en particulier les antivirus et/ou les outils EDR (détection et réponse des terminaux) et XDR (détection et réponse étendues).

> Remarque : adaptez le chemin C:\ au lecteur d'installation de Relay.

Windows
Fichiers
C:\Tenable*

C:\tools*
C:\ProgramData\Tenable*
Processus
nssm.exe --> chemin : C:\tools\nssm.exe
Tenable.Relay.exe --> chemin : C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> chemin : C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe --> chemin : C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> Chemin : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (peut être différent selon la version du système d'exploitation)
Tâches planifiées
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay
Clé de registre
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

Secure Relay pour Tenable Identity Exposure

À partir de la version 3.59, le composant **Secure Relay** prend en charge les tâches désignées sur la plateforme Tenable Identity Exposure :

- Permet de configurer les domaines à partir desquels il transfère les données au composant Directory Listener (DL) qui collecte les objets AD.
- Facilite la configuration et la maintenance des grandes infrastructures grâce aux mises à jour automatiques : n'a plus besoin de multiples DL qui nécessitent des mises à niveau simultanées.

- Agit comme un pont entre le DL unique et divers terminaux, tels que les contrôleurs de domaine, les serveurs SMTP ou SYSLOG ou les serveurs LDAP pour l'authentification dans le produit.
- Se lie à un ou plusieurs domaines. Le DL peut gérer un nombre illimité de Relays.
- Requiert une configuration dans la console Tenable Identity Exposure, telle que des dénominations et des mappages (domaine, SMTP, SYSLOG, authentification LDAP).

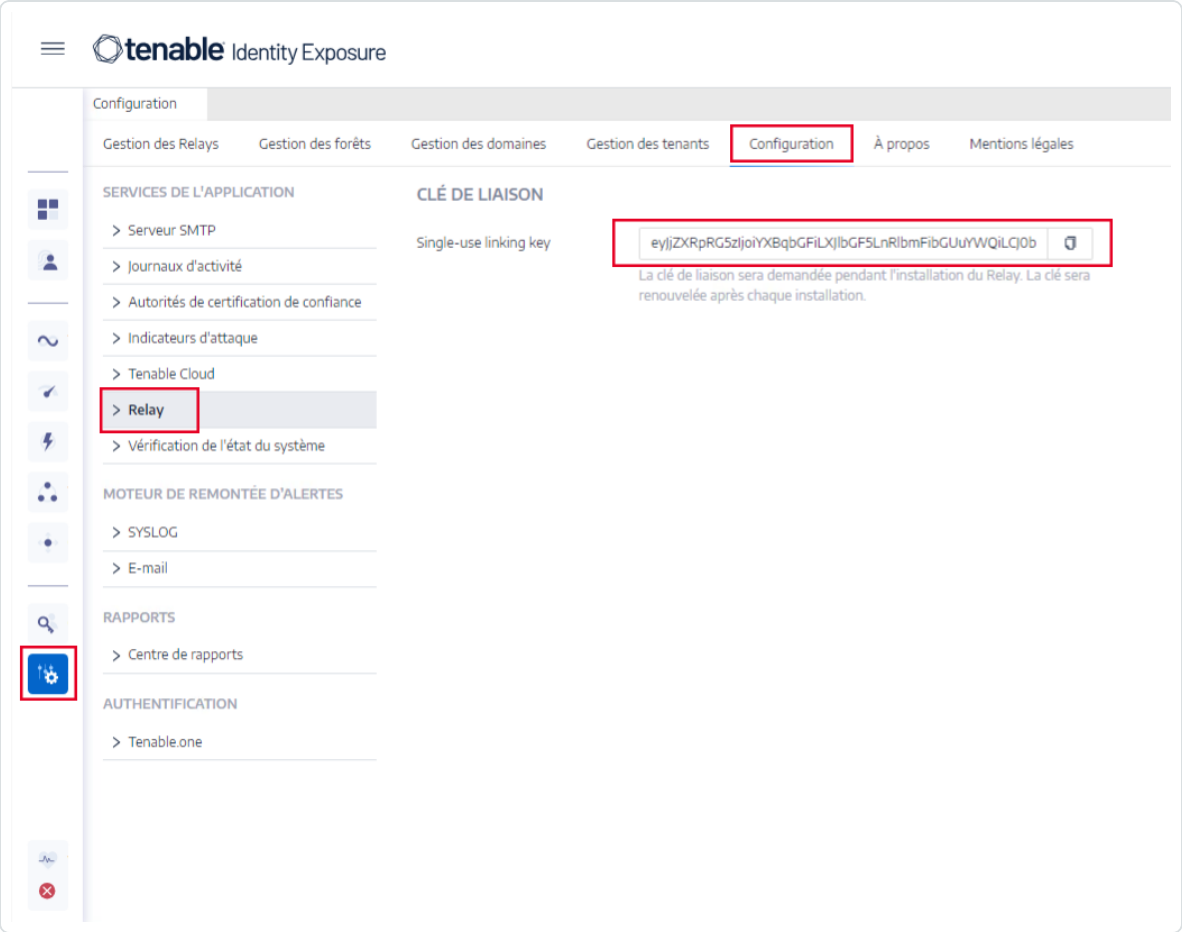
Avant de commencer

Suivez ces directives pour l'installation ou la mise à niveau vers Tenable Identity Exposure 3.59 avec Secure Relay :

1. Passez en revue les les Conditions requises pour Secure Relay.
2. **Configuration réseau requise** :
    - Dans les versions précédentes et actuelles, le DL communiquait directement avec le SEN, à l'aide du protocole AMQP(S).
    - Dans la version 3.59, les Relays qui remplacent les multiples DL communiquent avec le DL restant via HTTPS.
    - Envoy est le proxy inverse.
3. **Clé de liaison** : l'installation de Secure Relay nécessite une clé de liaison à usage unique contenant l'adresse de votre réseau et un jeton d'authentification. Tenable Identity Exposure génère une nouvelle clé après chaque installation réussie de Secure Relay.

    Pour récupérer la clé de liaison :

    1. Dans la console Tenable Identity Exposure, cliquez sur **Système** dans la barre de menu de gauche et sélectionnez l'onglet **Configuration** > **Relay**.



2. Cliquez sur pour copier la clé de liaison.

4. **Autorisations de rôle** : vous devez être un utilisateur pourvu d'autorisations basées sur le rôle pour configurer le Relay. Les autorisations requises sont les suivantes :

   - **Entités de type Donnée** : entité Relay
   - **Entités de type Interface** :
     - Gestion > Système > Configuration > Services de l'application > Relay
     - Gestion > Système > Gestion des Relays

   Pour plus d'informations, voir Définir les autorisations d'un rôle.

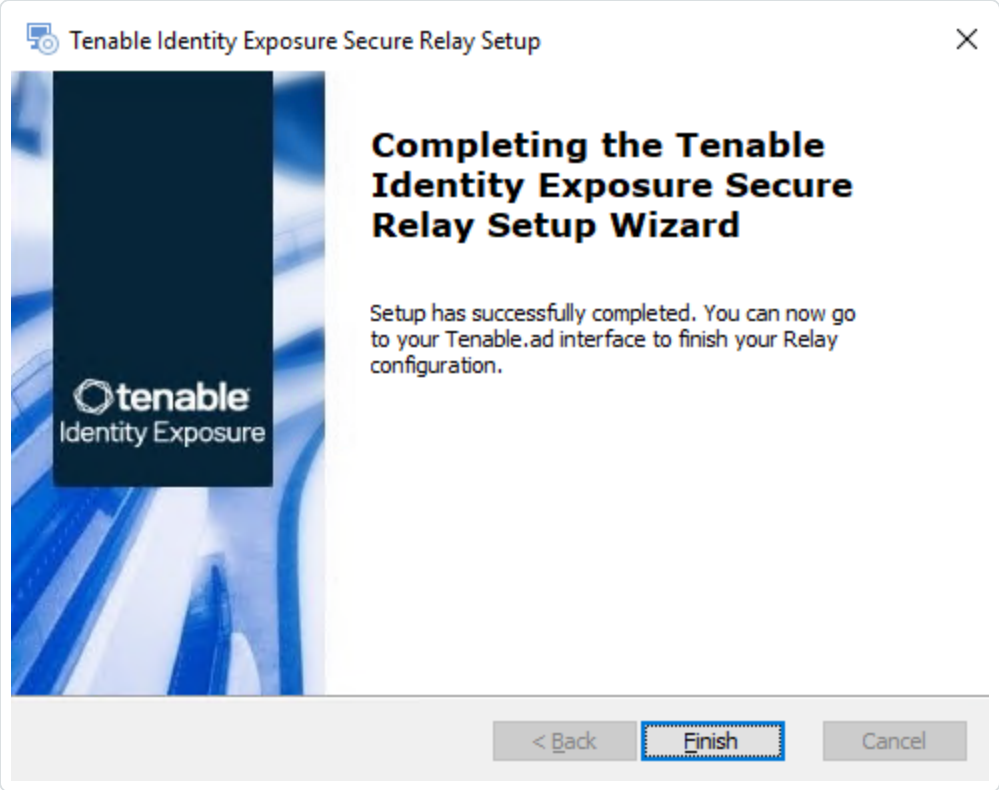
Procédure d'installation

Rôle utilisateur requis : administrateur sur l'ordinateur local.

Pour installer le Secure Relay :

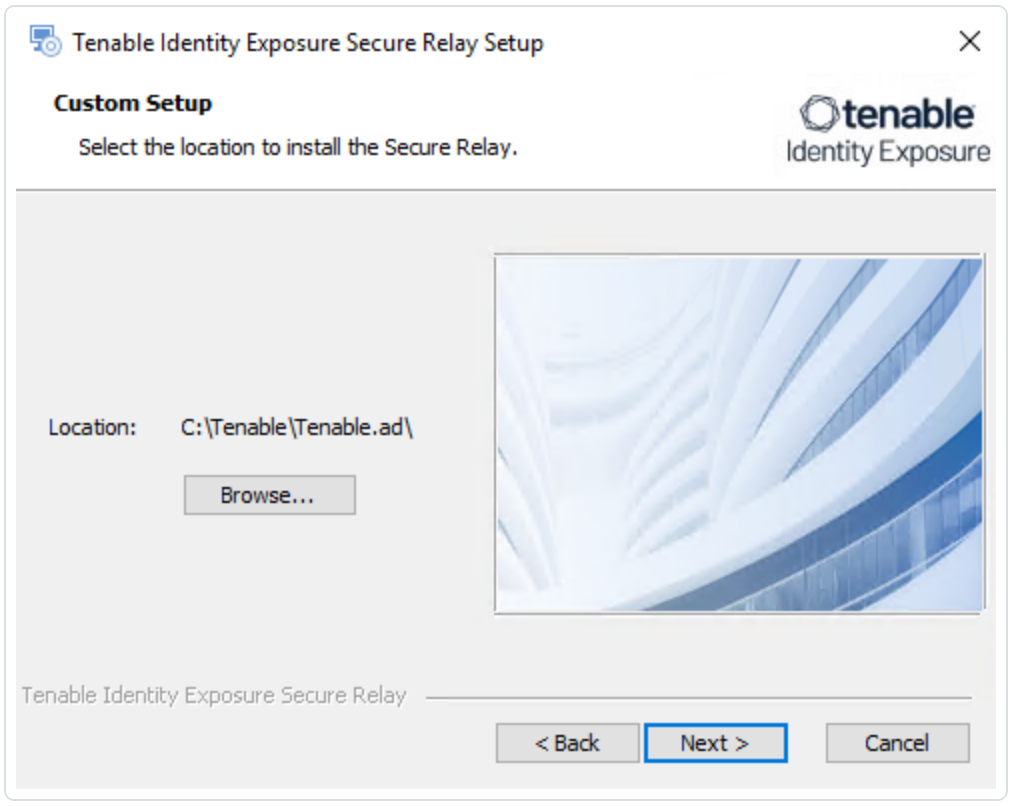
1. Téléchargez le programme exécutable pour Secure Relay à partir du site de téléchargements de Tenable.
2. Double-cliquez sur le fichier `tenable.ad_SecureRelay_v3.xx.x` pour lancer l'assistant d'installation.

   L'écran **Welcome** (Bienvenue) apparaît.



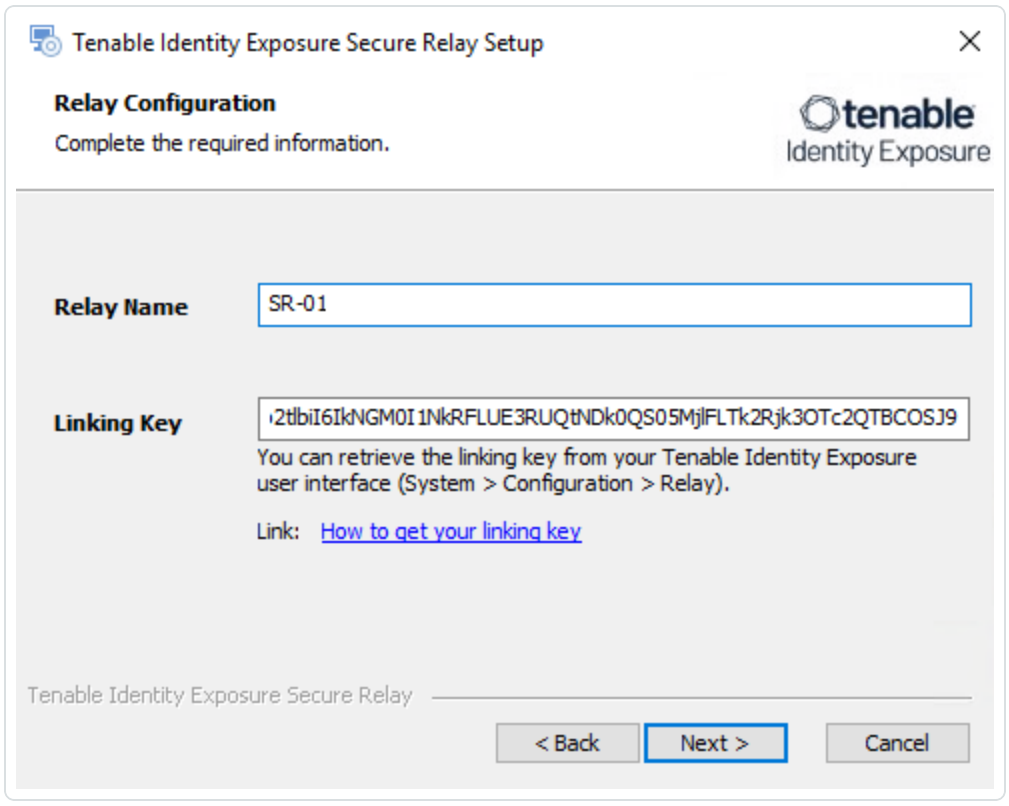
3. Cliquez sur **Next** (Suivant).

   La fenêtre **Custom Setup** (Configuration personnalisée) apparaît.



4. Cliquez sur **Browse** (Parcourir) pour sélectionner la partition de disque que vous avez réservée à Secure Relay (distincte de la partition système).
5. Cliquez sur **Next** (Suivant).

   La fenêtre **Relay Configuration** (Configuration du Relay) apparaît.



6. Fournissez les informations suivantes :

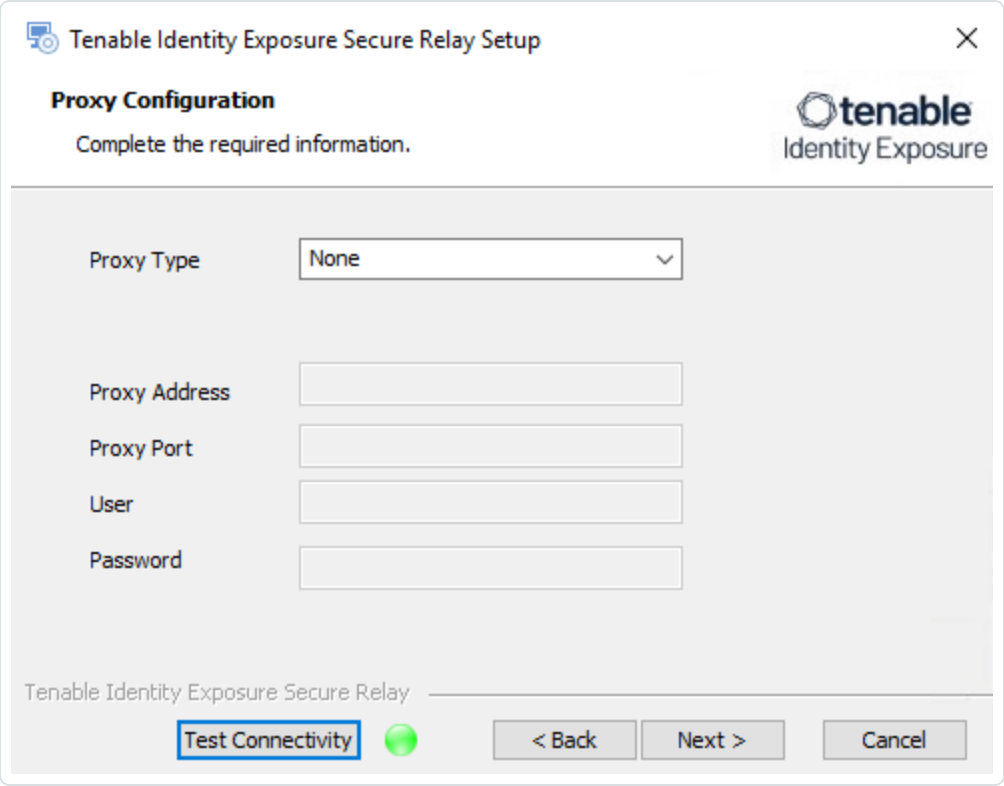
    a. Dans la zone **Relay Name** (Nom du Relay), saisissez le nom de votre Secure Relay.

    b. Dans la zone **Linking key** (Clé de liaison), collez la clé de liaison que vous avez récupérée sur le portail Tenable Identity Exposure.

    c. Si vous choisissez d'utiliser un serveur proxy, sélectionnez l'option **Use an HTTP Proxy for your Relay calls** (Utiliser un proxy HTTP pour les appels de votre Relay) et fournissez l'adresse et le numéro de port du proxy.

7. Cliquez sur **Next** (Suivant).

    La fenêtre Proxy Configuration (Configuration du proxy) apparaît.



8. Sélectionnez l'une des options suivantes :
    a. **None** (Aucun) : aucun serveur proxy n'est utilisé.
    b. **Unauthenticated** (Non authentifié) : saisissez l'adresse et le port du serveur proxy.
    c. **Basic authentication** (Authentification de base) : en plus de l'adresse et du port, saisissez l'utilisateur et le mot de passe du serveur proxy.

    Attention : pour configurer un proxy en utilisant « Unauthenticated » (Non authentifié) ou « Basic authentication » (Authentification de base), le Relay ne prend en charge que les adresses IPv4 (telles que `192.168.0.1`) ou un URI de proxy sans `http://` ou `https://` (tel que `monproxy.masociété.com`). Le Relay ne prend pas en charge les adresses IPv6 (telles que `2001:0db8:85a3:0000:0000:8a2e:0370:7334`).

9. Cliquez sur **Test Connectivity** (Tester la connectivité). Les événements suivants peuvent se produire :

- **Green light** (Feu vert) – La connexion a abouti.
- **Invalid linking key** (Clé de liaison non valide) – Extrayez la clé de liaison à partir du portail Tenable Identity Exposure.
- **Invalid Relay Name** (Nom de Relay non valide) – Cette zone ne peut pas rester vide. Fournissez un nom pour le Relay.
- **Connection failed** (Échec de la connexion) – Vérifiez votre accès à Internet.

10. Cliquez sur **Next** (Suivant).

    La fenêtre **Ready to Install** (Prêt pour l'installation) apparaît.

11. Cliquez sur **Install** (Installer).
12. Une fois l'installation terminée, cliquez sur **Finish** (Terminer).

Vérifications post-installation

Une fois l'installation du Secure Relay terminée, vérifiez les éléments suivants :

Liste des Relays installés dans Tenable Identity Exposure

Pour afficher la liste des Relays installés :

- Dans Tenable Identity Exposure, cliquez sur **Systèmes** dans la barre de menu de gauche et sélectionnez l'onglet **Gestion des Relays**.

  Le volet affiche la liste des Secure Relays et de leurs domaines liés.

Services

Lorsque l'installation aboutit, les services suivants sont en cours d'exécution :

- `Tenable_Relay`
- `tenable_envoy`

> **Remarque** : vous pouvez localiser la licence Envoy dans Tenable Identity Exposure sous **Systèmes** > **Mentions légales** > **Licence Envoy**.

Variables d'environnement

L'installation a également ajouté six nouvelles variables d'environnement liées à Secure Relay dont les noms commencent par « ALSID_CASSIOPEIA_ ». Si vous avez choisi d'utiliser un serveur proxy, il existe deux variables supplémentaires associées à l'adresse IP et au port du proxy.

Journaux pour la résolution des problèmes

Vous trouverez des journaux aux emplacements suivants :

- **Journaux d'installation** : `C:\Users\<votre utilisateur>\AppData\Local\Temp`
- **Journaux Relay** : sur la VM qui héberge Secure Relay dans le dossier spécifié au moment de l'installation.

Configuration du Relay

- Configurer le Relay

Mises à jour automatiques

Après l'installation de Secure Relay, Tenable Identity Exposure recherche régulièrement les nouvelles versions. Ce processus est entièrement automatisé et nécessite un accès HTTPS à votre domaine (TCP/443). Une icône dans la barre d'état réseau indique quand Tenable Identity Exposure met à jour Secure Relay. Une fois le processus terminé, les services Tenable Identity Exposure redémarrent et la collecte de données reprend.

Désinstallation

Pour désinstaller un Secure Relay :

1. Sous Windows, accédez à **Paramètres** > **Applications et fonctionnalités** > **Tenable Identity Exposure Secure Relay**.
2. Cliquez sur **Désinstaller**.

   Une fois la désinstallation terminée, les services et les variables d'environnement Tenable Identity Exposure Secure Relay n'apparaîtront plus dans votre système.
3. Dans Tenable Identity Exposure, cliquez sur **Systèmes** dans la barre de menu de gauche et sélectionnez l'onglet **Gestion des Relays**.

4. Sélectionnez le Relay que vous venez de désinstaller et cliquez sur pour le supprimer de la liste des Relays disponibles.

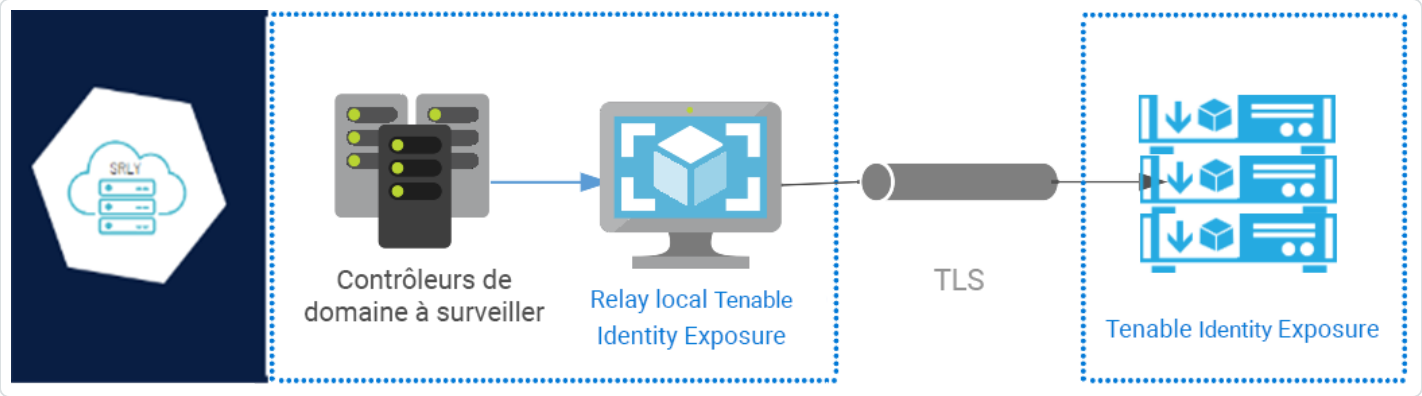
Voir aussi

- Résolution des problèmes liés à l'installation de Secure Relay

Conditions requises pour Secure Relay

Secure Relay est un mode de transfert de vos données Active Directory de votre réseau vers Tenable Identity Exposure qui utilise le protocole TLS (Transport Layer Security) au lieu d'un VPN, comme illustré dans ce diagramme. La fonctionnalité Relay prend aussi en charge le proxy HTTP avec ou sans authentification si votre réseau nécessite un serveur proxy pour accéder à Internet.

Tenable Identity Exposure peut prendre en charge plusieurs Secure Relays que vous pouvez mapper aux domaines en fonction de vos besoins.



Exigences TLS

Pour utiliser TLS 1.2, votre serveur Relay doit prendre en charge au moins l'une des suites de chiffrement suivantes à partir du 24 janvier 2024 :

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

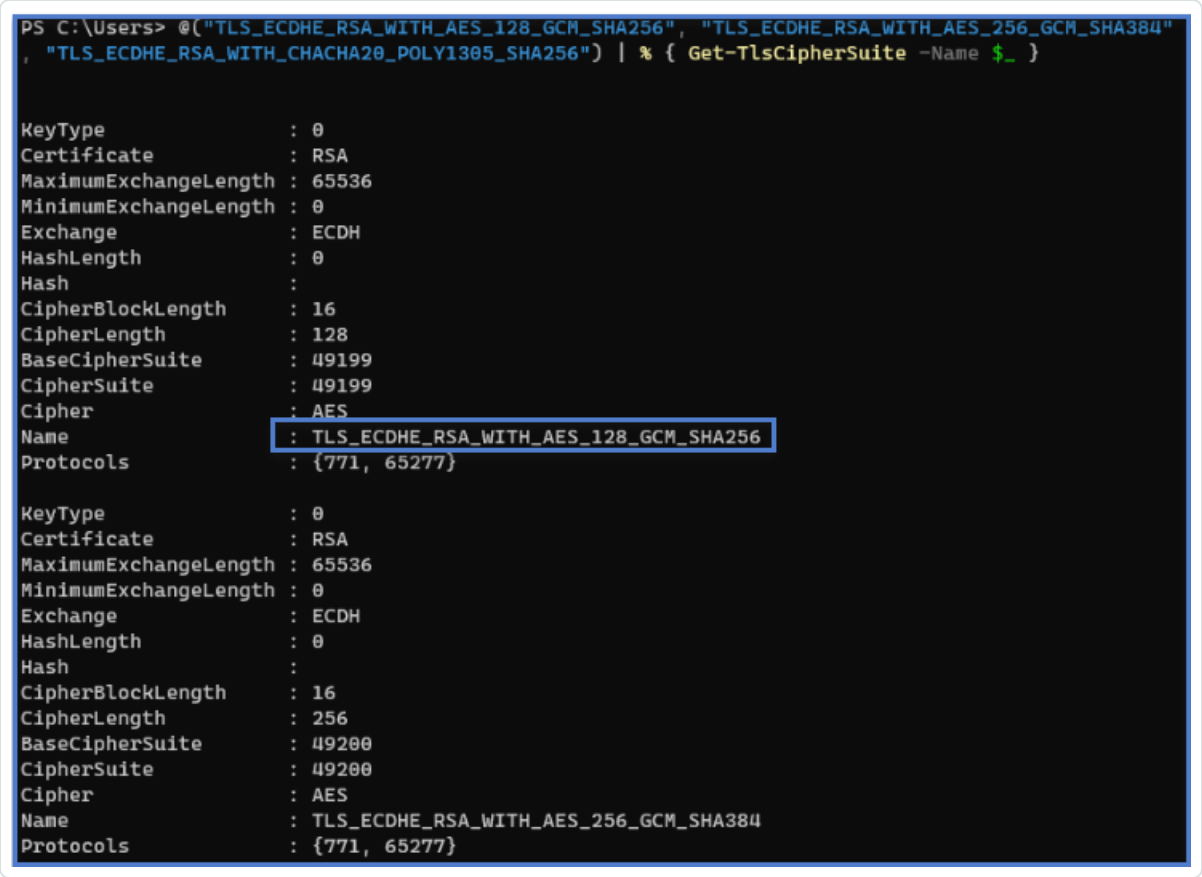
Assurez-vous également que votre configuration Windows correspond aux suites de chiffrement spécifiées pour assurer la compatibilité avec la fonctionnalité Relay.

Pour vérifier les suites de chiffrement :

1. Dans PowerShell, exécutez la commande suivante :

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. Vérifiez la sortie : `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`.



3. Une sortie vide indique qu'aucune des suites de chiffrement requises pour la connexion TLS du Relay n'est activée. Activez au moins une suite de chiffrement.

4. Vérifiez la courbe Elliptic Curve Cryptography (ECC) à partir du serveur du Relay. Cette vérification est obligatoire pour utiliser les suites de chiffrement Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Dans PowerShell, exécutez la commande suivante :

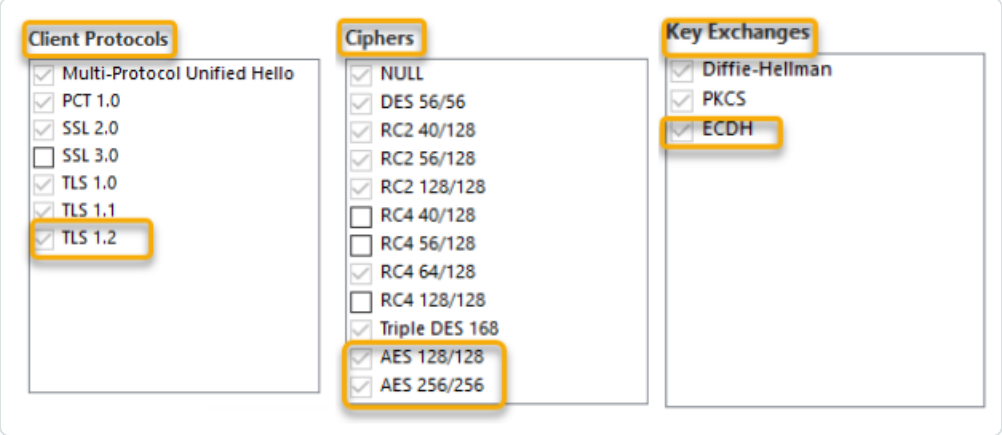
```
Get-TlsEccCurve
```

5. Vérifiez que vous disposez de la courbe **25519**. Si ce n'est pas le cas, activez-la.

```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

Pour vérifier les paramètres de chiffrement Windows :

1. Dans un outil IIS Crypto, vérifiez que les options suivantes sont activées :
   - Protocoles client : **TLS 1.2**
   - Chiffrements : **AES 128/128** et **AES 256/256**
   - Échanges de clés : **ECDH**

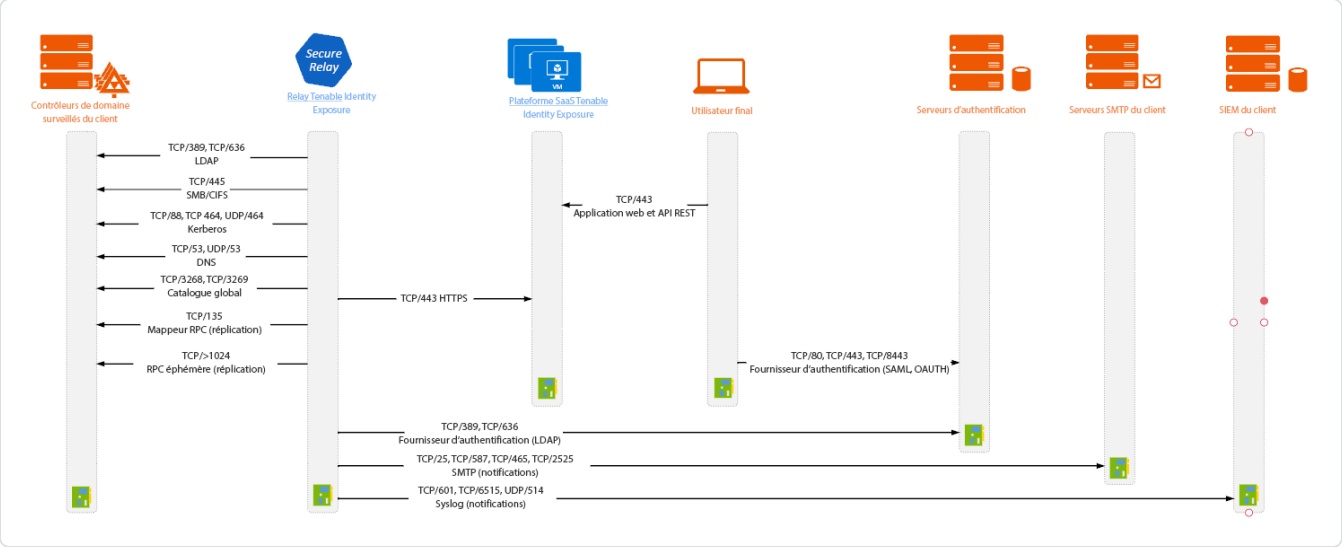


2. Après avoir modifié les paramètres de chiffrement, redémarrez la machine.

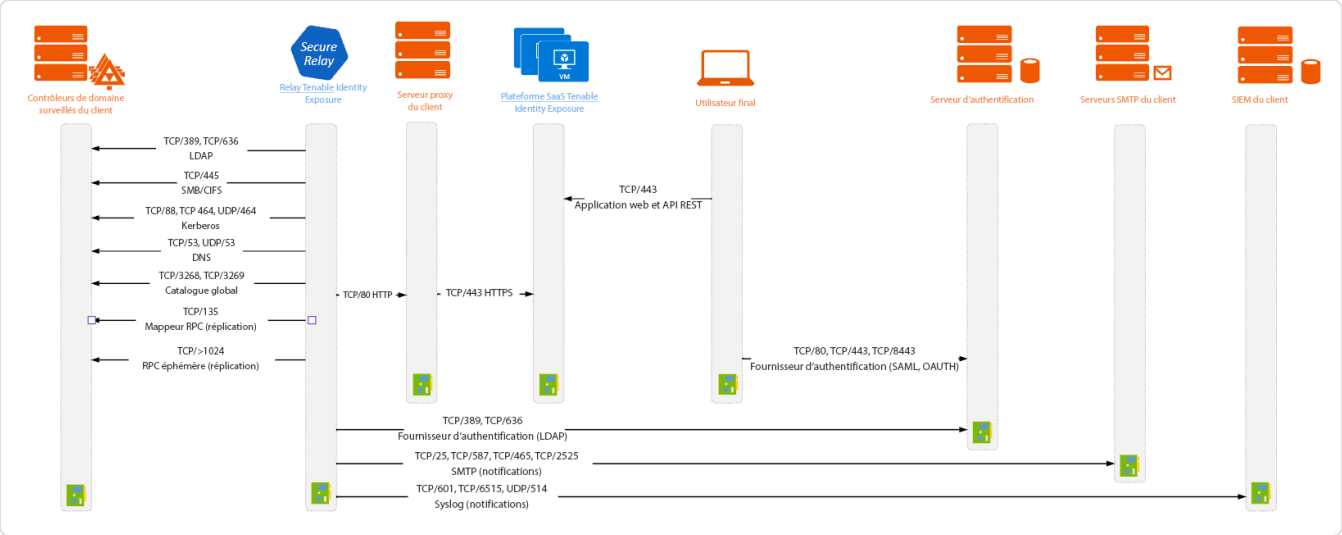
> **Remarque** : la modification des paramètres de chiffrement Windows affecte toutes les applications exécutées sur la machine et utilisant la bibliothèque TLS de Windows, connue sous le nom de « Schannel ». Par conséquent, assurez-vous que tout ajustement que vous effectuez n'entraîne pas d'effets secondaires non souhaités. Vérifiez que les configurations choisies sont compatibles avec les objectifs généraux de durcissement ou les mandats de conformité de l'organisation.

Ports requis

- Pour une configuration classique **sans serveur proxy**, le Relay nécessite les ports suivants :



Pour une configuration **avec un serveur proxy**, le Relay nécessite les ports suivants :



Remarque : les flux réseau fonctionnent de la même manière pour les plateformes sur site et SaaS.

Conditions préalables pour les machines virtuelles

La machine virtuelle (VM) hébergeant le Secure Relay doit présenter les caractéristiques suivantes :

Taille du client	Services Tenable	Instance	Mémoire (par	vCPU (par	Topologie de	Espace disque

	Identity Exposure	requise	instance)	instance)	disque	disponible (par instance)
N'importe quelle taille	• tenable_Relay • tenable_envoy	1	8 Go de RAM	2 vCPU	Partition pour les journaux distincte de la partition système	30 GB

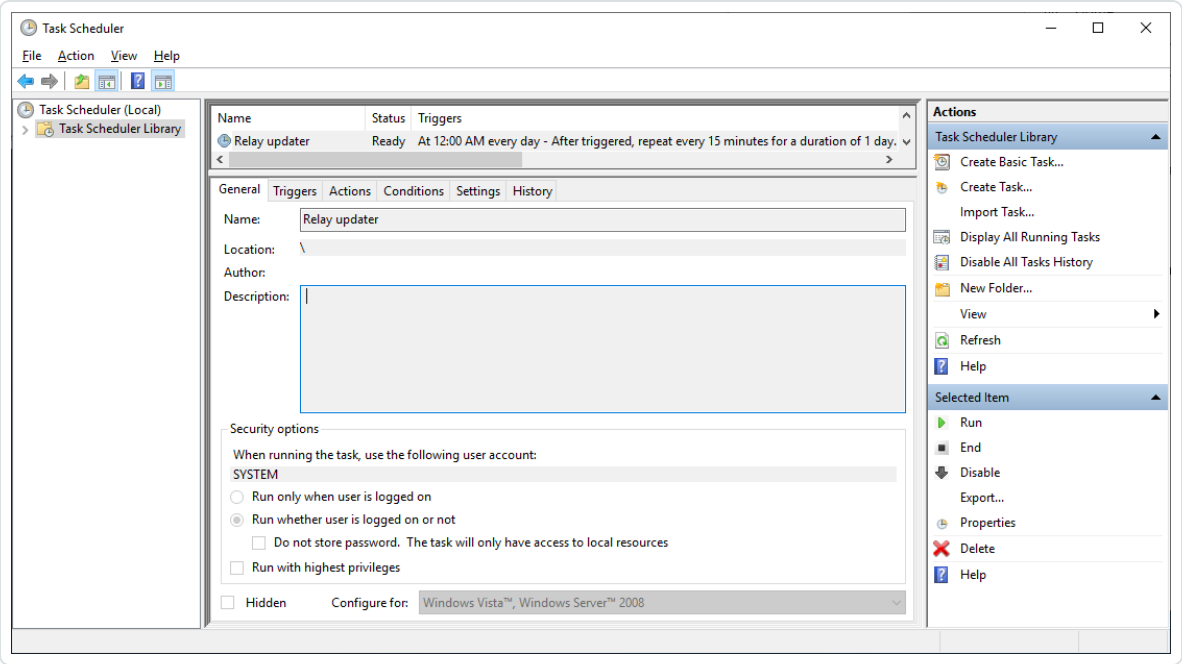
Remarque : si vous installez le Secure Relay et le Directory Listener sur la même machine virtuelle, vous devez combiner leurs exigences de dimensionnement. Voir Resource Sizing.

Conseil : pour l'installation initiale, il est préférable que la VM ne soit pas jointe au domaine, afin d'éviter d'hériter de politiques de GPO existantes susceptibles d'interférer avec le processus d'installation. Une fois l'installation terminée, vous pouvez joindre la VM au domaine.

La VM doit également présenter les caractéristiques suivantes :

- Trafic HTTPS – Supprimez, désactivez, contournez ou ajoutez à la liste d'autorisations tout client capable de diriger le trafic HTTP/HTTPS vers la machine Secure Relay. Cette action bloque l'installation du Secure Relay et interrompt ou ralentit le trafic entrant dans la plateforme Tenable.
- Un système d'exploitation Windows Server 2016+ (pas Linux)
- Une résolution des requêtes DNS orientées Internet et un accès à Internet pour au moins `cloud.tenable.com` et `*.tenable.ad` (TLS 1.2).
- Des privilèges d'administrateur local
- Une configuration EDR, antivirus et GPO :
    - Quantité de processeur suffisante disponible sur la VM – Par exemple, la fonctionnalité temps réel de Windows Defender consomme une quantité considérable de processeur et peut saturer la machine.

- Mises à jour automatiques :
  - Autorisez les appels vers `*.tenable.ad`, afin que la fonctionnalité de mise à jour automatique puisse télécharger un fichier exécutable Relay.
  - Vérifiez qu'aucune stratégie de groupe (GPO) ne bloque la fonction de mise à jour automatique.
  - Ne supprimez ni ne modifiez la tâche planifiée « Relay updater » :



Fichiers et processus autorisés

Pour que le Relay fonctionne correctement, vous devez autoriser certains fichiers et processus auprès des outils de sécurité tiers, en particulier les antivirus et/ou les outils EDR (détection et réponse des terminaux) et XDR (détection et réponse étendues).

> Remarque : adaptez le chemin C:\ au lecteur d'installation de Relay.

Windows
Fichiers
C:\Tenable*

C:\tools*
C:\ProgramData\Tenable*
Processus
nssm.exe --> chemin : C:\tools\nssm.exe
Tenable.Relay.exe --> chemin : C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> chemin : C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe --> chemin : C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> Chemin : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (peut être différent selon la version du système d'exploitation)
Tâches planifiées
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay
Clé de registre
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

Configurer le Relay

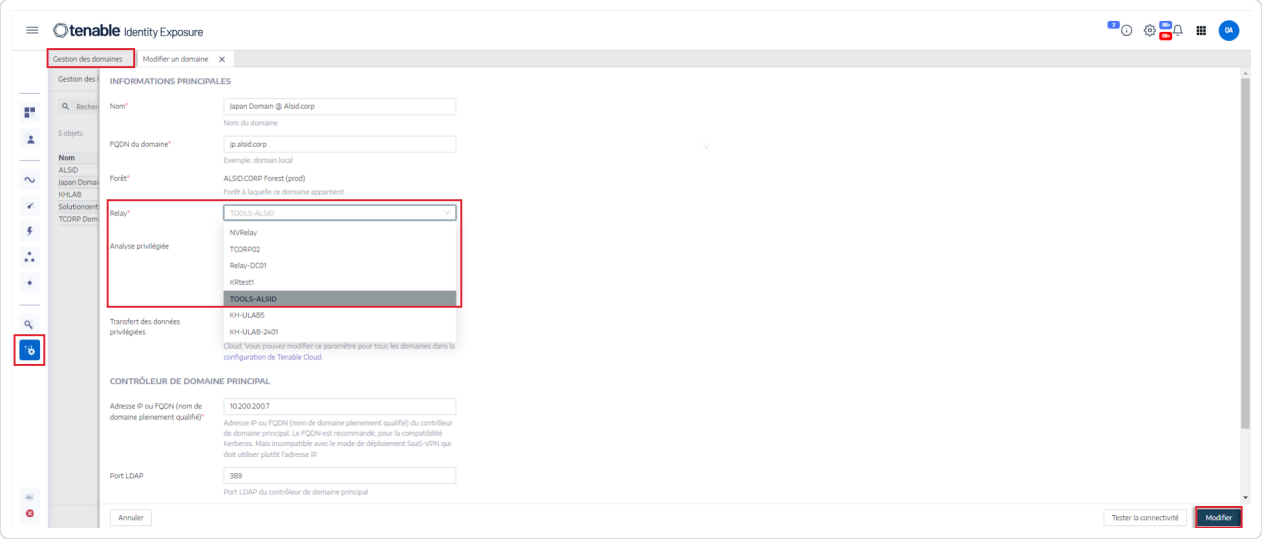
Après les vérifications d'installation et de post-installation, vous devez configurer votre Relay dans Tenable Identity Exposure pour le lier à un domaine et pour configurer des alertes.

- Mappage de domaine : remplacez les paramètres d'application multi-DL ou les variables d'environnement réseau par les paramètres de domaine nécessaires (le nombre de modifications peut varier).

  Pour mapper un domaine à un Secure Relay :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** dans la barre de menu de gauche et sélectionnez l'onglet **Gestion des domaines**.
2. Dans la liste des domaines, sélectionnez un domaine à lier et cliquez sur à la fin de la ligne.

   Le volet **Modifier un domaine** apparaît.
3. Dans la zone **Relay**, cliquez sur la flèche pour afficher la liste déroulante des Relays installés et sélectionnez un Relay à lier au domaine.



   Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour le domaine. SYSVOL et LDAP se synchronisent pour inclure la modification. Le Trail Flow commence à recevoir de nouveaux événements.

- Mappage des alertes :
  - Configuration SMTP : apportez les modifications nécessaires à la Configuration de serveur SMTP.
  - Alertes Syslog : configurez les Alertes Syslog (le nombre de modifications peut varier).
- Mappage LDAP : implémentez l'Authentification à l'aide de LDAP.

Installer le Secure Relay (CLI)

La procédure suivante installe le Secure Relay en utilisant la ligne de commande. Avant de commencer, vérifiez que les conditions préalables sont remplies et que vous disposez de la **clé de liaison requise**, comme décrit dans Secure Relay pour Tenable Identity Exposure .

Pour installer le Secure Relay à l'aide de la CLI :

1. Téléchargez le programme d'installation depuis le portail des téléchargements Tenable Identity Exposure sur votre VM.
2. Dans Powershell, tapez la commande suivante :

   Installation de Secure Relay

   ```
   <PATH>\tenable.ad_SecureRelay_v3.43.0.exe /qn OPTIONS
   ```

   Avec les options suivantes :

   - `APPDIR=<chemin>` (obligatoire) – Chemin d'accès au dossier d'installation du Relay. Choisissez une partition qui n'est pas la partition `système` car le Relay crée des fichiers journaux volumineux.
   - `EDIT_LINKINGKEY=<chaîne>` (obligatoire) – La clé de liaison que vous avez récupérée à partir de votre instance Tenable Identity Exposure.
   - `EDIT_INSTANCENAME=<chaîne>` (facultatif) – Le nom du Relay. Si vous ne définissez pas de nom, Tenable Identity Exposure utilise le nom de la machine. Vous pouvez modifier ce nom dans Tenable Identity Exposure. Ce nom doit être unique.
   - `PROXY_ADDRESS=<IP ou DNS>` (facultatif) – L'adresse proxy à utiliser si votre réseau nécessite un serveur proxy pour atteindre les domaines Tenable. Si vous fournissez une adresse proxy, vous devez également fournir un port proxy.
   - `PROXY_PORT=<nombre>` (facultatif) – Le port proxy à utiliser si votre réseau nécessite un serveur proxy pour atteindre les domaines Tenable. Si vous fournissez une adresse proxy, vous devez également fournir un port proxy.
   - `/L* <dossier>` (facultatif) – Le chemin d'accès où l'installation crée un fichier contenant uniquement les journaux d'installation du Relay.

   Exemple d'installation de Secure Relay avec options

```
.\tenable.ad_SecureRelay_v3.43.0.exe /qn APPDIR=D:\Tenable\Tenable.ad\ EDIT_
LINKINGKEY=eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmxlLmFkIiwidG9rZW4iOiI4NkYwMzMzQS01Mk
I5LTQ4QTctQjMxMS05RDdGRkM5QjkzNTUifQ== EDIT_INSTANCENAME="US Network Area" /L*
C:\Users\Administrator\Desktop\log.txt
```

Remarque : une fois que vous avez appuyé sur Entrée, l'installation commence en arrière-plan. L'invite de la CLI réapparaît immédiatement, mais cela n'indique pas que l'installation est terminée. Si vous avez sélectionné l'option `/L*`, vous pouvez consulter le fichier journal pour confirmer la réussite de l'installation.

Examples

Voici des exemples d'entrées de journal indiquant des installations réussies ou infructueuses :

Installation réussie

```
MSI (s) (D8:EC) [17:39:04:383]: Product: Tenable.ad Secure Relay -- Installation completed
successfully.

MSI (s) (D8:EC) [17:39:04:383]: Windows Installer installed the product. Product Name: Tenable.ad
Secure Relay. Product Version: 3.43.0. Product Language: 1033. Manufacturer: Tenable. Installation
success or error status: 0.

=== Logging stopped: 3/15/2023  17:39:04 ===
```

Échec de l'installation

```
MSI (s) (74:38) [17:18:35:713]: Product: Tenable.ad Secure Relay -- Installation failed.

MSI (s) (74:38) [17:18:35:713]: Windows Installer installed the product. Product Name: Tenable.ad
Secure Relay. Product Version: 3.43.0. Product Language: 1033. Manufacturer: Tenable. Installation
success or error status: 1603.

=== Logging stopped: 3/15/2023  17:18:35 ===
```

Installer le Secure Relay (Agent Tenable)

La procédure suivante installe le Secure Relay en utilisant un Agent Tenable.

Avant de commencer

- Vérifiez que vous avez téléchargé et installé Agent Tenable.

  Remarque : le programme d'installation de Agent Tenable demande une clé d'agent. Cette clé n'est **pas requise** pour la fonctionnalité Secure Relay.

- Veillez à respecter les conditions préalables nécessaires et munissez-vous de la **clé de liaison requise**, comme décrit dans Secure Relay.

Pour installer le Secure Relay à l'aide de Nessus :

1. Sur une machine qui héberge Agent Tenable et fait office de Relay, ouvrez une fenêtre d'invite de commande d'administrateur dans le répertoire Agent Tenable `c:\Program Files\Tenable\Nessus Agent` et saisissez la commande suivante :

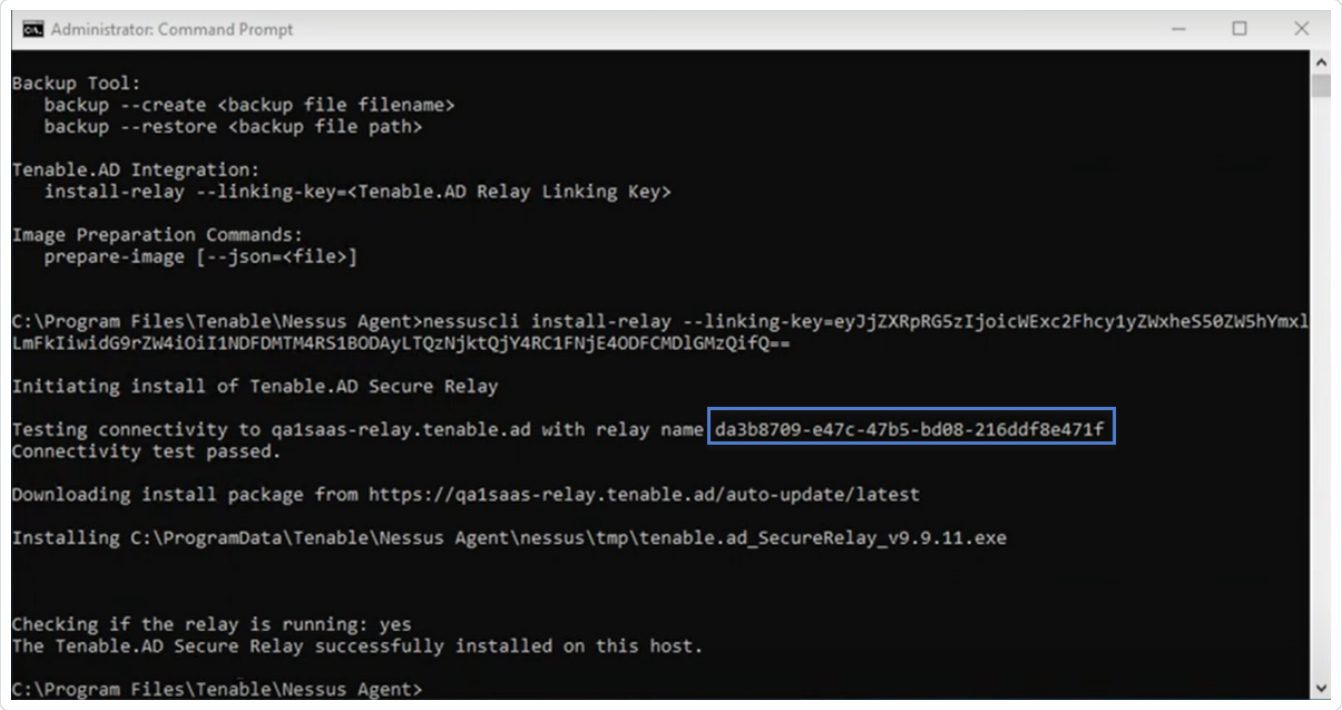
   Installation de Secure Relay

   ```
   nessuscli install-relay --linking-key=<Relay Linking Key> --proxy-host=<Customer Proxy IP or DNS> --proxy-port=<Customer Proxy Port>
   ```

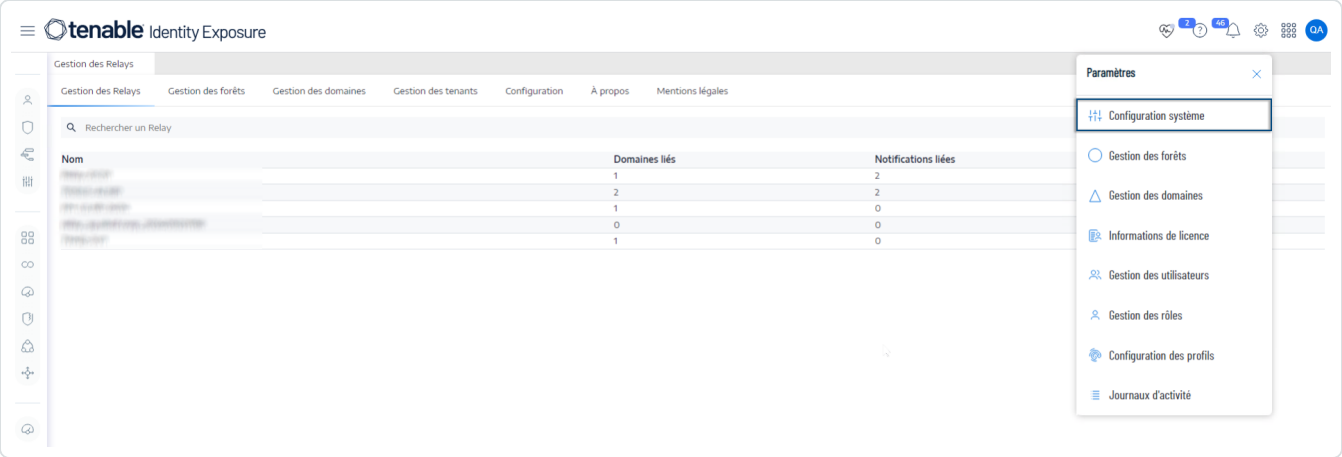
2. Remplacez <Tenable Identity Exposure Relay Linking Key> par la valeur que vous avez copiée précédemment à partir de votre instance Tenable Identity Exposure et fournissez une adresse et un numéro de port de proxy si vous utilisez un serveur proxy.

   L'installation commence. Quelques minutes sont nécessaires pour exécuter les vérifications de connectivité et le processus d'installation.

   Une fois l'installation terminée, un message indique que le Relay s'exécute sur la machine hôte.



3. Dans Tenable Identity Exposure, cliquez sur **Système** > **Gestion des Relays**. Le Relay nouvellement installé apparaît dans la liste des Relays avec l'identifiant affiché dans la fenêtre d'installation.



Résolution des problèmes liés à l'installation de Secure Relay

Suppression du fichier de configuration par un outil EDR ou un antivirus lors de l'installation

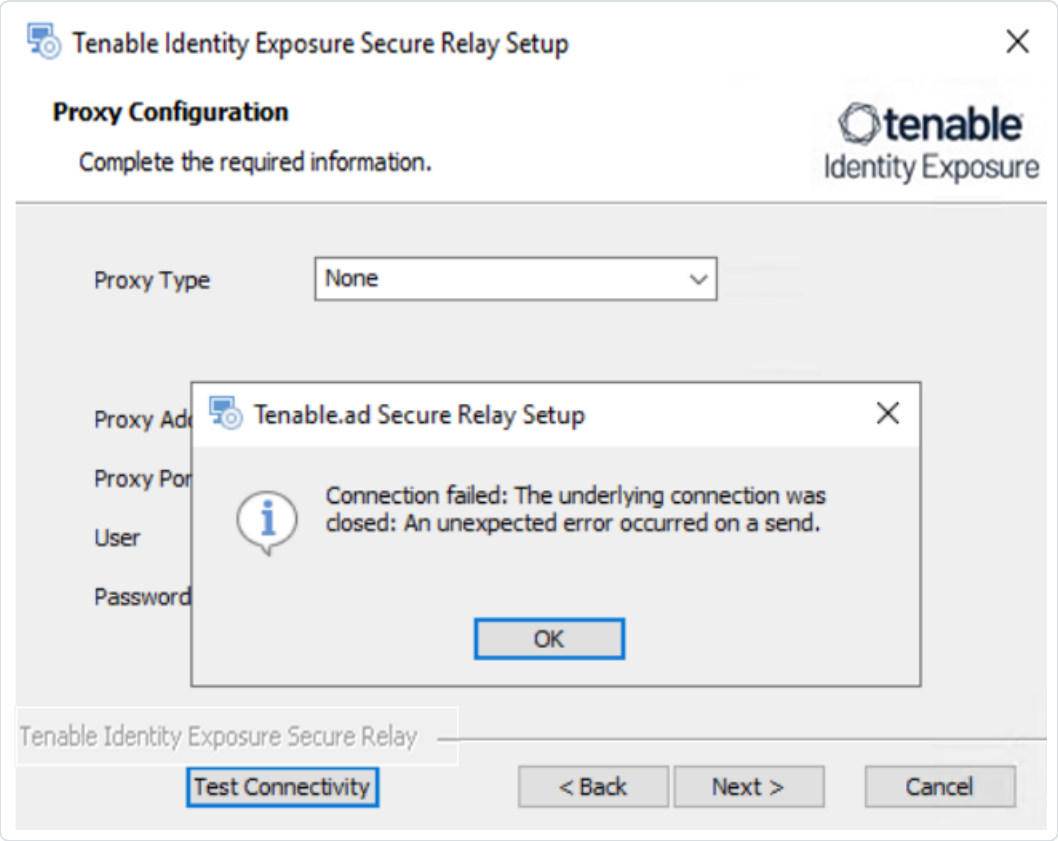
- **Raison** : lors de l'installation de Secure Relay, les logiciels EDR (détection et réponse des terminaux) ou les antivirus peuvent interférer avec le processus en supprimant automatiquement le fichier de configuration `envoy.yaml`. Ce fichier est essentiel pour le bon fonctionnement du Secure Relay. S'il est supprimé, l'installation échoue.
- **Message d'erreur** : si vous pensez que l'échec de l'installation est dû à la suppression du fichier `envoy.yaml` par votre solution EDR ou un logiciel antivirus, vous pouvez le vérifier en consultant le journal des erreurs MSI. Le journal des erreurs MSI est généré dans le dossier TEMP de votre système. Recherchez le message d'erreur suivant : `Erreur : le fichier envoy.yaml est manquant.`

  Si cette erreur apparaît dans votre journal, cela indique que le fichier `envoy.yaml` a été supprimé pendant le processus d'installation, probablement par un logiciel de sécurité.
- **Correction** : pour résoudre ce problème et assurer la réussite de l'installation, suivez ces étapes :

  1. Ajoutez le dossier d'installation ou le fichier de configuration à votre liste blanche :
     - Configurez votre logiciel EDR ou antivirus de manière à exclure le répertoire suivant des scans et des actions de suppression : `[chemin_installation]\Tenable.ad\SecureRelay\`
     - Vous pouvez également ajouter le fichier `[chemin_installation]\Tenable.ad\SecureRelay\envoy.yaml` à la liste blanche si l'exclusion de l'ensemble du dossier n'est pas possible.
  2. Tentez à nouveau l'installation : après avoir ajouté les exclusions nécessaires, relancez l'installation de Secure Relay.

Échec de l'installation de plusieurs Secure Relays et d'un Secure Relay sur un serveur autonome

- **Cause** : pendant la mise à niveau, le programme d'installation ne sélectionne pas la variable d'environnement pour l'adresse IP de l'hôte Ceti et utilise par défaut « 127.0.0.1 ».
- **Message d'erreur** : la connexion a échoué en raison d'une erreur inattendue lors de la transmission.



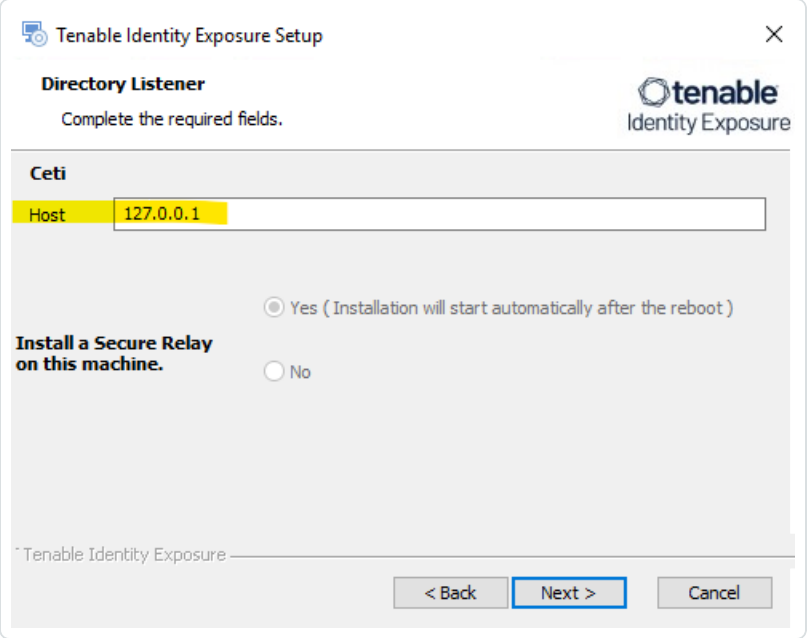
- **Correctif** :

  1. Vérifiez la variable d'environnement « TENABLE_CASSIOPEIA_CETI_Service__Broker__Host » sur le serveur Directory Listener.
  2. Assurez-vous qu'elle est **définie sur l'adresse IP du Security Engine Node**. Si la variable est définie sur la valeur par défaut « 127.0.0.1 », elle entraîne l'échec de l'installation de Secure Relay.
  3. Une fois la variable d'environnement « TENABLE_CASSIOPEIA_CETI_Service__Broker__Host » mise à jour, **redémarrez le service Ceti**.
  4. **Relancez l'installation de Secure Relay**. Sinon, le processus revient en arrière, ne désinstalle pas les services Relay et Envoy et bloque toute autre installation.

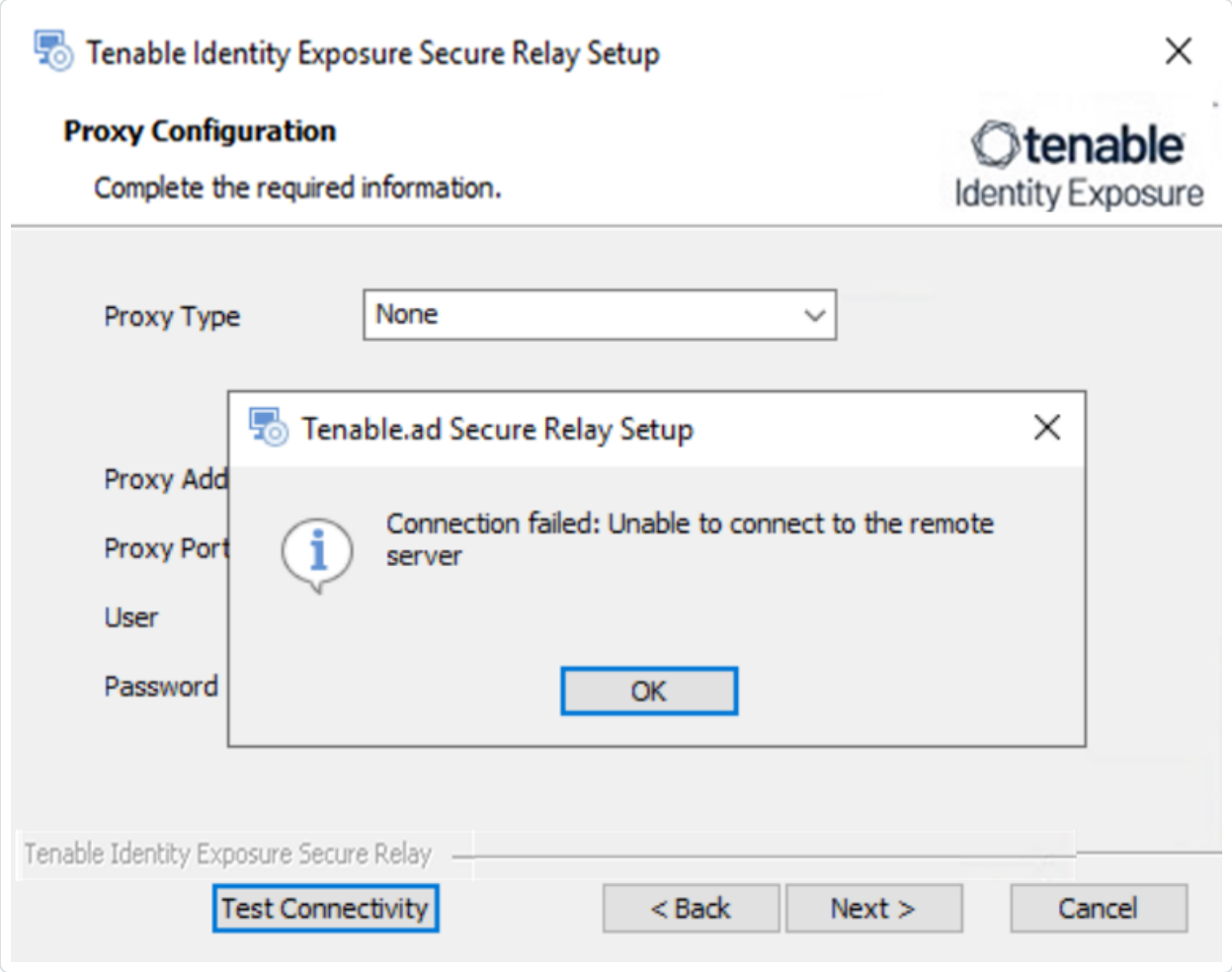
Nom CetiDNS non valide

- **Cause** : l'adresse IP du serveur Ceti n'a pas été définie lors de la mise à niveau ou de l'installation du serveur Security Engine Node. Le programme d'installation est défini par

défaut sur la valeur « 127.0.0.1 » :



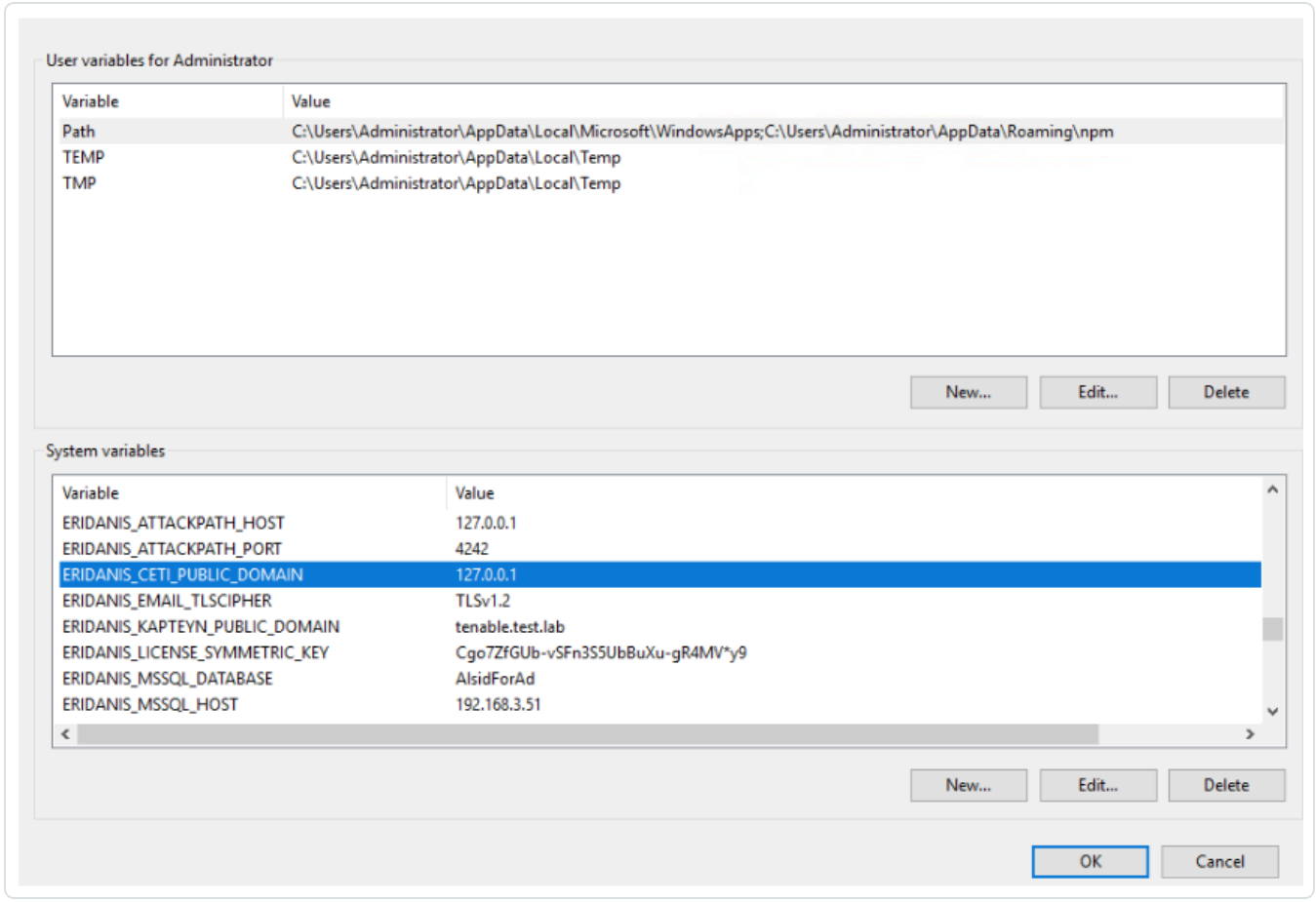
- **Message d'erreur** – Échec de la connexion : impossible de se connecter au serveur distant.



Pour le service « tenable_envoy_server » en pause : identifiez l'application occupant actuellement le port `0.0.0.0:443` à l'aide de la commande PowerShell `netstat -anob | findstr 443`. Si vous trouvez une autre application, supprimez-la ou arrêtez-la pour résoudre le conflit et permettre le bon fonctionnement du service « tenable_envoy_server ».

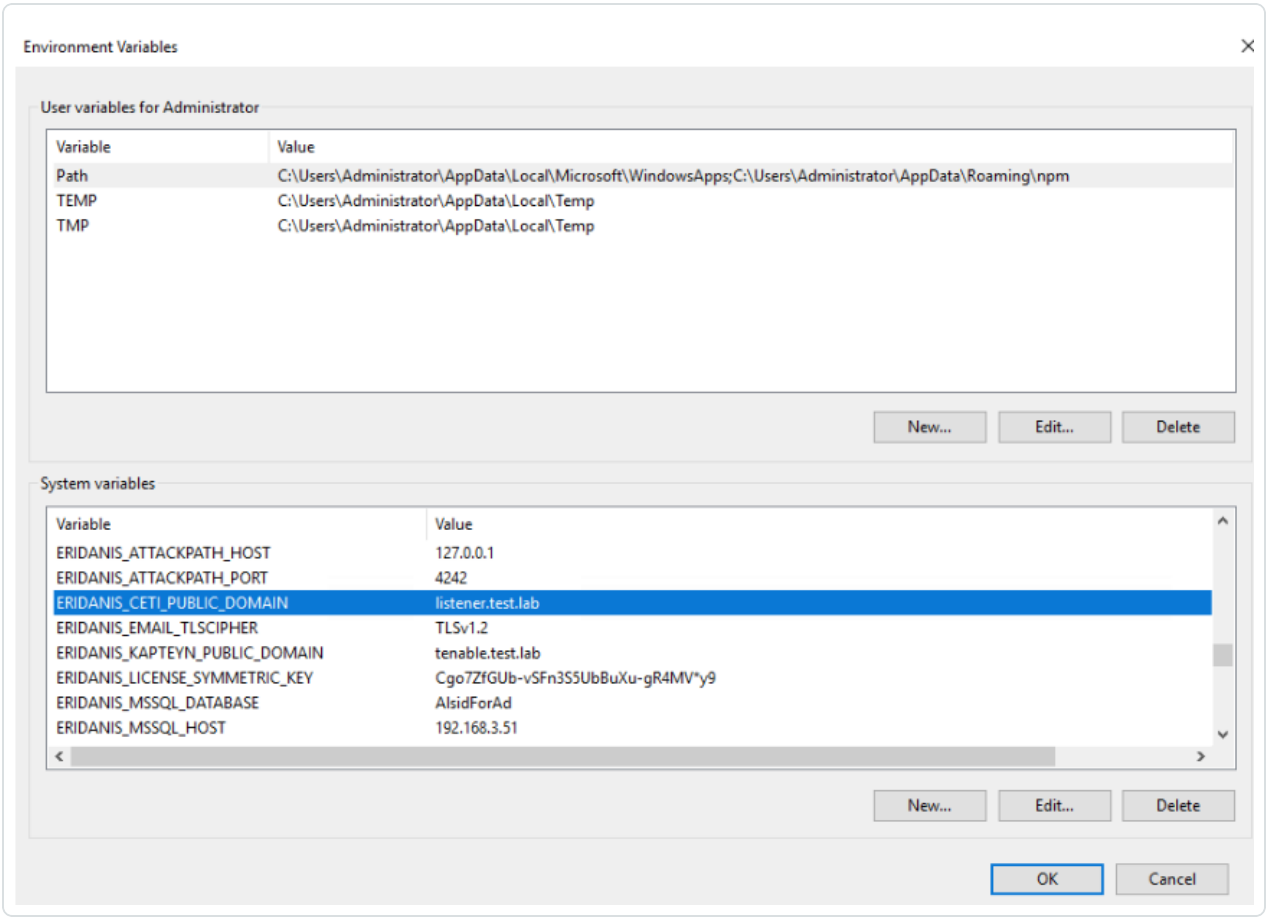
Correctif :

1. Connectez-vous au serveur Security Engine Node.
    - Si vous utilisez une architecture Security Engine Node fractionnée, connectez-vous au serveur qui exécute le service Eridanis.
2. Ouvrez les variables d'environnement et localisez le nom de la variable `ERIDANIS_CETI_PUBLIC_DOMAIN`.

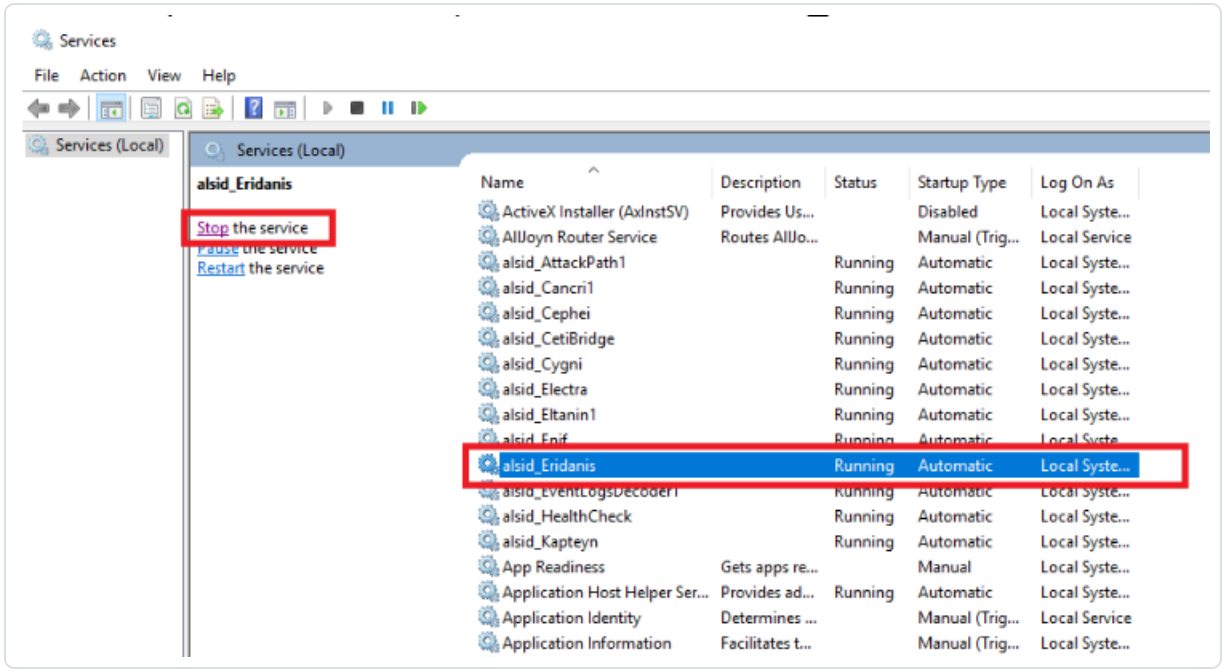


3. Modifiez la valeur de la variable `ERIDANIS_CETI_PUBLIC_DOMAIN` pour insérer l'**adresse IP ou le nom du Directory Listener** :
    - Mettez à jour la valeur d'environnement `ERIDANIS_CETI_PUBLIC_DOMAIN` afin qu'elle corresponde à l'adresse IP ou au nom du Directory Listener. Cette synchronisation permet une communication transparente entre les composants déployés sur des serveurs distincts.
    - La valeur de la variable « ERIDANIS_CETI_PUBLIC_DOMAIN » passe de `127.0.0.1` à

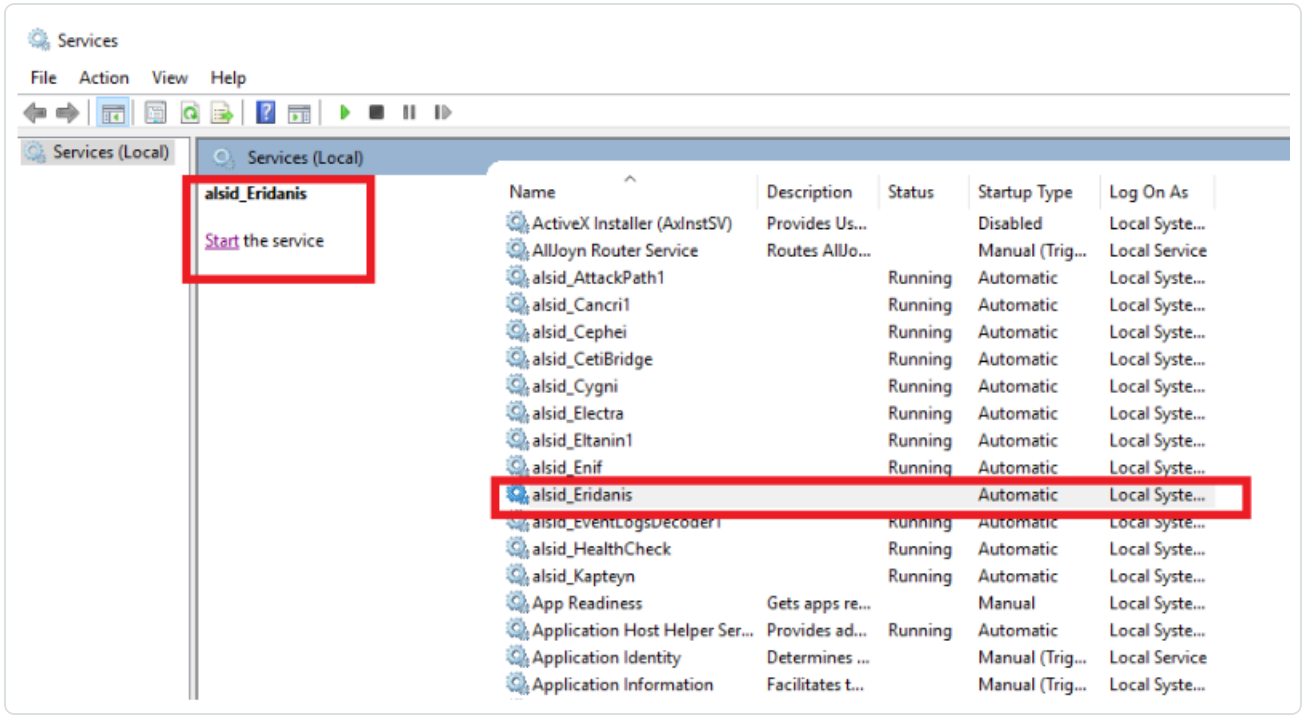
l'adresse IP ou au nom d'hôte du Directory Listener `listener.test.lab`.



4. Ouvrez les services et arrêtez le service `tenable_Eridanis`.



5. Démarrez le service `tenable_Eridanis`.

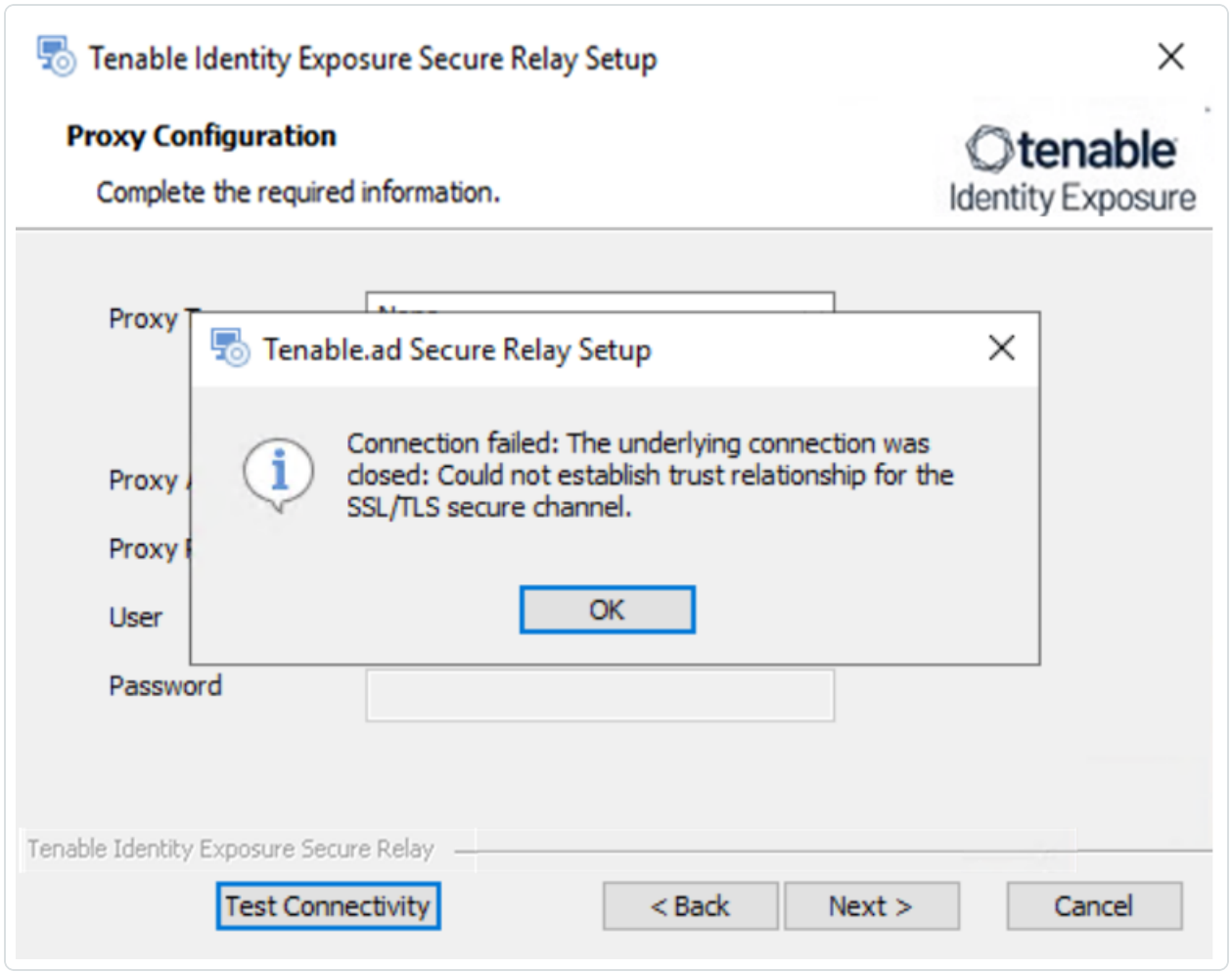


6. Connectez-vous au serveur Secure Relay. Quittez le programme d'installation de Secure Relay s'il est déjà ouvert et relancez l'installation de Secure Relay.

   Attention : veillez à **quitter le programme d'installation** et à démarrer une nouvelle installation. Si vous ne quittez pas le programme d'installation et poursuivez l'installation, le processus d'installation sera interrompu et vous ne pourrez pas continuer (bloqueur).

Pas de « relation d'approbation » pour la connexion sécurisée SSL/TLS

- **Cause** : le programme d'installation ne trouve pas les certificats CA sur le serveur local.
- **Message d'erreur** – Échec de la connexion : la connexion sous-jacente a été fermée : une relation d'approbation n'a pas pu être établie pour le canal sécurisé SSL/TLS.



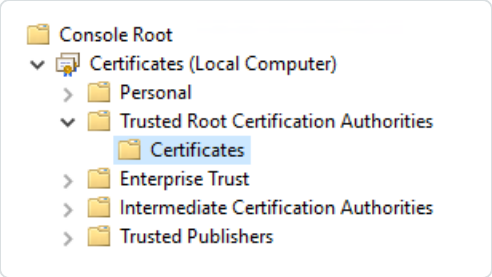
- **Correctif** :

1. Accédez au système source (serveur Directory Listener) ou au référentiel où les certificats CA de confiance sont stockés et localisez ces derniers, généralement dans des répertoires tels que :

    - Emplacement du certificat auto-signé par défaut : `“installation_drive”:\Tenable\Tenable.ad\DefaultPKI\Certificates\ca`
    - Emplacement du certificat personnalisé : `“installation_drive”:\Tenable\Tenable.ad\Certificates`

2. Copiez les fichiers de certificat CA de confiance du système source (serveur Directory Listener) vers le serveur local (serveur Secure Relay).

3. Importez les certificats dans le magasin de certificats de confiance du serveur Secure Relay.

4. Une fois l'importation réussie, **quittez le programme d'installation de Secure Relay et relancez l'installation**.

    Attention : veillez à **quitter le programme d'installation** et à démarrer une nouvelle installation. Si vous ne quittez pas le programme d'installation et poursuivez l'installation, le processus d'installation sera interrompu et vous ne pourrez pas continuer (bloqueur).

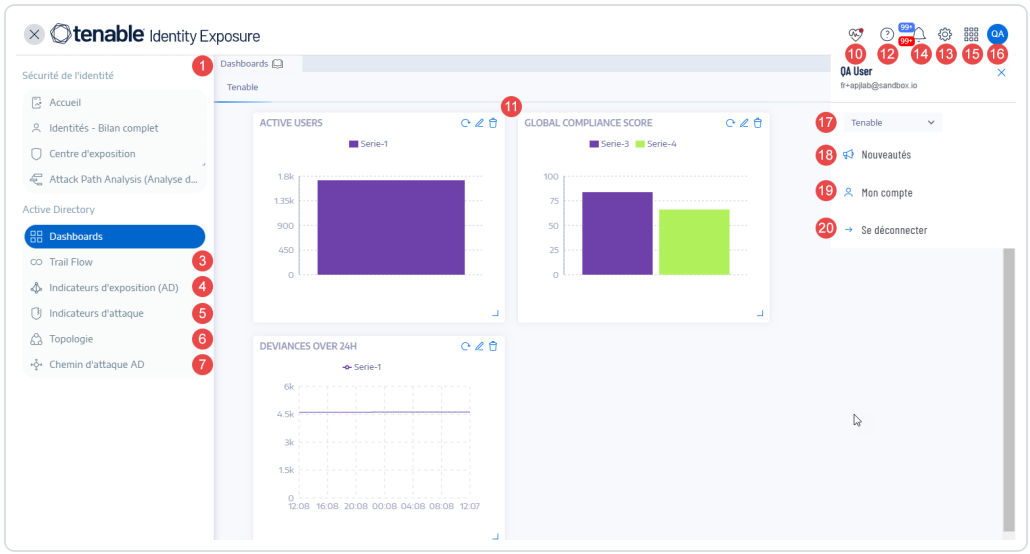
Commencer à utiliser Tenable Identity Exposure

Une fois Tenable Identity Exposure déployé, cette section vous guide à travers les étapes clés pour commencer à utiliser Tenable Identity Exposure efficacement.

Chaque section contient des liens vers des descriptions et des instructions plus détaillées pour la tâche associée.

1. ## Se connecter et parcourir l'interface utilisateur

   - Connectez-vous au portail Se connecter à Tenable Identity Exposure. La page d'accueil, représentée ci-dessous, apparaît.
   - Votre identifiant initial est `hello@tenable.ad` et le mot de passe `Hello@tenable.ad123!.`
   - Développez ou réduisez la barre de navigation latérale :
     - Pour la développer : cliquez sur le menu ☰ dans l'angle supérieur gauche de la fenêtre.
     - Pour la réduire : cliquez sur le signe ✕ dans l'angle supérieur gauche de la fenêtre.



   - Accédez au Portail utilisateur Tenable Identity Exposure.

2. ## Installer le Secure Relay

   Un Secure Relay transfère en toute sécurité les données Active Directory de votre réseau vers la plateforme Tenable Identity Exposure SaaS en utilisant le chiffrement TLS au lieu d'une connexion VPN. Plusieurs Secure Relays sont possibles en fonction de vos besoins.

   Conditions préalables :

- Accès administrateur à un serveur Windows pour la machine virtuelle (VM) Secure Relay
- Dernier programme d'installation de Secure Relay téléchargé depuis le portail des téléchargements Tenable Identity Exposure
- Une clé de liaison à usage unique du portail Tenable Identity Exposure contenant l'adresse réseau et le jeton d'authentification

Pour plus de détails sur les conditions préalables, voir Secure Relay pour Tenable Identity Exposure

Récupérer la clé de liaison :

1. Connectez-vous au portail web Tenable Identity Exposure avec un compte administrateur.
2. Cliquez sur **Système** > **Configuration** > onglet **Relay**.
3. Cliquez sur l'icône **Copier dans le presse-papiers** à côté de la clé de liaison.

Installer le Secure Relay :

1. Sur votre VM de serveur Windows, effectuez un clic droit sur le fichier d'installation et sélectionnez **Exécuter en tant qu'administrateur**.
2. Dans l'assistant d'installation, cliquez sur **Next** (Suivant) sur l'écran de bienvenue.
3. Dans la fenêtre **Custom Setup** (Configuration personnalisée), cliquez sur **Browse** (Parcourir) pour modifier la partition de disque si nécessaire, puis sur **Next** (Suivant).
4. Dans la fenêtre **Linking Key** (Clé de liaison) :
    - Collez la clé de liaison copiée à partir du portail.
    - Donnez un nom à votre Secure Relay.
    - Cliquez sur **Test Connectivity** (Tester la connectivité).

5. Si le test réussit (icône verte), cliquez sur **Next** (Suivant). Si ce n'est pas le cas, cliquez sur **Back** (Retour) pour corriger les erreurs.
6. Dans la fenêtre **Ready to Install** (Prêt pour l'installation), cliquez sur **Install** (Installer).
7. Une fois l'installation réussie, cliquez sur **Finish** (Terminé).

   Pour la procédure détaillée, voir Secure Relay pour Tenable Identity Exposure .

Vérifiez l'installation du Relay sur le portail :

1. Revenez au portail Tenable Identity Exposure.
2. Cliquez sur **Système** > onglet **Gestion des Relays**.

   Le Relay nouvellement installé apparaît dans la liste des Relays.

Configurer le Relay :

Lorsque vous ajoutez des domaines à surveiller, une nouvelle option apparaît pour vous permettre de sélectionner le Secure Relay en charge de ce domaine. Pour la procédure complète, voir Configurer le Relay.

Mises à jour automatiques :

Tenable Identity Exposure recherche automatiquement et installe régulièrement les mises à jour Secure Relay (nécessite un accès HTTPS). Une icône de la barre réseau indique quand des mises à jour sont effectuées. Après la mise à jour, les services Tenable Identity Exposure redémarrent et la collecte de données reprend.

3. **Activer les indicateurs d'exposition (IoE) pour un domaine Active Directory**

Avant de configurer les indicateurs d'exposition, vous devez posséder ou créer un compte de service Active Directory avec les autorisations appropriées. Bien que Tenable Identity Exposure ne nécessite pas de privilèges administrateur pour la surveillance de la sécurité, certains conteneurs exigent une configuration manuelle pour autoriser l'accès en lecture pour l'utilisateur du compte de service.

> Pour des informations complètes, voir Accès aux objets ou conteneurs AD.

1. Connectez-vous au portail web Tenable Identity Exposure avec des identifiants administrateur tels que le compte par défaut « hello@tenable.ad ».
2. Cliquez sur l'icône de menu dans l'angle supérieur gauche pour développer le panneau de navigation, puis cliquez sur **Système** dans le panneau de gauche.

Ajouter une forêt :

1. Dans l'onglet **Gestion des forêts**, cliquez sur **Ajouter une forêt**.
2. Indiquez un nom d'affichage pour la forêt (par exemple, Tenable).
3. Saisissez l'identifiant et le mot de passe du compte de service pour vous connecter à tous les domaines de cette forêt.
4. Cliquez sur **Ajouter**.

   Pour des informations complètes, voir Forêts.

Ajouter un domaine :

1. Cliquez sur **Ajouter un domaine**.
2. Indiquez un nom d'affichage pour le domaine à surveiller (par exemple, HQ).
3. Saisissez le nom de domaine complet (par exemple, sky.net).
4. Sélectionnez la forêt correspondante dans la liste déroulante.
5. Si vous utilisez SaaS avec Secure Relay, sélectionnez le relais destiné à gérer ce domaine.
6. Activez le curseur « Analyse privilégiée » si le compte dispose des privilèges requis.
7. Si vous activez la fonctionnalité **Analyse privilégiée**, activez également l'option **Transfert des données privilégiées** pour Tenable Cloud.
8. Fournissez des détails pour le contrôleur de domaine avec le rôle FSMO d'émulateur de contrôleur de domaine principal :

- Adresse IP ou nom d'hôte
- Pour les ports LDAP, de catalogue global et SMB, conservez les valeurs par défaut pré-remplies

9. Cliquez sur **Tester la connectivité** en bas de l'écran.
10. En cas de succès, cliquez sur **Ajouter**.

    Dans la vue Gestion des domaines, vous verrez des colonnes pour les statuts d'initialisation de l'analyseur LDAP, d'initialisation de l'analyseur SISFul et de configuration du honey account (compte leurre) affichant une icône de chargement circulaire jusqu'à ce que le scan initial soit terminé.

    Pour des informations complètes, voir Domaines.

Initialisation de la surveillance :

1. Basculez vers la vue **Trail Flow**. Après quelques minutes, les données commencent à affluer une fois l'analyse lancée.
2. Revenez à **Système** > **Gestion des domaines**.
3. Attendez que les icônes vertes indiquant l'achèvement de l'initialisation de l'analyseur LDAP et de l'analyseur SYSVOL apparaissent.

   Vous avez maintenant activé la surveillance des indicateurs d'exposition pour ce domaine. Sur le portail web, les notifications apparaissent après quelques minutes/heures selon la taille de l'environnement.

Examiner les données d'exposition :

1. Cliquez sur **Indicateurs d'exposition** dans le menu de gauche pour voir tous les indicateurs déclenchés pour le domaine ajouté.
2. Cliquez sur un indicateur pour afficher les détails d'un objet déviant à l'origine d'une non-conformité.
3. Fermez les détails et accédez à **Dashboards** pour voir les métriques de l'environnement.

4. ### Déployer les indicateurs d'attaque (IoA) pour un domaine

Pour déployer les IoA, vous devez d'abord effectuer les trois configurations décrites ci-dessous :

1. Le script IoA est obligatoire pour tous les scénarios d'attaque.
2. Le honey account (compte leurre) configuré pour détecter des attaques spécifiques telles que l'attaque Kerberoasting.
3. Installation de Sysmon sur tous les contrôleurs de domaine du domaine surveillé pour détecter les attaques telles que le dumping des identifiants système.

Tenable Identity Exposure fournit le script IoA, sa ligne de commande et la ligne de commande de configuration du honey account (compte leurre). Cependant, vous devez remplir ces conditions préalables directement sur les contrôleurs de domaine ou sur une machine administrateur disposant des droits appropriés.

> Pour des informations complètes, voir Déploiement des indicateurs d'attaque.

Configurer les scénarios d'attaque :

1. Connectez-vous au portail web Tenable Identity Exposure à l'aide d'identifiants administrateur (par exemple, hello@tenable.ad).
2. Accédez à **Système** > **Configuration** > **Indicateurs d'attaque**.
3. Sélectionnez les scénarios d'attaque que vous souhaitez activer pour votre environnement.
4. Cochez la case sous le nom de domaine pour activer tous les scénarios d'attaque disponibles.
5. Cliquez sur **Enregistrer** dans l'angle inférieur droit.
6. Cliquez sur **Voir la procédure** en haut.

   Une fenêtre montrant la procédure de déploiement du moteur IoA apparaît.

7. Utilisez le curseur pour activer ou désactiver la fonction de mises à jour automatiques.
8. Cliquez sur le premier bouton **Télécharger** pour télécharger le fichier PS1.
9. Cliquez sur le deuxième bouton **Télécharger** pour télécharger le fichier JSON.
10. Notez l'emplacement où vous avez téléchargé les fichiers d'installation.
11. Localisez le champ étiqueté **Exécuter les commandes PowerShell suivantes**.
12. Copiez le contenu du champ de texte et collez-le dans un fichier texte.
13. Copiez les fichiers PS1 et JSON dans un contrôleur de domaine ou un serveur d'administrateur disposant des droits appropriés.
14. Démarrez le module Active Directory pour Windows PowerShell en tant qu'administrateur et accédez au dossier hébergeant les fichiers.
15. Collez la commande copiée à partir du portail web Tenable Identity Exposure et appuyez sur Entrée.
16. Ouvrez la console de gestion des stratégies de groupe et trouvez la GPO nommée « Tenable.ad » liée à l'OU du contrôleur de domaine.

Pour la procédure détaillée, voir Installer des indicateurs d'attaque.

Configurer le honey account (compte leurre) :

1. Revenez au portail web Tenable Identity Exposure.
2. Accédez à **Système** > onglet **Gestion des domaines**.
3. Cliquez sur l'icône **+** sous **Statut de configuration du Honey Account** à droite de votre domaine (disponible une fois que les deux autres statuts sont verts).
4. Dans la zone de recherche **Nom**, saisissez le nom du compte à utiliser comme honey pot (compte leurre).
5. Sélectionnez le nom distinctif de l'objet dans la liste déroulante.

6. Copiez le contenu du champ de texte de la ligne de commande et collez-le dans un fichier texte.
7. Revenez sur le serveur sur lequel vous avez exécuté le script IoA.
8. Ouvrez ou démarrez une ligne de commande PowerShell en tant qu'administrateur.
9. Collez la commande copiée à partir du portail web Tenable Identity Exposure et appuyez sur Entrée.
10. Vérifiez que la ligne de commande s'est exécutée correctement.
11. Revenez au portail web Tenable Identity Exposure et cliquez sur le bouton **Ajouter** en bas.

    Après quelques secondes, le statut de configuration du honey account (compte leurre) doit afficher un point vert.

> Pour la procédure détaillée, voir Honey Accounts.

Installer Sysmon :

Le portail web Tenable Identity Exposure ne fournit pas de déploiement automatique pour Sysmon. Voir Programme d'installation de Microsoft Sysmon pour le fichier de configuration de Sysmon requis. Vous pouvez installer Sysmon manuellement comme indiqué dans la documentation ou par GPO.

> Pour la procédure détaillée, voir Programme d'installation de Microsoft Sysmon.

5. #### Configurer Microsoft Entra ID pour Tenable Identity Exposure :

Tenable Identity Exposure prend également en charge Microsoft Entra ID conjointement avec Active Directory avec des IoE spécifiques pour les identités Entra ID.

> Pour des informations complètes, voir Prise en charge de Microsoft Entra ID.

Créer l'application Entra ID :

1. Connectez-vous au portail d'administration Azure à l'adresse portal.azure.com avec les identifiants appropriés.
2. Cliquez sur la tuile **Azure Active Directory**, puis sur **Inscriptions d'application** dans le menu de gauche.
3. Cliquez sur **Nouvelle inscription** et indiquez un nom d'application (par exemple, « Application Identity Exposure »).
4. Cliquez sur **S'inscrire** en bas de l'écran.
5. Sur la page Vue d'ensemble de l'application, notez l'« ID de l'application (client) » et l'« ID de l'annuaire (locataire) ».
6. Cliquez sur **Certificats et secrets** dans le menu de gauche.
7. Cliquez sur **Nouvelle clé secrète client**, fournissez une description et définissez l'expiration par politique.
8. Cliquez sur **Ajouter**, puis enregistrez la valeur secrète affichée de manière sécurisée.
9. Cliquez sur **Autorisations d'API** et **Ajouter une autorisation**.
10. Sélectionnez **Microsoft Graph**, puis **Autorisations de l'application**.
11. Ajoutez les autorisations suivantes : `Audit Log.Read.All`, `Directory.Read.All`, `IdentityProvider.Read.All`, `Policy.Read.All`, lReports.Read.All, `RoleManagement.Read.All`, `UserAuthenticationMethod.Read.All`.
12. Cliquez sur **Ajouter des autorisations** et **Accorder le consentement administrateur**.

Configurer Tenable Vulnerability Management

1. Connectez-vous au portail web Tenable Vulnerability Management avec le compte approprié.
2. Cliquez sur **Menu** > **Paramètres** > **Informations d'identification**.
3. Cliquez sur **Créer des informations d'authentification** et sélectionnez le type **Microsoft Azure**.

4. Saisissez un nom et une description, puis collez l'ID de tenant, l'ID d'application et le secret de client.
5. Cliquez sur **Créer**.
6. Cliquez sur **Menu** > **Paramètres** > **Mon compte** > **Clés API**.
7. Cliquez sur **Générer**, passez en revue l'avertissement et cliquez sur **Continuer**.
8. Copiez les valeurs Clé d'accès et Clé secrète.

Configurer Tenable Identity Exposure :

1. Connectez-vous avec un compte d'administrateur global.
2. Cliquez sur **Menu** > **Système** > **Configuration** > **Tenable Cloud**.
3. Activez l'option **Activer la prise en charge de Microsoft Entra ID** à l'aide du curseur.
4. Saisissez la clé d'accès et la clé secrète générées précédemment.
5. Cliquez sur la coche pour soumettre les clés API.
6. Cliquez sur l'onglet **Gestion des tenants**, puis sur **Ajouter un tenant**.
7. Donnez un nom au tenant Azure AD.
8. Sélectionnez l'identifiant Azure créé précédemment.
9. Cliquez sur **Ajouter**.

Surveiller et consulter les détections :

1. Tenable Identity Exposure scanne le tenant. Pour voir la date et l'heure du prochain scan, passez le pointeur de la souris sur **Statut du scan**.
2. Lorsque le premier scan est terminé, une icône verte apparaît dans la colonne **Statut du scan**.
3. Cliquez sur **Indicateurs d'exposition** dans le menu de gauche.
4. Utilisez les onglets pour filtrer les indicateurs AD et Azure AD.

5. Activez **Afficher tous les indicateurs** pour voir tous les indicateurs disponibles.
6. Trois onglets fournissent des **détails sur les indicateurs**, des **détections de tenant** et des **recommandations**.
7. Examinez les risques d'exposition potentiels et les conseils de remédiation.

6. ### Configurer et utiliser les IoE dans votre environnement

Tenable Identity Exposure utilise des indicateurs d'exposition pour mesurer la maturité de la sécurité de votre infrastructure Active Directory et attribuer des niveaux de sévérité au flux d'événements qu'il surveille et analyse.

> Pour des informations complètes sur les IoE, voir Indicateurs d'exposition.

Accéder aux IoE :

1. Connectez-vous à Tenable Identity Exposure.
2. Cliquez sur l'icône dans l'angle supérieur gauche pour développer le panneau.
3. Cliquez sur **Indicateurs d'exposition** sur le côté gauche pour voir les IoE.

   La vue par défaut affiche les éléments de configuration de votre environnement qui sont potentiellement vulnérables, classés par sévérité : critique, élevée, moyenne et faible.

Afficher tous les IoE :

- Cliquez sur le curseur à droite de l'option **Afficher tous les indicateurs**.
  - Vous pouvez voir tous les IoE disponibles dans votre instance Tenable Identity Exposure. Les éléments n'affichant aucun domaine sont ceux où cette exposition n'est pas présente.
  - À droite de l'option **Afficher tous les indicateurs**, vous pouvez voir **Domaine**. Si votre environnement contient plusieurs domaines, cliquez dessus et sélectionnez les domaines à afficher.

Rechercher des IoE :

- Cliquez sur **Rechercher un indicateur** et saisissez un mot-clé, tel que « mot de passe ».

  Tous les IoE liés aux mots de passe apparaissent.

Examiner les détails des IoE :

- Pour afficher plus d'informations sur un indicateur, cliquez dessus.
  - La vue détaillée commence par un résumé de l'exposition particulière.
  - Elle répertorie ensuite les documents connexes et les outils d'attaque connus qui peuvent exposer cet élément particulier.
- À droite, vous pouvez voir les **Domaines impactés**.
  - Cliquez sur l'onglet **Détails de la vulnérabilité** pour lire des informations supplémentaires sur les vérifications effectuées pour cet IoE.
  - Cliquez sur l'onglet **Objets déviants** pour voir la liste des objets et des motifs qui ont déclenché l'exposition.
  - Si vous développez un objet de la liste, vous pouvez obtenir plus de détails sur l'origine de la déviance.

Créer des requêtes :

1. Pour créer une requête, cliquez sur **Saisir une expression** et saisissez une requête booléenne pour un élément. Vous pouvez également cliquer sur l'icône de filtre à gauche pour générer une requête.
2. Définissez les dates de début et de fin, choisissez des domaines et recherchez les éléments ignorés en cliquant sur le curseur **Ignorer**.

   > Pour les procédures complètes, voir Rechercher des objets déviants.

Ignorer/Exporter les objets déviants :

- Vous pouvez masquer des objets de la liste en les ignorant.
    - Sélectionnez un ou plusieurs objets, puis cliquez sur **Sélectionner une action** en bas de la page.
    - Sélectionnez **Ignorer les objets sélectionnés** et cliquez sur **OK**.
    - Choisissez la date jusqu'à laquelle vous souhaitez ignorer les objets sélectionnés.
    - Vous pouvez cesser d'ignorer les objets de la même manière à l'aide de l'option **Ne plus ignorer les objets sélectionnés**.
- Pour exporter la liste de tous les objets déviants de cet indicateur dans un fichier CSV, cliquez sur le bouton **Tout exporter**.

> Pour les procédures complètes, voir Objets déviants.

Recommandations en matière de remédiation :

- Cliquez sur l'onglet **Recommandations** pour voir des recommandations sur la façon de remédier à cet indicateur.

> Voir aussi Remédier à des déviances liées à des indicateurs d'exposition pour les cas d'utilisation de la remédiation.

7. **Suivre les changements de configuration dans AD à l'aide du Trail Flow**

Le Trail Flow affiche la surveillance et l'analyse en temps réel des événements qui affectent vos infrastructures AD. Il permet d'identifier les vulnérabilités critiques et les mesures correctives recommandées.

> Pour des informations complètes, voir Trail Flow et Cas d'utilisation du Trail Flow.

Accéder au Trail Flow :

1. Connectez-vous à Tenable Identity Exposure.
2. Cliquez sur l'icône dans l'angle supérieur gauche pour développer la barre de navigation.
3. Cliquez sur **Trail Flow**.

Parcourir la page Trail Flow :

La page Trail Flow apparaît et affiche une liste d'événements, dont le type de source, le chemin de l'objet, le domaine et la date.

1. Cliquez dans la zone de la date dans l'angle supérieur droit pour indiquer les dates recherchées.
2. Cliquez sur **Domaine** pour modifier les serveurs ou les forêts Active Directory.
3. Cliquez sur le bouton pause dans le coin supérieur droit pour suspendre ou redémarrer la capture de Trail Flow.

Créer des requêtes :

Vous pouvez créer des requêtes pour votre recherche de deux manières : manuellement ou à l'aide de l'assistant.

- Pour filtrer manuellement les événements, saisissez une expression dans la zone de recherche afin d'affiner les résultats à l'aide des opérateurs booléens.

  > Pour des informations complètes, voir Recherche manuelle dans Trail Flow.

- Pour utiliser l'assistant de recherche :

  1. Cliquez sur l'icône de la baguette magique à gauche.
  2. Suivez les invites pour créer et combiner des expressions de requête.

  > Pour des informations complètes, voir Lancer une recherche dans Trail Flow à l'aide de l'assistant et Personnaliser les requêtes Trail Flow.

Afficher les détails d'un événement :

Une fois que vous avez identifié un événement important :

1. Cliquez sur l'événement. Cela fera apparaître les attributs de la modification de cet objet.
2. Survolez l'icône du point bleu à gauche pour comparer les valeurs avant et pendant l'événement.
3. Survolez les éléments pour voir des informations supplémentaires.
4. Cliquez sur **Voir la valeur entière** et cliquez sur le bouton pour copier ces informations dans le presse-papiers.

Identifier les changements de configuration :

L'un des défis liés à la cyber-sécurité des serveurs Active Directory réside dans le grand nombre de changements de configuration qui n'affectent pas la cyber-exposition. Pour identifier les changements de configuration :

1. Cliquez sur l'icône de la baguette magique.
2. Activez **Déviants uniquement**.
3. Cliquez sur **Valider**.

Afficher les éléments de cyber-exposition :

Vous remarquerez qu'un symbole de losange figure en regard des événements. Cliquez sur un événement pour afficher des informations concernant le changement de configuration. Un onglet supplémentaire étiqueté « Déviances » est disponible. Cliquez dessus pour voir les éléments de cyber-exposition spécifiques qui ont été créés ou résolus.

8. ### Identifier les attaques AD potentielles à l'aide des IoA

Les indicateurs d'attaque (IoA) de Tenable Identity Exposure permettent de détecter les attaques contre votre infrastructure Active Directory (AD).

> Pour des informations complètes, voir Indicateurs d'attaque.

Accéder aux IoA :

1. Connectez-vous à Tenable Identity Exposure.
2. Cliquez sur l'icône dans l'angle supérieur gauche pour développer la barre de navigation.
3. Cliquez sur **Indicateurs d'attaque**.

Filtrer la chronologie :

Par défaut, vous voyez la chronologie de la détection d'attaque d'aujourd'hui. Pour changer le filtre :

- Cliquez sur **Jour**, `Mois` ou **Année**.
- Pour modifier la période, cliquez sur l'icône du calendrier et sélectionnez la période appropriée.

Filtrer la vue :

Vous pouvez filtrer la vue sur des domaines ou des IoA spécifiques à l'aide du sélecteur sur le côté droit du portail.

1. Cliquez sur **Domaines** pour afficher les choix et effectuer des sélections.
2. Cliquez sur la croix **X** pour fermer.
3. Cliquez sur **Indicateurs** pour afficher les choix et effectuer des sélections.
4. Cliquez sur la croix **X** pour fermer.

À titre d'exemple, concentrons-nous sur ce qui s'est passé en 2022 :

1. Cliquez sur le bouton **Année** et sélectionnez « 2022 ».
2. Cliquez sur la barre rouge et jaune dans la chronologie.
3. Vous pouvez désormais voir une nouvelle vue avec les trois principales attaques

critiques et les trois principales attaques moyennes détectées ce mois-là.

4. Fermez la vue en cliquant en dehors de la zone noire.

Afficher les détails des attaques détectées :

Sous la chronologie, vous pouvez voir une carte du domaine surveillé sur lequel l'attaque a été détectée.

- Cliquez sur le menu déroulant **Trier par**.
- Vous pouvez trier la carte par domaine, par criticité d'indicateur ou par forêt.
- Pour rechercher un domaine ou une attaque spécifique, utilisez la zone de recherche.
- Par défaut, vous ne voyez qu'une carte pour le domaine attaqué. Changez de vue pour voir chaque domaine en faisant passer la fonction **N'afficher que les domaines attaqués** de **Oui** à **Non**.

Personnaliser le graphique :

Une carte contient deux types d'informations : un graphique et les trois principales attaques.

1. Pour modifier le type de graphique, cliquez sur l'icône de crayon dans l'angle supérieur droit de la carte.
2. Sélectionnez **Distribution des attaques** ou **Nombre d'événements**.
3. Cliquez sur **Enregistrer**.

Afficher les détails d'un événement :

Pour voir plus de détails sur l'attaque détectée :

- Cliquez sur la carte pour voir les incidents relatifs au domaine.
- Pour filtrer, utilisez la zone de recherche, sélectionnez une date de début ou de fin, des indicateurs spécifiques, ou activez la case **Non**/**Oui** pour afficher ou masquer les incidents clos.

- Pour clore des incidents, sélectionnez une alerte, cliquez sur le menu **Sélectionner une action** en bas, sélectionnez **Clore les incidents sélectionnés** et cliquez sur **OK**.
- Pour rouvrir des incidents, sélectionnez une alerte, cliquez sur le menu **Sélectionner une action** en bas, puis sélectionnez **Rouvrir les incidents sélectionnés** et cliquez sur **OK**.

Afficher les détails de l'attaque et les règles de détection Yara :

- Cliquez sur une attaque pour ouvrir la vue détaillée. Dans le panneau Description se trouvent la description de l'incident de l'attaque, les informations sur le cadre MITRE ATT&CK et des ressources supplémentaires contenant des liens vers des sites web externes.
- Cliquez sur le panneau Règles de détection YARA pour voir un exemple de règle permettant d'effectuer des recherches de malwares dans les outils de détection.
- Exportez la liste des incidents en cliquant sur **Tout exporter**. Le format CSV est le seul format disponible.

Notifications et alertes :

L'icône de cloche dans l'angle supérieur droit affiche une notification lorsque Tenable Identity Exposure détecte une attaque. Ces attaques apparaissent dans l'onglet Alertes d'attaque.

9. **Configurer et utiliser des alertes**

Le système d'alerte de Tenable Identity Exposure permet d'identifier les régressions de sécurité ou les attaques au sein de votre infrastructure Active Directory supervisée. Il envoie les données d'analyse sur les vulnérabilités et les attaques en temps réel par e-mail ou par notification Syslog.

> Pour les procédures complètes, voir Alertes.

Configurer le serveur SMTP :

1. Connectez-vous à Tenable Identity Exposure.
2. Cliquez sur **Système** > **Configuration**.
3. Configurez le serveur SMTP à partir de ce menu.

Créer des alertes e-mail :

1. Sous **Moteur de remontée d'alertes**, cliquez sur **E-mail**.
2. Cliquez sur le bouton **Ajouter une alerte e-mail**.
3. Dans la zone **Adresse e-mail**, saisissez l'adresse e-mail du destinataire.
4. Dans la zone **Description**, saisissez la description de l'adresse du destinataire.
5. Dans la liste déroulante **Déclencher les alertes**, sélectionnez **En cas de changement**, **À chaque déviance** ou **À chaque attaque**.
6. Dans le menu déroulant **Profils**, sélectionnez les profils à utiliser pour cette alerte e-mail.
7. Cochez la case **Envoyer des alertes quand des déviances sont détectées** pour envoyer des notifications par e-mail lorsqu'un redémarrage du système déclenche des alertes.
8. Dans le menu déroulant **Seuil de sévérité**, sélectionnez le seuil auquel Tenable Identity Exposure enverra des alertes.
9. Sélectionnez les indicateurs pour lesquels envoyer des alertes.
10. Sélectionnez des domaines pour les alertes :
    a. Cliquez sur **Domaines** pour sélectionner les domaines pour lesquels Tenable Identity Exposure envoie des alertes.
    b. Sélectionnez la forêt ou le domaine et cliquez sur le bouton **Filtrer sur la sélection**.
11. Cliquez sur le bouton **Tester la configuration**.

    Un message confirme que Tenable Identity Exposure a envoyé une alerte e-mail au serveur.

12. Cliquez sur le bouton **Ajouter**.

    Un message confirme que Tenable Identity Exposure a créé l'alerte e-mail.

Créer des alertes Syslog :

1. Cliquez sur **Syslog** puis sur le bouton **Ajouter une alerte Syslog**.
2. Dans la zone **Adresse IP ou nom d'hôte du collecteur**, saisissez l'adresse IP ou le nom d'hôte du serveur recevant les notifications.
3. Dans la zone **Port**, saisissez le numéro de port du collecteur.
4. Dans le menu déroulant **Protocole**, sélectionnez UDP ou TCP.
5. Si vous choisissez TCP, cochez la case de l'option **TLS** pour activer le protocole de sécurité TLS.
6. Dans la zone **Description**, saisissez une brève description du collecteur.
7. Choisissez l'une des trois options de déclenchement des alertes : **En cas de changement**, **À chaque déviance** ou **À chaque attaque**.
8. Dans le menu déroulant **Profils**, sélectionnez les profils à utiliser pour cette alerte Syslog.
9. Pour envoyer des alertes après le redémarrage ou la mise à niveau du système, cochez la case **Envoyer des alertes quand des déviances sont détectées pendant la phase d'analyse initiale**.
10. Si vous avez configuré des alertes pour qu'elles se déclenchent en cas de changement, saisissez une expression pour déclencher la notification d'événement.
11. Cliquez sur le bouton **Tester la configuration**.

    Un message confirme que Tenable Identity Exposure a envoyé une alerte Syslog au serveur.

12. Cliquez sur **Ajouter**.

    Un message confirme que Tenable Identity Exposure a créé l'alerte Syslog.

10. ## Configurer des dashboards dans le portail Tenable Identity Exposure

Les dashboards vous permettent de visualiser des données et des tendances sur la sécurité de votre infrastructure Active Directory. Vous pouvez les personnaliser avec des widgets pour afficher des graphes et des compteurs selon vos besoins.

> Pour des informations complètes, voir Dashboards.

Accéder aux dashboards :

1. Connectez-vous à Tenable Identity Exposure.
2. Cliquez sur l'icône dans l'angle supérieur gauche pour développer la barre de navigation.

Créer un dashboard personnalisé :

1. Accédez à **Dashboards** et cliquez sur **Ajouter**.
2. Cliquez sur **Ajouter un dashboard**.
3. Nommez-le et cliquez sur **OK**.

Ajouter des widgets au dashboard :

1. Cliquez sur **Ajouter** dans l'angle supérieur droit.
2. Sélectionnez **Ajouter un widget sur ce dashboard** ou cliquez sur le bouton au centre de l'écran.
3. Choisissez le type de widget (histogramme, courbe ou compteur).

Configurer un widget de type courbe :

1. Cliquez sur **Courbes**.
2. Nommez le widget, par exemple « Déviances au cours des 30 derniers jours ».

3. Choisissez le type de données (nombre d'utilisateurs, nombre de déviances ou score de conformité).
4. Sélectionnez **Déviances** et choisissez une période d'un mois.
5. Cliquez sur **Aucun indicateur** et sélectionnez les indicateurs à utiliser.
6. Nommez l'ensemble de données, par exemple « Critique ».
7. Ajoutez d'autres ensembles de données selon les besoins (par exemple, pour le niveau moyen et faible).
8. Cliquez sur **Ajouter**.

Ajouter un widget de type histogramme :

1. Cliquez sur **Histogramme**.
2. Nommez-le **Conformité** et choisissez le type de données Score de conformité.
3. Sélectionnez tous les indicateurs.
4. Nommez l'ensemble de données, par exemple « IoE ».
5. Cliquez sur **Ajouter**.

Ajouter un widget de type compteur :

1. Cliquez sur **Compteur**.
2. Nommez le widget, par exemple « Utilisateurs », et définissez le type de données sur **Nombre d'utilisateurs**.
3. Choisissez le statut **Tout** et sélectionnez le domaine.
4. Nommez l'ensemble de données et cliquez sur **Ajouter**.

11. **Afficher les chemins d'attaque**

Tenable Identity Exposure offre plusieurs façons de visualiser la vulnérabilité potentielle d'un asset opérationnel à l'aide de représentations graphiques.

Pour des informations complètes, voir Chemin d'attaque.

Accéder à la fonctionnalité Chemin d'attaque :

1. Connectez-vous à Tenable Identity Exposure.
2. Cliquez sur l'icône de menu dans l'angle supérieur gauche pour développer la barre de navigation.
3. Dans la section **Analyse de sécurité**, cliquez sur **Chemin d'attaque**. La fonction Chemin d'attaque comporte trois modes :
    - Chemin d'attaque
    - Blast Radius (rayon d'impact)
    - Exposition d'un asset

Utiliser le mode Blast Radius :

1. Dans la zone de recherche, saisissez le nom de l'asset (par exemple, « John Doe »).
2. Sélectionnez le compte dans la liste et cliquez sur l'icône de loupe.
3. Explorez le Blast Radius (rayon d'impact) à partir du compte compromis sélectionné.
4. Filtrez et affichez les nœuds selon vos besoins.
5. Survolez les terminaux pour afficher le chemin d'attaque.
6. Activez l'option pour afficher toutes les info-bulles des nœuds.
7. Utilisez la barre de zoom pour ajuster la vue.
8. Pour modifier l'objet de la recherche, cliquez sur la croix (**X**) à côté du nom du compte et lancez une nouvelle recherche.

Utiliser le mode Exposition d'un asset :

1. Dans la zone de recherche, saisissez le nom du serveur sensible (par exemple, « srv-fin »).
2. Sélectionnez l'objet dans la liste et cliquez sur l'icône de loupe.

3. Explorez l'exposition de l'asset au serveur sensible sélectionné.
4. Utilisez des options similaires à celles utilisées pour le mode Blast Radius.
5. Survolez les chemins pour afficher les détails.
6. Activez l'option pour afficher toutes les info-bulles des nœuds.
7. Ajustez la vue à l'aide de la barre inférieure.

Utiliser le mode Chemin d'attaque :

1. Dans la zone de recherche Nœud de départ, saisissez le nom du compte compromis (par exemple, « John Doe »).
2. Cliquez sur le nom du compte.
3. Dans la zone de recherche Nœud d'arrivée, saisissez le nom de l'asset sensible (par exemple, « s or v-fin »).
4. Cliquez sur le nom de l'asset.
5. Cliquez sur l'icône de loupe.
6. Explorez les chemins d'attaque disponibles entre le compte compromis et l'asset sensible.
7. Utilisez des options similaires à celles utilisées pour les modes Blast Radius et Exposition d'un asset.

Fonctionnalités supplémentaires :

- **Qui a un contrôle sur mes assets privilégiés ?** : affiche tous les comptes utilisateur et machine dont un chemin d'attaque mène à un asset privilégié.
- **Quels sont mes assets privilégiés ?** : répertorie les assets et les comptes Tier 0 avec les chemins d'attaque potentiels menant aux assets.
- Passez d'un onglet à l'autre pour afficher les listes.
- Cliquez sur l'icône de loupe en regard d'un élément pour changer de vue.

- Cliquez sur la flèche bleue et l'icône représentant un point pour ouvrir la vue d'exposition des assets filtrée afin d'afficher uniquement cet asset.

Interpréter les résultats :

1. Utilisez la fonctionnalité Chemin d'attaque pour confirmer les hypothèses et visualiser les chemins d'attaque dangereux entre les entités.
2. Prenez des mesures de remédiation pour fermer les chemins d'attaque identifiés.

Conseil : pour plus d'informations sur Tenable Identity Exposure, consultez les supports de formation suivants :

- Guide d'intégration autonome Tenable Identity Exposure (en anglais)
- Introduction à Tenable Identity Exposure (Tenable University) (en anglais)

Bases de Tenable Identity Exposure

Cette section couvre les tâches quotidiennes essentielles que la plupart des utilisateurs doivent connaître pour prendre en main Tenable Identity Exposure et profiter pleinement de la solution.

Que vous découvriez le produit ou que vous ayez simplement besoin d'un rappel des bases, vous trouverez ici des instructions pas à pas pour réaliser des opérations courantes telles que l'authentification, la navigation dans l'espace de travail, la définition des préférences et des notifications, l'utilisation des dashboards et des widgets, l'exploration des identités avec le Centre d'exposition, la visualisation des pistes de données avec Trail Flow et la compréhension des indicateurs d'exposition et des indicateurs d'attaque.

Pour trouver des informations relatives à une tâche spécifique, cliquez sur les rubriques correspondantes dans le volet de menu sur le côté gauche de l'écran.

Se connecter à Tenable Identity Exposure

Vous accédez à l'application web Tenable Identity Exposure par le biais d'une URL cliente.

Pour vous connecter à Tenable Identity Exposure, sélectionnez l'une des options suivantes :

- Utilisation d'un compte Tenable Identity Exposure
- Utilisation d'un compte LDAP
- Utilisation de SAML

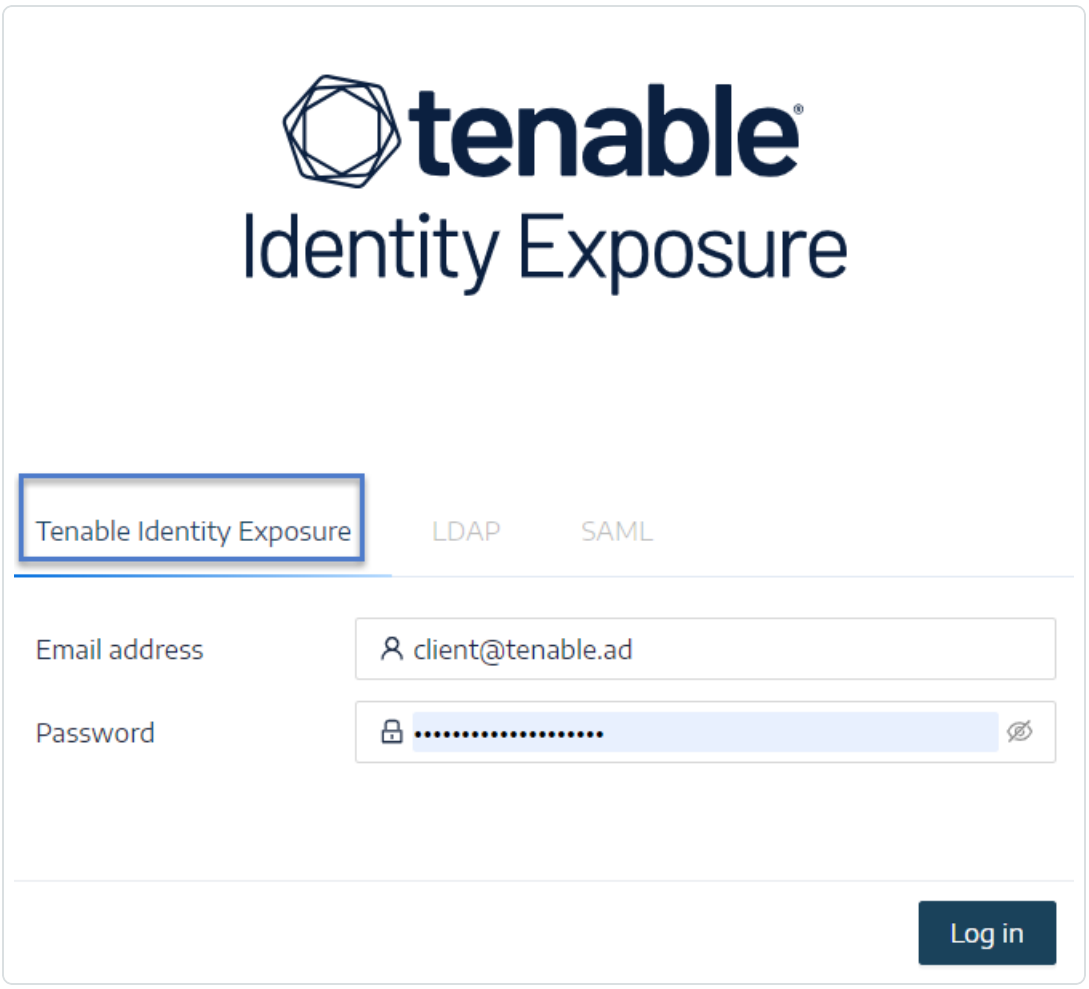
Remarque : vos identifiants initiaux sont le nom d'utilisateur `hello@tenable.ad` et le mot de passe `Hello@tenable.ad123!.`

Utilisation d'un compte Tenable Identity Exposure

Pour vous connecter avec votre compte Tenable Identity Exposure :

1. Dans un navigateur, saisissez l'URL de votre client (par exemple : client.tenable.ad) dans la barre d'adresse.

   La fenêtre de **connexion** apparaît.



2. Cliquez sur l'onglet **Tenable Identity Exposure**.
3. Saisissez votre adresse e-mail.
4. Saisissez votre mot de passe.
5. Cliquez sur **Se connecter**.

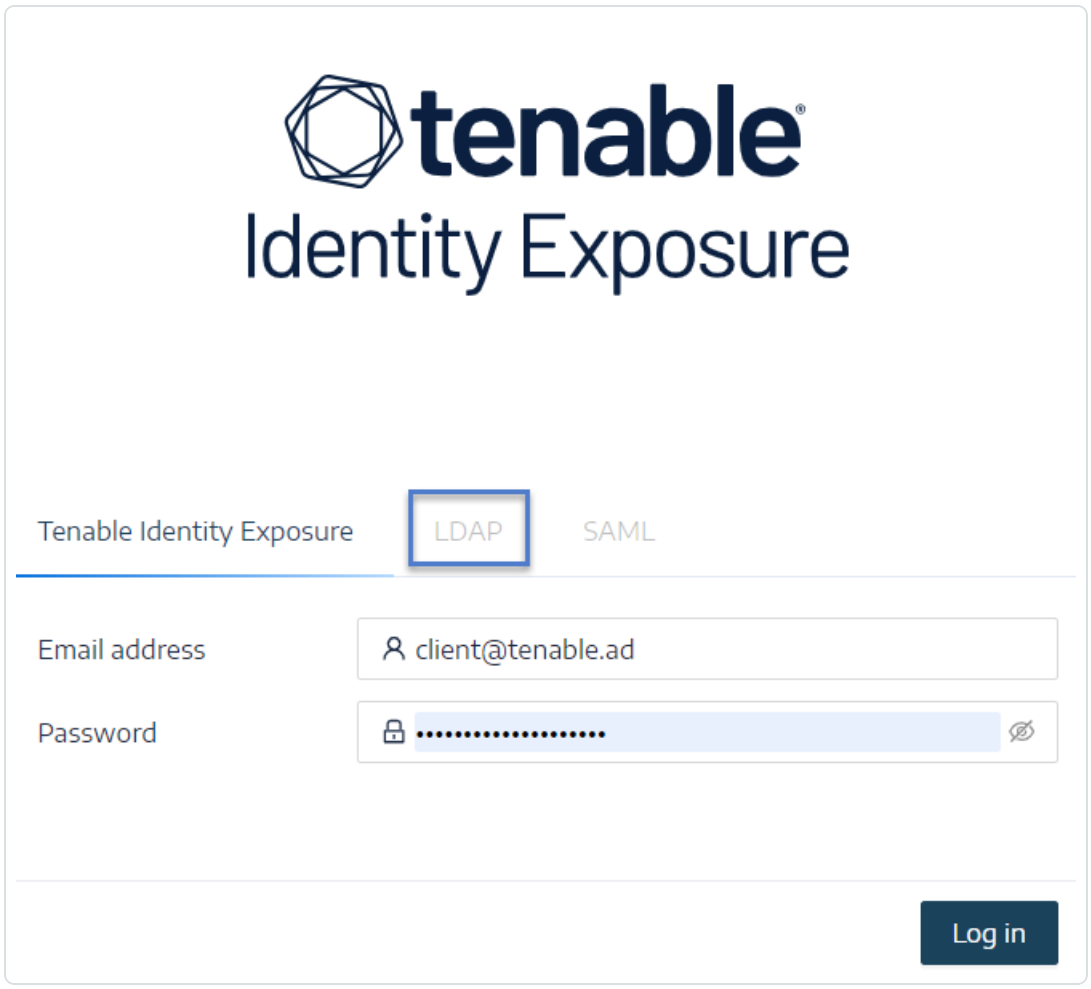
   La page Tenable Identity Exposure apparaît.

Utilisation d'un compte LDAP

Pour vous connecter avec LDAP :

1. Dans un navigateur, saisissez l'URL de votre client (par exemple : client.tenable.ad) dans la barre d'adresse.

La fenêtre de **connexion** apparaît.



2. Cliquez sur l'onglet **LDAP**.
3. Saisissez votre nom de compte LDAP.
4. Saisissez votre mot de passe LDAP.
5. Cliquez sur **Se connecter**.

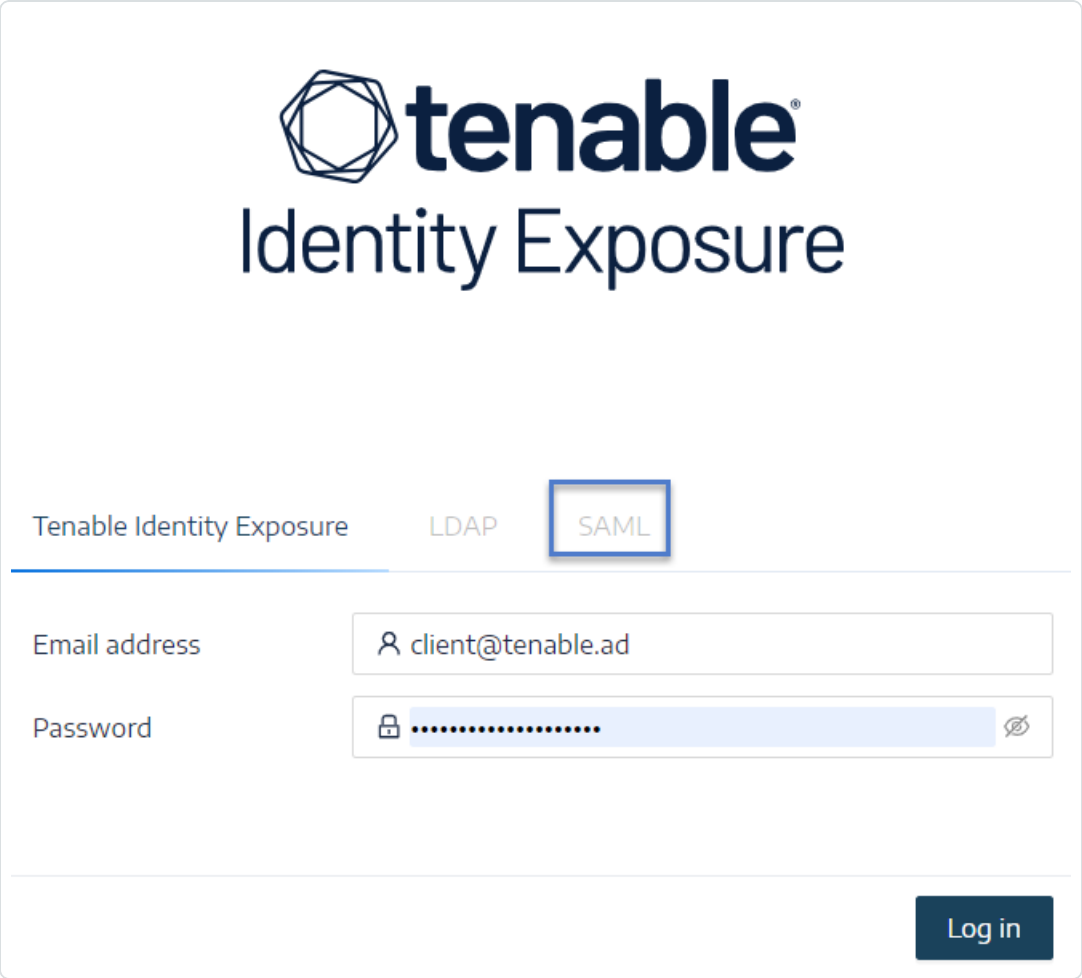
   La page Tenable Identity Exposure apparaît.

Utilisation de SAML

Pour vous connecter avec SAML :

1. Dans un navigateur, saisissez l'URL de votre client (par exemple : client.tenable.ad) dans la barre d'adresse.

   La fenêtre de **connexion** apparaît.



2. Cliquez sur l'onglet **SAML**.
3. Cliquez sur le lien d'accès à votre fournisseur d'identité (IDP).

   Tenable Identity Exposure vous redirige vers votre serveur SAML pour l'authentification.
4. Saisissez les identifiants de votre entreprise sur votre IDP.

   Vous êtes redirigé vers Tenable Identity Exposure en tant qu'utilisateur connecté.

Attention : si votre tentative de connexion échoue à plusieurs reprises, Tenable Identity Exposure verrouille votre compte. Contactez votre administrateur.

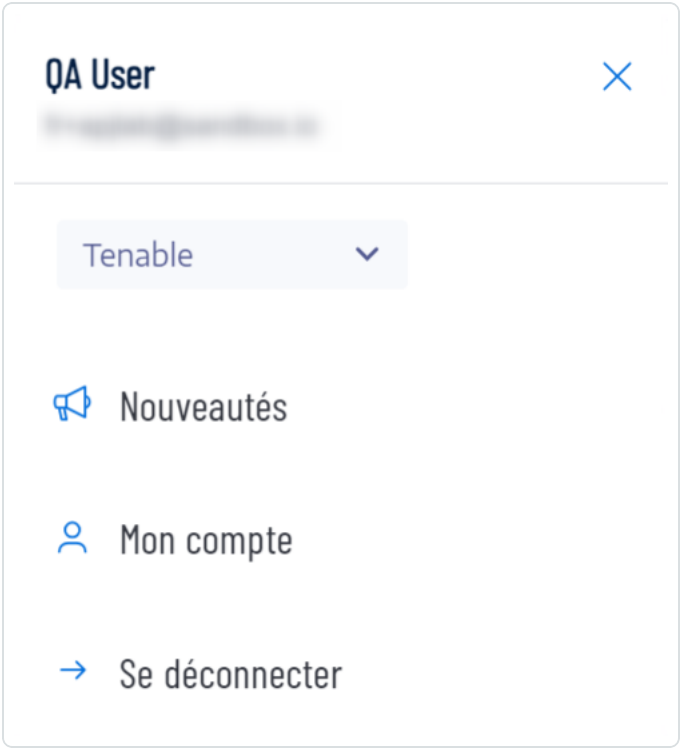
Pour réinitialiser votre mot de passe après la première connexion :

Lors de la première connexion avec le compte `hello@tenable.ad`, Tenable Identity Exposure vous invite à réinitialiser votre mot de passe par défaut.

Remarque : les informations de mot de passe ne sont pas disponibles si vous disposez d'une licence Tenable One. Dans ce cas, Tenable Vulnerability Management gère tous vos paramètres d'authentification. Pour plus d'informations, voir Contrôle d'accès dans le Guide de l'utilisateur Tenable Vulnerability Management.

1. Dans Tenable Identity Exposure, cliquez sur l'icône de votre profil utilisateur dans l'angle supérieur droit.

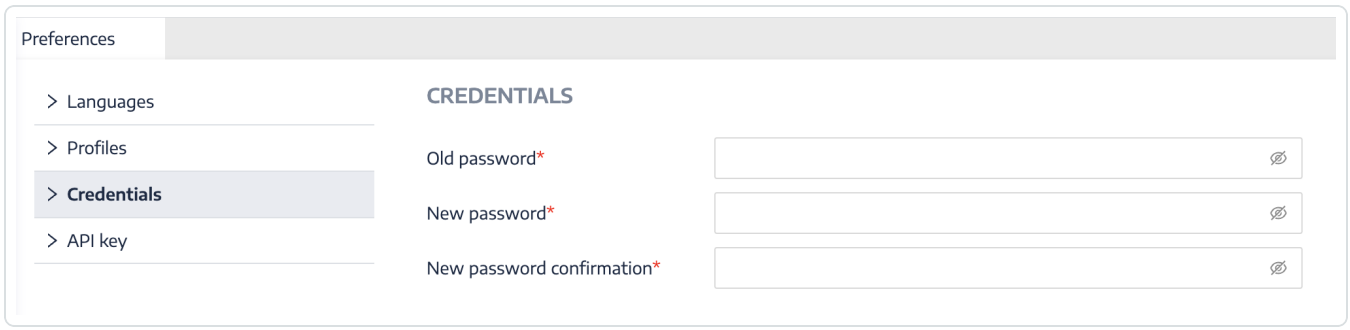
   Un sous-menu apparaît.

2. Sélectionnez **Mon compte**.

   La page **Préférences** apparaît.

3. Sous **Préférences**, cliquez sur **Identifiants**.



4. Dans le champ **Ancien mot de passe**, saisissez votre ancien mot de passe.
5. Dans le champ **Nouveau mot de passe**, saisissez un nouveau mot de passe. Respectez les règles de complexité suivantes, alignées sur les exigences relatives aux mots de passe des comptes Tenable One :
    - Au moins 12 caractères.
    - Au moins un exemplaire de chacun des éléments suivants :
        - Lettre majuscule (A-Z)
        - Lettre minuscule (a-z)
        - Chiffre (0-9)
        - Caractère spécial (p. ex., !, @, #, $)
    - Ne peut pas contenir la chaîne `verysecure` pour éviter la réutilisation du mot de passe par défaut précédent `verySecure1!`.
6. Dans la zone **Confirmation du nouveau mot de passe**, resaisissez le nouveau mot de passe.
7. Cliquez sur **Enregistrer**.

    Un message confirme que Tenable Identity Exposure a changé votre mot de passe.

Pour vous déconnecter de Tenable Identity Exposure :

1. Dans Tenable Identity Exposure, cliquez sur votre icône d'utilisateur.

    Un sous-menu apparaît.
2. Cliquez sur **Se déconnecter**.

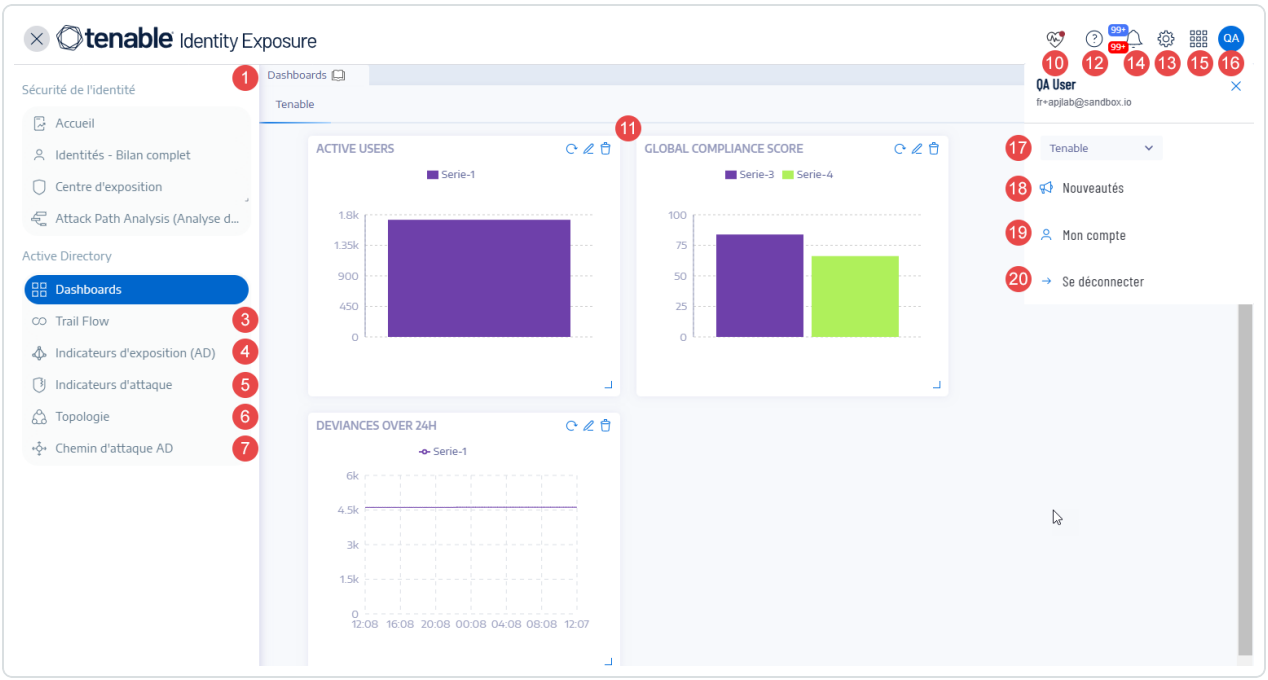
    Tenable Identity Exposure revient à la page de connexion.

Portail utilisateur Tenable Identity Exposure

Après vous être connecté à Tenable Identity Exposure, la page d'accueil, représentée ci-dessous, apparaît.

Pour développer ou réduire la barre de navigation latérale :

- Pour la développer : cliquez sur le menu ☰ dans l'angle supérieur gauche de la fenêtre.
- Pour la réduire : cliquez sur le signe ✕ dans l'angle supérieur gauche de la fenêtre.



#	Élément	Fonction
1	Dashboards	Les dashboards vous permettent de gérer et de surveiller efficacement et visuellement la sécurité au sein d'une infrastructure Active Directory.
2	-	-
3	Trail Flow	Le Trail Flow affiche la surveillance et l'analyse en temps réel des événements qui affectent votre infrastructure Active Directory.

4	Indicateurs d'exposition	Tenable Identity Exposure utilise des indicateurs d'exposition (IoE) pour mesurer la maturité de la sécurité de votre infrastructure Active Directory et attribuer des niveaux de sévérité (critique, élevé, moyen ou faible) au flux d'événements qu'il surveille et analyse.
5	Indicateurs d'attaque	Tenable Identity Exposure détecte les attaques en temps réel par le biais des indicateurs d'attaque.
6	Topologie	La page Topologie affiche votre infrastructure Active Directory sous la forme d'un graphique interactif. Elle montre les forêts, les domaines et les relations d'approbation qui existent entre eux.
7	Chemin d'attaque	Les pages Chemin d'attaque sont des représentations graphiques des relations Active Directory : • Blast Radius : (litéralement « rayon d'impact ») évalue les mouvements latéraux dans l'infrastructure AD à partir d'un asset potentiellement compromis. • Chemin d'attaque : anticipe les techniques d'élévation de privilèges pour atteindre un asset à partir d'un point d'entrée donné.

		• Exposition d'un asset : mesure la vulnérabilité d'un asset en visualisant son exposition et permet de mettre en évidence/traiter toutes les élévations de privilèges via les chemins empruntés.
8, 9	Gestion **Rôle utilisateur requis** : utilisateur organisationnel disposant des autorisations appropriées.	Cette section vous permet de configurer les éléments suivants : • Comptes : comptes utilisateurs, rôles et profils de sécurité. • Système : forêts et domaines, services d'application, alertes et authentification. Pour plus d'informations, voir le Configuration et administration de Tenable Identity Exposure.
10	Vérifications de l'état du système	Les vérifications de l'état du système vous offrent une visibilité en temps réel sur la configuration de vos domaines et comptes de service dans une seule vue unifiée, à partir de laquelle vous pouvez accéder à des informations plus détaillées.
11	Widgets	Les widgets sont des datasets (ou ensembles de données) personnalisables sur un dashboard. Ils peuvent contenir des histogrammes, des graphiques en courbes et des compteurs.
12	Actualités du produit	Informations sur les dernières

		fonctionnalités du produit.
13	Paramètres	Accès à la configuration système, à la gestion des forêts et des domaines, à la gestion des licences, des utilisateurs et des rôles, aux profils et aux journaux d'activité.
14	Notifications (icône de cloche)	L'icône de cloche et le badge compteur vous signalent les alertes d'attaque et/ou les alertes d'exposition en attente dont vous devez prendre connaissance.
15	Accéder à l'espace de travail	Cliquez sur cette icône pour passer d'une application à l'autre à partir de l'espace de travail Tenable.
16, 19	Icône de profil utilisateur (Préférences utilisateur)	Cliquez sur cette icône pour accéder à un sous-menu contenant les profils de sécurité, les notes de version, les journaux d'activité, les préférences ou la déconnexion.
17	Profils de sécurité	Les profils de sécurité permettent à différents types d'utilisateurs d'examiner l'analyse de la sécurité sous différents angles de reporting.
18	Nouveautés	Cliquez pour ouvrir les notes de version pour la dernière version de Tenable Identity Exposure.
20	Déconnexion	Cliquez pour vous déconnecter de Tenable Identity Exposure.

Page d'informations de Tenable Identity Exposure

La page **Informations** de Tenable Identity Exposure offre une interface complète et conviviale, conçue pour répondre aux besoins critiques des organisations en matière de gestion de la sécurité des identités. Elle permet notamment d'évaluer la fluidité de votre paysage des risques liés aux identités, met en évidence les risques liés aux identités les plus urgents pour votre organisation et apporte des conseils sur la priorisation des étapes de remédiation à fort impact et à faible effort pour soutenir les équipes soumises à des contraintes strictes dans l'environnement de sécurité complexe d'aujourd'hui.

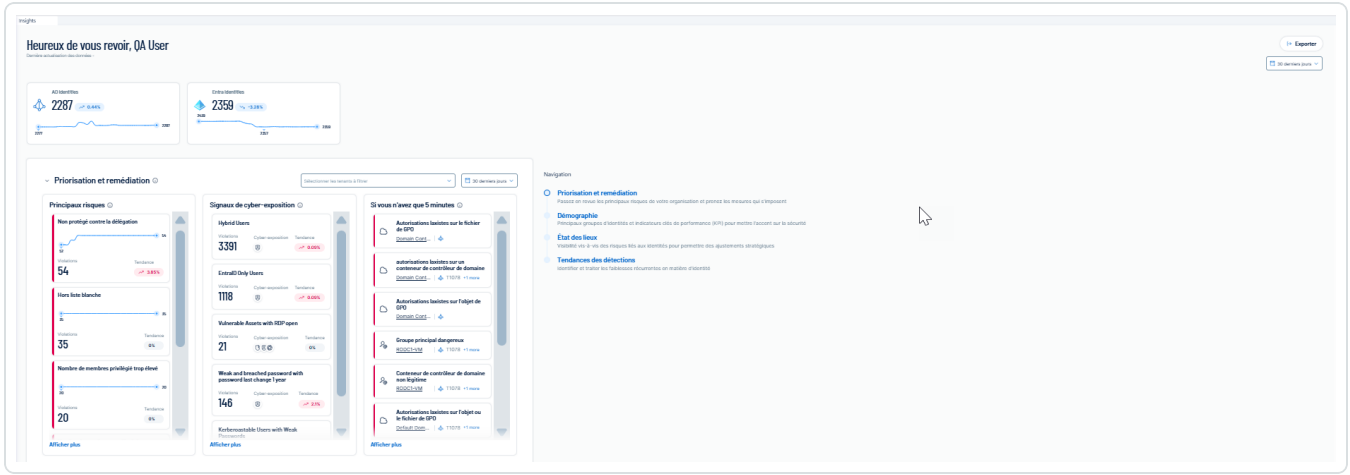
Conçu pour offrir une page de destination immersive, ce dashboard regroupe les métriques et les informations essentielles sur la sécurité des identités au sein d'une vue centralisée, unique et interactive. Grâce à une approche simplifiée de la surveillance de la sécurité des identités, Tenable Identity Exposure vous permet d'évaluer rapidement votre posture de sécurité, d'identifier et de prioriser les vulnérabilités à haut risque et de prendre des mesures concrètes pour atténuer les menaces potentielles.

La page **Informations** vous offre des fonctionnalités d'exploration complète, de filtrage spécifique aux identités et de partage transparent des données et des informations critiques via une expérience de reporting détaillée. Elle est conçue pour servir différents rôles axés sur la sécurité des identités.

> **Remarque** : la page **Informations** affiche actuellement exclusivement les données associées au profil de sécurité « Tenable » et ignore tous les autres profils de sécurité.

Pour accéder à la page **Informations** de Tenable Identity Exposure :

- Dans Tenable Identity Exposure, cliquez sur  dans la barre de navigation de gauche.



En-tête

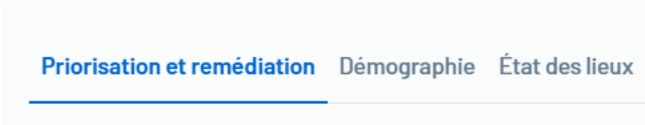
L'en-tête résume les nouveaux risques ainsi que les risques résolus pour vous offrir une vue instantanée de l'état de sécurité actuel, sans avoir à vous plonger dans des rapports détaillés. Cette fonctionnalité permet de prendre des décisions et de passer à l'action plus rapidement.

- Message de bienvenue – Ce message accueille les utilisateurs réguliers en les appelant par leur nom d'utilisateur.
- Métriques d'identité pour les différents fournisseurs (Active Directory, Entra ID, etc.) : la représentation visuelle vous aide à repérer les changements inhabituels chez les différents fournisseurs d'identité ; ces changements peuvent en effet indiquer des problèmes de sécurité potentiels ou mettre en évidence une progression de l'exposition des identités.
    - Les tuiles correspondant aux identités AD, aux identités Entra, etc., affichent le nombre actuel d'identités de chaque fournisseur, accompagné d'un pourcentage de tendance illustré par une petite courbe. Vous pouvez cliquer sur une tuile pour afficher des informations supplémentaires sur la plateforme d'identité en question.
    - Cliquez sur **>** pour afficher toutes les plateformes d'identité si elles ne sont pas toutes visibles sur la page.
- Sélecteur de période : grâce au menu déroulant permettant de sélectionner une période (par exemple, « 90 derniers jours »), vous pouvez adapter les données affichées afin de visualiser les tendances sur différentes périodes. Cette fonctionnalité offre une grande flexibilité en matière d'analyse, pour faciliter à la fois le suivi des risques à court terme et la planification stratégique à long terme.

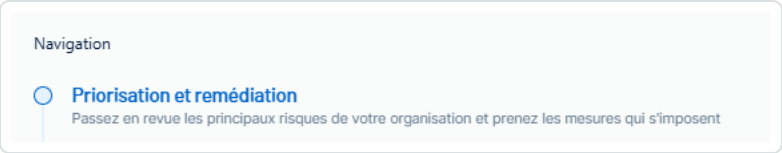
Navigation dans les sections

Vous pouvez parcourir les sections de la page **Informations** à l'aide des options suivantes :

- Onglets situés sous les tuiles des métriques d'identités :



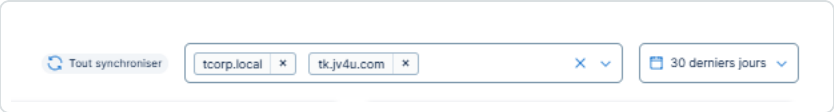
- Sur la droite, un menu de navigation vertical vous permet de consulter les différentes sections de la page **Informations**. Cliquez sur une section pour accéder à cette vue.



Conseil : réduisez le niveau de zoom de la page pour faire apparaître la barre de navigation à droite.

Sélection d'un domaine ou d'une organisation

À l'aide de la zone de filtre, vous pouvez sélectionner un ou plusieurs domaines pour vous concentrer sur des domaines ou des unités opérationnelles spécifiques.



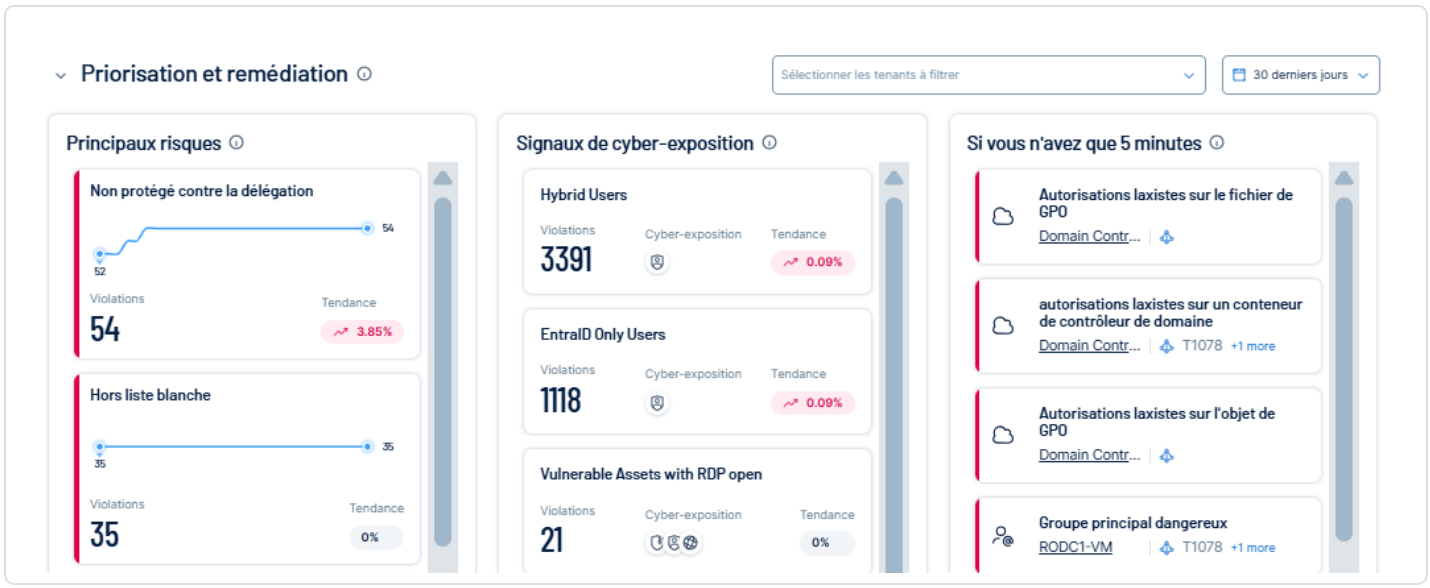
Pour sélectionner des domaines ou des organisations :

1. Cliquez sur la flèche dans la zone de filtre pour afficher les domaines ou les organisations, puis sélectionnez les éléments à filtrer.
2. Cliquez sur la flèche du sélecteur de période pour ajuster la fenêtre temporelle de l'analyse de données et suivre l'évolution des tendances au fil du temps.
3. Cliquez sur « Tout synchroniser » pour appliquer le filtre. Un message confirme que Tenable Identity Exposure a bien appliqué le filtre.

Cette zone de filtre est disponible pour chaque section de la page **Informations**.

Section « Priorisation et remédiation »

Cette section sert essentiellement de centre de contrôle de la sécurité. Elle présente clairement les vulnérabilités de sécurité les plus importantes aux administrateurs pour les aider à prioriser efficacement leurs efforts de remédiation.



Principaux risques

Ce panneau affiche les risques les plus importants pour les domaines et la période sélectionnés, classés par niveau de sévérité. Il affiche le nombre de violations actuelles dans votre environnement et illustre les tendances à l'aide de courbes qui indiquent si les problèmes sont en augmentation ou en recul.

- Cliquez sur la tuile pour savoir sur quoi concentrer les efforts de remédiation immédiats.

Signaux de cyber-exposition

Les signaux de cyber-exposition sont des faisceaux de risques susceptibles de devenir un chemin d'attaque ou une combinaison toxique. Ces informations sont classées par sévérité et contiennent chacune le nombre de violations et les types de risques à l'origine de l'exposition (indiqués par des icônes). Elles incluent également un indicateur de tendance qui affiche l'évolution sous forme de pourcentage.

- Cliquez sur la tuile pour accéder à des informations détaillées sur le signal de cyber-exposition.

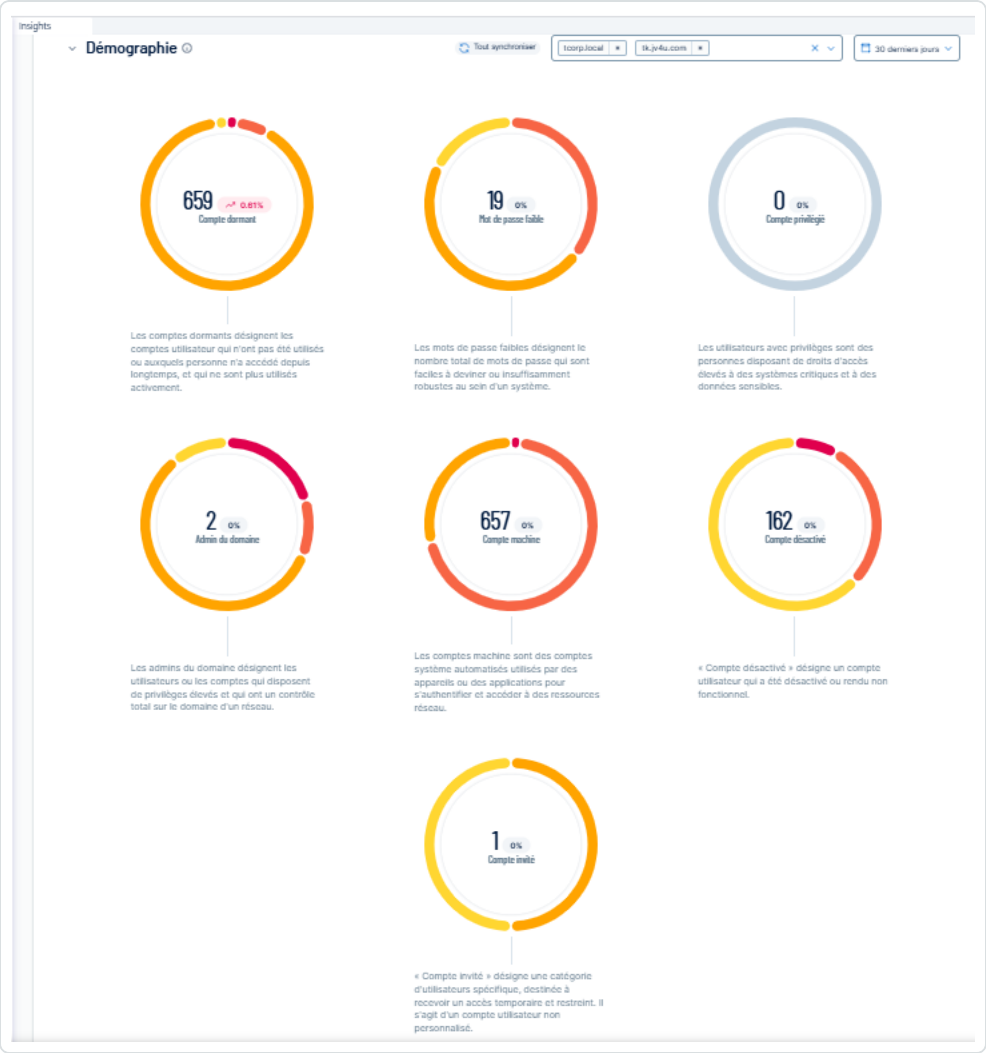
Si vous avez 5 minutes

Ce panneau se concentre sur les risques hautement prioritaires et invite à agir rapidement pour résoudre les problèmes urgents.

- Cliquez sur la tuile pour afficher plus de détails sur la remédiation du risque.

Section « Démographie »

La section **Démographie** fournit des informations critiques sur les principales cohortes d'identités (groupes d'identités ou d'utilisateurs qui partagent des caractéristiques communes) qui méritent l'attention des équipes de sécurité. Elle vous aide à mieux comprendre la répartition des risques au sein de votre organisation afin d'éclairer la prise de décision.



Ces graphiques circulaires représentent les principales cohortes d'identités au sein de la section Démographie. Chaque graphique met en évidence une catégorie spécifique de comptes ou d'indicateurs de sécurité critiques pour la surveillance.

- **Nombre central** – Le nombre au centre de chaque visuel représente le décompte actuel ou la valeur actuelle d'une faiblesse ou d'une cohorte d'identités spécifique. Ce nombre offre une vue instantanée du nombre total d'instances liées à cette catégorie, comme le nombre de comptes dormants, de mots de passe faibles ou de comptes privilégiés, etc. Il donne une indication visuelle rapide de l'étendue des problèmes de sécurité potentiels ou des risques liés aux identités au sein de l'organisation. Interprétez ce nombre conjointement avec l'indicateur de tendance et le code couleur pour comprendre parfaitement sa signification.
- **Indicateur de tendance** – Cet indicateur affiche le pourcentage d'évolution de la métrique par rapport à une période de rapport précédente pour indiquer si la situation s'améliore, se détériore ou se stabilise avec le temps.
    - Flèche vers le bas (↓) avec pourcentage en vert – Indique une diminution, ce qui est généralement un signe positif lorsqu'il s'agit de risques de sécurité (par exemple, moins de mots de passe faibles).
    - Flèche vers le haut (↑) avec pourcentage en rouge – Représente une augmentation, ce qui peut indiquer une préoccupation croissante selon la métrique.
- **Indicateur de couleur** – Les cercles colorés entourant chaque métrique représentent la répartition des niveaux de risque associés à cette faiblesse spécifique, allant de critique (rouge) à faible (jaune).
- **Texte explicatif** – Le texte situé sous chaque cercle coloré donne une brève description de la faiblesse spécifique afin de vous aider à comprendre les implications de sécurité des éléments suivis par la métrique, comme les mots de passe faibles, les comptes dormants, etc.

Pour afficher des informations détaillées :

- Pour plus d'informations sur les assets affectés par une faiblesse donnée, cliquez au centre du cercle pour accéder à Tenable Inventory.
- Pour plus d'informations sur la répartition des risques pour une faiblesse donnée, cliquez sur le segment coloré du cercle pour accéder à la Vue d'ensemble de la cyber-exposition. Pour plus d'informations, voir Centre d'exposition.

Remarque : les détails des « comptes machine » sont actuellement désactivés car ces comptes ont été temporairement supprimés de Tenable Inventory. Par conséquent, les « comptes machine » n'apparaissent pas dans Tenable Inventory, ce qui se traduit par un écart entre les nombres affichés dans Tenable Identity Exposure et Tenable Inventory.

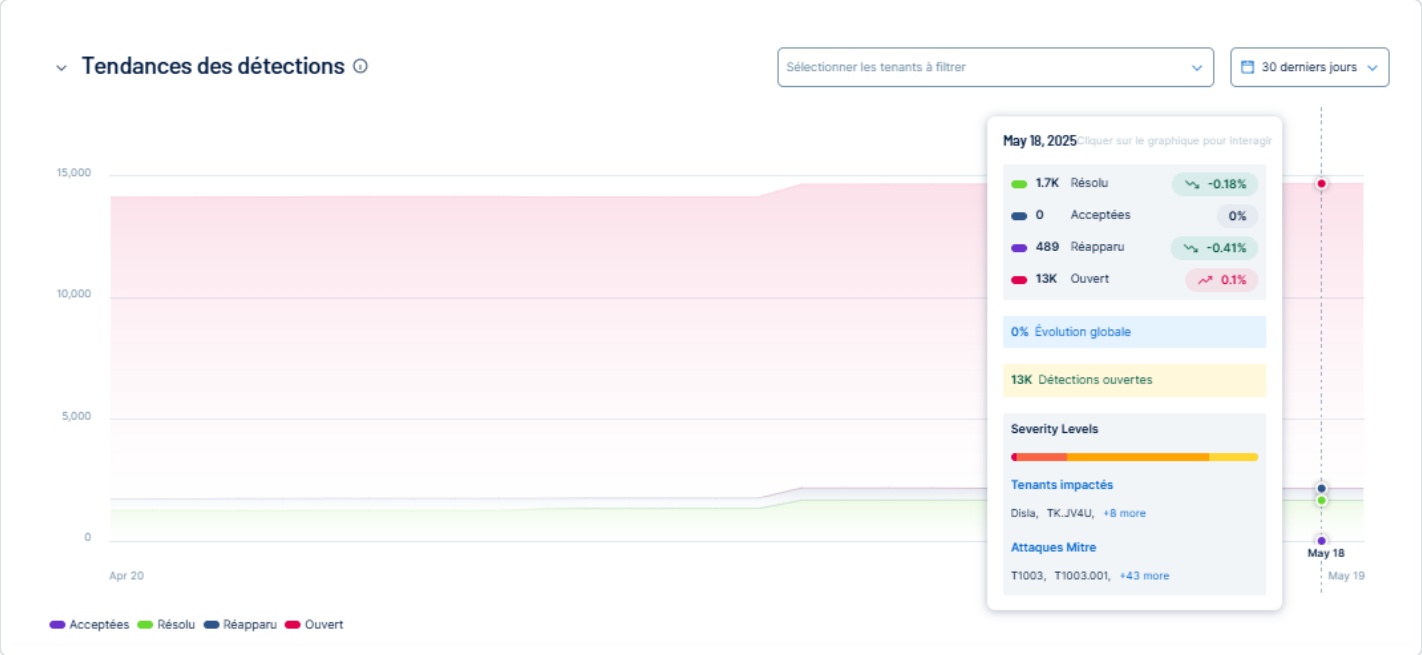
Remarque : la fonctionnalité Vue d'ensemble de la cyber-exposition affiche actuellement des données liées aux faiblesses en fonction du **profil Tenable par défaut** et ne reflète pas automatiquement le **statut des déviances sur les objets AD que vous avez ajoutés à la liste blanche dans d'autres profils**.

Par conséquent :

- Si vous avez **ajouté un objet AD à la liste blanche** pour un indicateur d'exposition spécifique (p. ex., « Membre d'un groupe d'administrateurs natif »), **la Vue d'ensemble de la cyber-exposition le signalera toujours comme une faiblesse de sécurité si le profil par défaut l'a identifié comme déviant**.
- Vous pouvez ainsi avoir l'impression que le problème n'a pas été résolu, même si l'objet a déjà été ajouté à la liste blanche sous un profil différent.
- Si une mesure de remédiation (telle que la suppression de l'appartenance à un groupe) est prise sur la base des indications de la Vue d'ensemble de la cyber-exposition, l'objet disparaît de la vue. Mais si l'objet était déjà sur liste blanche ailleurs, il est possible que cette mesure ait été facultative.

Section « Tendances des détections »

La section **Tendances des détections** affiche une analyse continue des données de sécurité historiques de votre organisation pour identifier des schémas dans les vulnérabilités et les faiblesses liées aux identités. Cette analyse historique aide les équipes de sécurité à garder une longueur d'avance sur les menaces potentielles en comprenant les problèmes récurrents et l'évolution des tendances en matière de risque.



La section **Tendances des détections** présente une vue chronologique qui suit différentes catégories de détections de sécurité, affichées sous la forme d'un graphique en aires empilées. La visualisation répartit les détections en quatre statuts clés :

- Détections résolues (affichées en vert)
- Détections acceptées (affichées en bleu)
- Détections réapparues (affichées en violet)
- Détections ouvertes (affichées en rose/rouge)

Pour filtrer l'un de ces statuts, cliquez sur le nom du statut en bas du graphique.

Autres fonctionnalités :

- Métriques d'évolution globale
- Compteur du nombre total de détections
- Indicateurs de niveau de sévérité

Pour obtenir des informations détaillées sur les données, cliquez sur ces liens :

- MITRE ATT&CK
- Tenants impactés

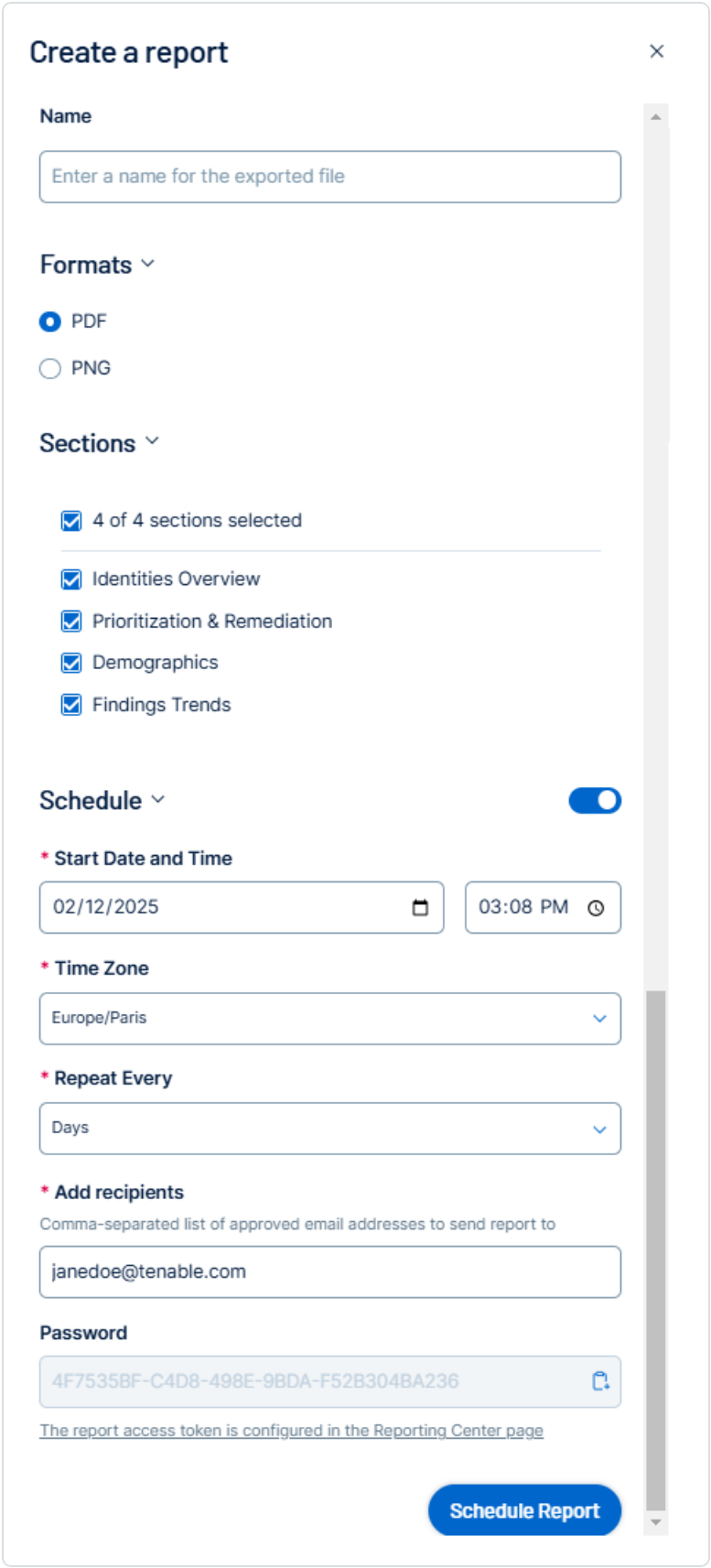
Création de rapports

La fonction Exporter sur la page **Informations** ouvre une fenêtre de création de rapports qui vous permet de personnaliser et de générer des rapports détaillés en fonction de vos besoins.

Pour créer un rapport :

1. Cliquez sur **Exporter** dans l'angle supérieur droit de la page **Informations**.

   La fenêtre **Créer un rapport** apparaît.


Create a report
Name
Enter a name for the exported file
Formats
PDF
PNG
Sections
4 of 4 sections selected
Identities Overview
Prioritization & Remediation
Demographics
Findings Trends
Schedule
* Start Date and Time
02/12/2025
03:08 PM
* Time Zone
Europe/Paris
* Repeat Every
Days
* Add recipients
Comma-separated list of approved email addresses to send report to
janedoe@tenable.com
Password
4F7535BF-C4D8-498E-9BDA-F52B304BA236
The report access token is configured in the Reporting Center page
Schedule Report

2. Dans la zone **Nom**, donnez au rapport un nom qui vous permette à vous et aux autres d'identifier son contenu. Par exemple, utilisez des noms tels que « Informations hebdomadaires sur la sécurité » ou « Tendances mensuelles des identités ».
3. Sous **Formats**, choisissez le format de fichier du rapport. Vous pouvez choisir l'option **PDF** (pour un format de document standard) ou **PNG** (utile pour des instantanés ou des éléments visuels individuels).
4. Choisissez une **section** à inclure dans le rapport :
    - **Vue d'ensemble des identités** : présente un inventaire des identités de divers fournisseurs (Identités 360).
    - **Priorisation et remédiation** : résume les risques critiques et les actions recommandées.
    - **Démographie** : fournit des informations sur les principales cohortes d'identités.
    - **Tendances des détections** : affiche une analyse continue pour identifier des schémas dans les vulnérabilités et les faiblesses liées aux identités.
5. Pour planifier un rapport, activez le bouton **Calendrier** et effectuez les opérations suivantes :
    - **Date et heure de début** : définissez la date et l'heure de début du premier rapport.
    - **Fuseau horaire** : sélectionnez le fuseau horaire approprié pour une planification précise.
    - **Répéter** : choisissez la fréquence du rapport (par exemple, hebdomadaire ou mensuel). Par exemple, pour recevoir un rapport hebdomadaire, sélectionnez « Toutes les semaines ».
    - **Ajouter des destinataires** : saisissez les adresses e-mail des personnes qui doivent recevoir le rapport. Séparez les adresses par des virgules.
    - **Mot de passe** : jeton en lecture seule configuré dans le Centre de rapports à titre d'information.
6. Cliquez sur **Planifier le rapport** pour enregistrer les paramètres et générer le rapport selon le calendrier spécifié.

    Les destinataires reçoivent une notification par e-mail contenant une URL pour télécharger les rapports.

Accéder à l'espace de travail

Lorsque vous vous connectez à Tenable, la page Espace de travail apparaît par défaut. Sur la page **Espace de travail**, vous pouvez passer d'une application Tenable à une autre ou définir une application par défaut pour y accéder sans afficher la page **Espace de travail** à l'avenir.

Le menu Espace de travail qui apparaît dans la barre de navigation supérieure vous permet de passer rapidement d'une application Tenable à l'autre depuis n'importe quelle page.

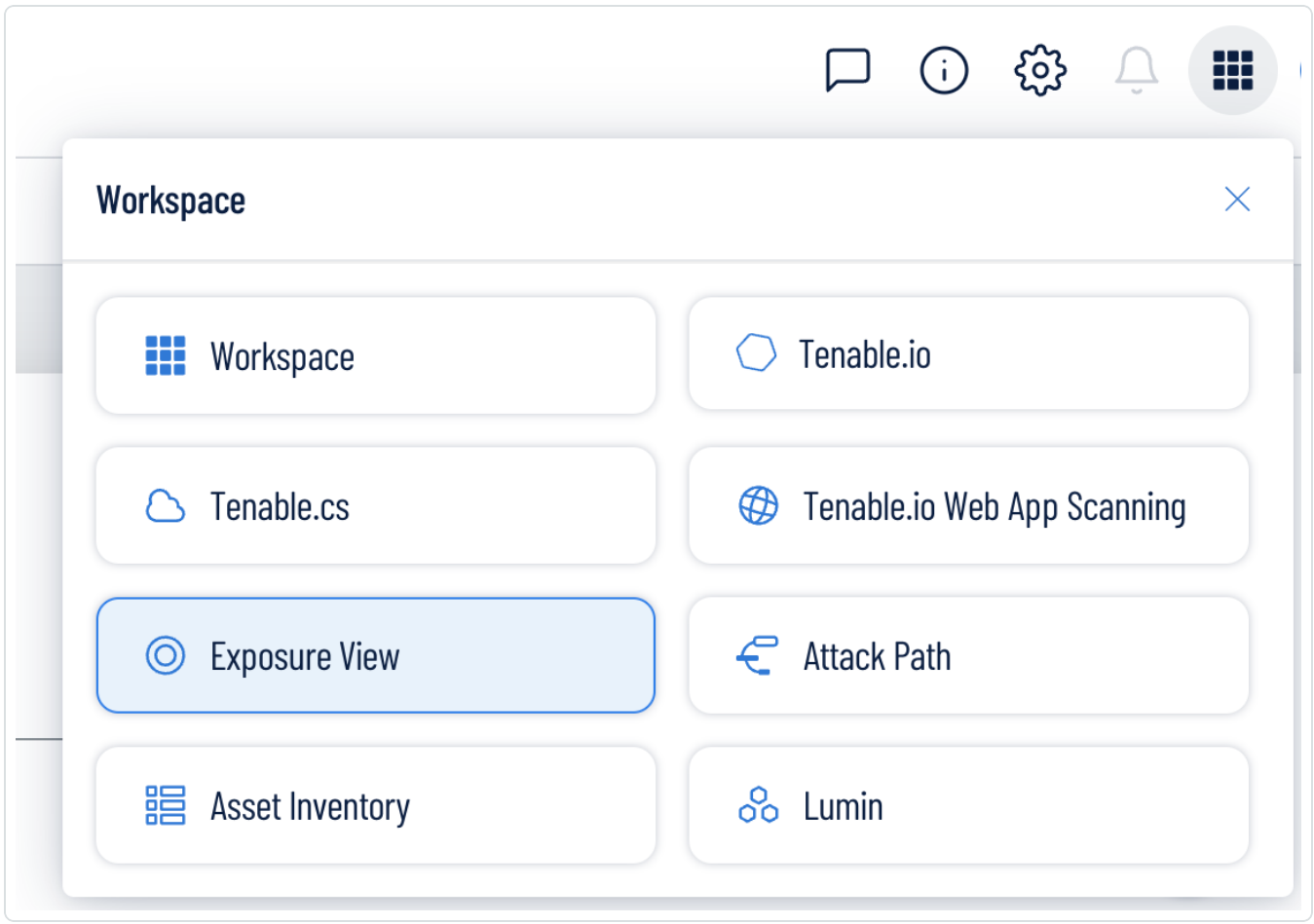
Important : Tenable désactive les tuiles des applications expirées. Tenable supprime les tuiles des application expirées de la page et du menu **Espace de travail** 30 jours après l'expiration.

Menu Espace de travail

Pour ouvrir le menu **Espace de travail** :

1. À partir de n'importe quelle application Tenable, dans l'angle supérieur droit, cliquez sur le bouton .

   Le menu **Espace de travail** apparaît.



2. Cliquez sur une tuile d'application pour l'ouvrir.

Page Espace de travail

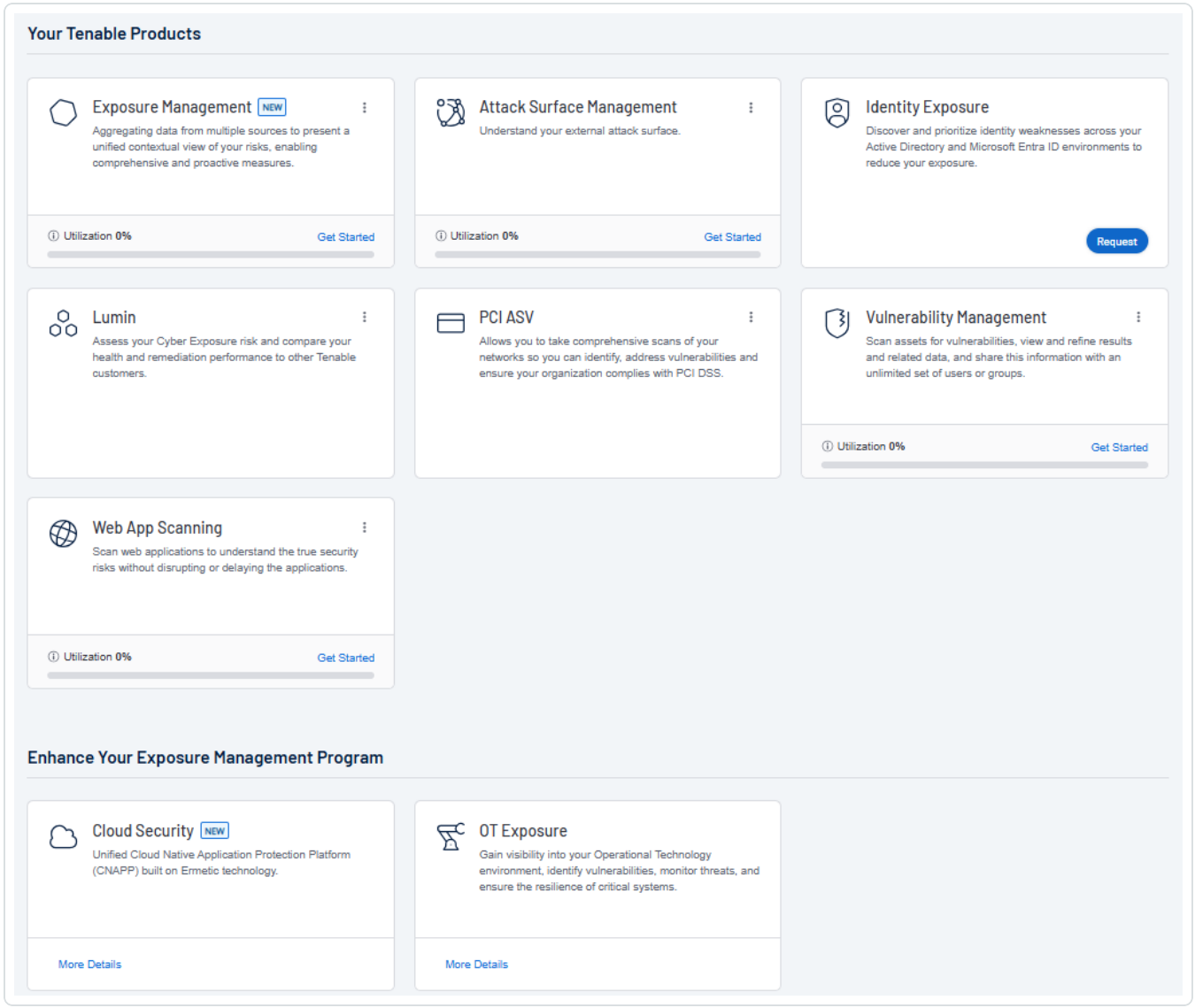
Pour afficher la page Espace de travail :

1. À partir de n'importe quelle application Tenable, dans l'angle supérieur droit, cliquez sur le bouton .

   Le menu **Espace de travail** apparaît.

2. Dans le menu **Espace de travail**, cliquez sur **Espaces de travail**.

La page **Espace de travail** apparaît.



Sur la page **Espace de travail**, vous pouvez effectuer les opérations suivantes :

- Le cas échéant, au bas d'une tuile, vous pouvez voir le pourcentage d'utilisation de votre licence pour l'application. Cliquez sur **Voir plus** pour accéder directement à la page **Informations de licence** de l'application sélectionnée.

  Conseil : pour obtenir plus d'informations sur le fonctionnement des licences Tenable, et la façon dont les licenses s'appliquent aux assets et aux ressources dans chaque produit, voir Licences des produits Tenable.

- **Définir une application par défaut :**

  Lorsque vous vous connectez à Tenable, la page **Espace de travail** apparaît par défaut. Cependant, vous pouvez définir une application par défaut pour y accéder sans passer par la page **Espace de travail** à l'avenir.

  > Par défaut, les utilisateurs ayant les rôles **Administrateur**, **Gestionnaire de scan**, **Opérateur de scan**, **Standard** et **De base** peuvent définir une application par défaut. Si vous avez un autre rôle, contactez votre administrateur et demandez l'autorisation **Gérer** sous **Mon compte**. Pour plus d'informations, voir Rôles personnalisés.

  Pour définir une application de connexion par défaut :

  1. Dans l'angle supérieur droit de l'application à choisir, cliquez sur le bouton ⋮.

     Un menu apparaît.

  2. Dans le menu, cliquez sur **Choisir comme page de connexion par défaut**.

     Cette application apparaît désormais lorsque vous vous connectez.

- **Supprimer une application par défaut :**

  Pour supprimer une application d'accueil par défaut :

  1. Dans l'angle supérieur droit de l'application à supprimer, cliquez sur le bouton ⋮.

     Un menu apparaît.

  2. Cliquez sur **Ne plus utiliser comme page de connexion par défaut**.

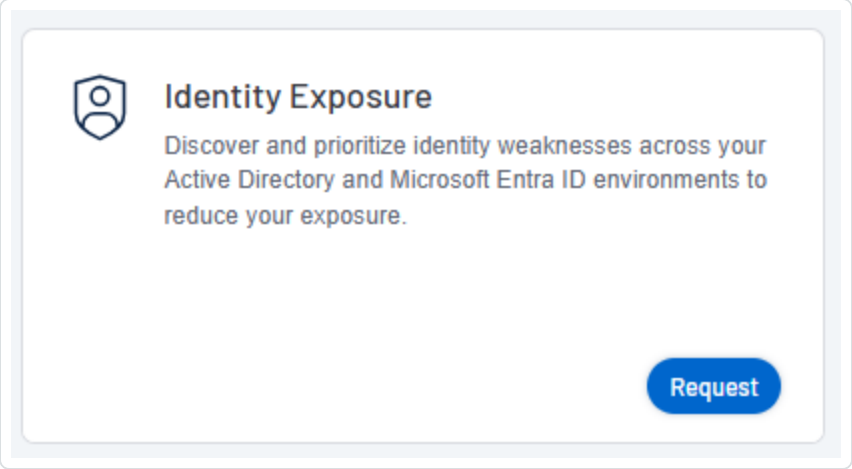
     La page **Espace de travail** apparaît désormais lorsque vous vous connectez.

- **Demander l'accès à une application Tenable :**

  Pour accéder à certaines applications, comme Tenable Identity Exposure, il est nécessaire d'en faire la demande. Vous pouvez le faire directement via la page **Espace de travail**.

  Pour demander l'accès à une application Tenable :

1. Dans le coin inférieur droit de la tuile, cliquez sur **Demander**.



   Vous accédez directement à la page de demande de l'application sélectionnée.

Préférences utilisateur

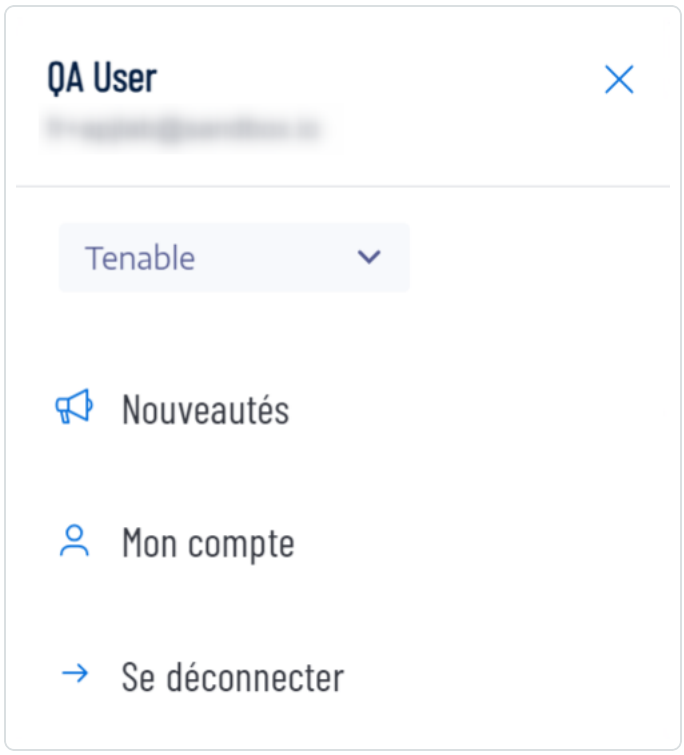
Vous pouvez définir vos préférences utilisateur dans Tenable Identity Exposure.

- Pour sélectionner votre langue :
- Pour sélectionner votre profil :
- Pour changer votre mot de passe :
- Pour sélectionner votre profil :

Pour définir vos préférences :

1. Dans Tenable Identity Exposure, cliquez sur l'icône de votre profil utilisateur dans l'angle supérieur droit.

   Un sous-menu apparaît.



2. Sélectionnez **Mon compte**.

   La page **Préférences** apparaît.

Pour sélectionner votre langue :

a. Dans **Languages** (Langues), cliquez sur la flèche de la liste déroulante pour sélectionner la langue de votre choix.

b. Cliquez sur **Enregistrer**.

   Un message confirme que Tenable Identity Exposure a mis à jour vos préférences. L'interface utilisateur apparaît dans la langue que vous avez sélectionnée.

Pour sélectionner votre profil :

Le passage d'un profil de sécurité à un autre modifie la façon dont Tenable Identity Exposure affiche la configuration des indicateurs et la représentation des données sur les dashboards, les widgets et le Trail Flow.

a. Sous **Préférences**, cliquez sur **Profils**.

b. Dans **Profil préféré**, cliquez sur la flèche déroulante pour sélectionner votre profil par défaut après vous être connecté à Tenable Identity Exposure.

c. Cliquez sur **Enregistrer**.

   Un message confirme que Tenable Identity Exposure a mis à jour vos préférences.

Pour plus d'informations, voir Profils de sécurité.

Pour changer votre mot de passe :

Remarque : les informations de mot de passe ne sont pas disponibles si vous disposez d'une licence Tenable One. Dans ce cas, Tenable Vulnerability Management gère tous vos paramètres d'authentification. Pour plus d'informations, voir Contrôle d'accès dans le Guide de l'utilisateur Tenable Vulnerability Management.

a. Sous **Préférences**, cliquez sur **Identifiants**.

b. Dans le champ **Ancien mot de passe**, saisissez votre ancien mot de passe.

c. Dans le champ **Nouveau mot de passe**, saisissez un nouveau mot de passe. Respectez les règles de complexité suivantes, alignées sur les exigences relatives aux mots de passe des comptes Tenable One :

   - Au moins 12 caractères.
   - Au moins un exemplaire de chacun des éléments suivants :
     - Lettre majuscule (A-Z)
     - Lettre minuscule (a-z)
     - Chiffre (0-9)
     - Caractère spécial (p. ex., !, @, #, $)
   - Ne peut pas contenir la chaîne `verysecure` pour éviter la réutilisation du mot de passe par défaut précédent `verySecure1!`.

d. Dans la zone **Confirmation du nouveau mot de passe**, resaisissez le nouveau mot de passe.

e. Cliquez sur **Enregistrer**.

Un message confirme que Tenable Identity Exposure a changé votre mot de passe.

> **Remarque** : vous ne pouvez pas modifier le mot de passe des comptes connectés par le biais de fournisseurs externes tels que LDAP ou SAML dans Tenable Identity Exposure.

Pour gérer votre clé API :

a. Sous **Préférences**, cliquez sur **Clé API**.

Votre jeton d'accès apparaît dans la zone **Clé API actuelle**.

b. Vous pouvez effectuer les opérations suivantes :

c. Cliquez sur l'icône pour copier la clé API vers le presse-papiers, afin de l'utiliser selon vos besoins.

d. Cliquez sur **Actualiser la clé API** pour générer un nouveau jeton d'accès.

Un message vous demande confirmation.

> **Remarque** : si vous actualisez la clé API, Tenable Identity Exposure désactive le jeton actuel.

Pour plus d'informations, voir Utiliser l'API publique.

Notifications

Dans la partie supérieure droite de la page d'accueil de Tenable Identity Exposure, figurent une icône de cloche et un badge compteur qui signalent les alertes d'attaque et/ou les alertes d'exposition en attente dont vous devez prendre connaissance. Lorsqu'il reçoit de nouvelles alertes, Tenable Identity Exposure augmente le compteur du badge de notification.

	**Bleu**	Alertes d'exposition
	Rouge	Alertes d'attaque

Pour afficher les alertes :

1. Dans Tenable Identity Exposure, cliquez sur l'icône de cloche.

Le volet **Alertes** apparaît.

2. Effectuez l'une des actions suivantes :
    - Cliquez sur l'onglet **Alertes d'exposition** pour afficher les alertes d'exposition.
    - Cliquez sur l'onglet **Alertes d'attaque** pour afficher les alertes d'attaque.

      La liste des alertes associées apparaît.

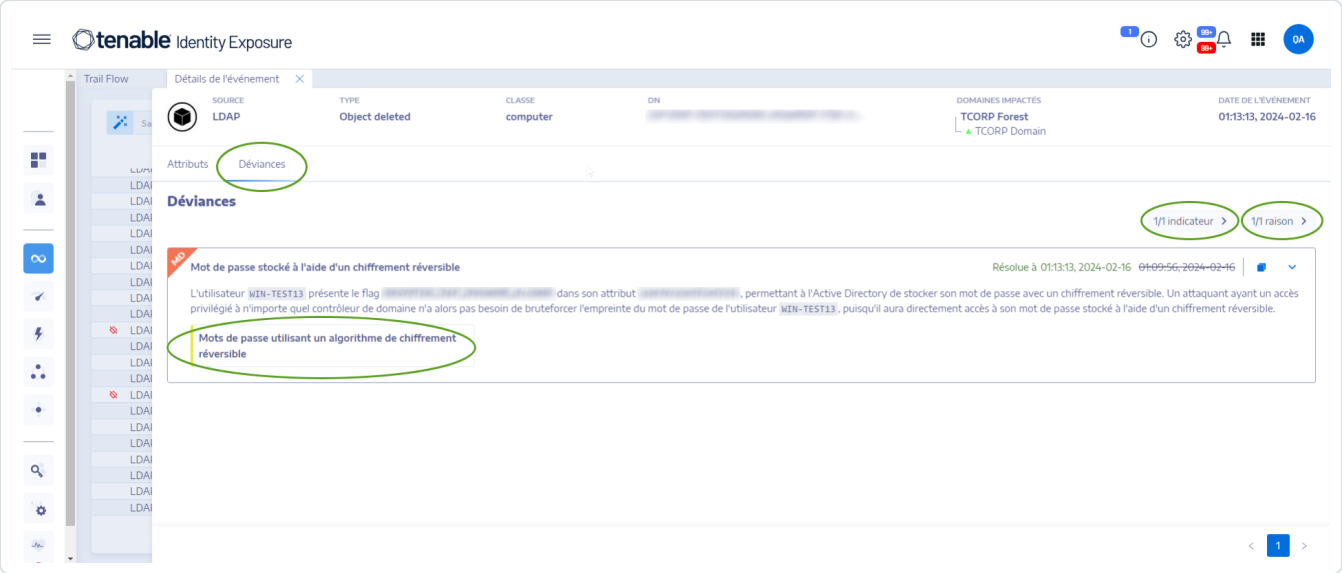
Pour afficher un événement associé à une alerte :

1. Sélectionnez une alerte dans la liste et cliquez sur **Actions** > **Voir la déviance**.

   Le volet Détails de l'événement apparaît avec les informations suivantes :
    - Source (collecteur d'événements)
    - Type d'objet
    - Fichier
    - Chemin d'accès
    - Domaines impactés
    - Date
    - Liste d'attributs avec leurs valeurs au moment de l'événement et leur valeur actuelle

2. Cliquez sur l'onglet **Déviances**.

   Le volet **Déviances** apparaît avec la liste des déviances associées à l'événement.



3. Cliquez sur **n/n indicateurs** pour afficher le volet de l'indicateur d'exposition qui a déclenché l'alerte.
4. Cliquez sur **n/n raisons** pour afficher les raisons de l'alerte.
5. Cliquez sur la flèche pour développer ou réduire les informations relatives à l'alerte.
6. Cliquez sur le nom de l'indicateur pour afficher la page Détails de l'indicateur.

Pour archiver l'alerte :

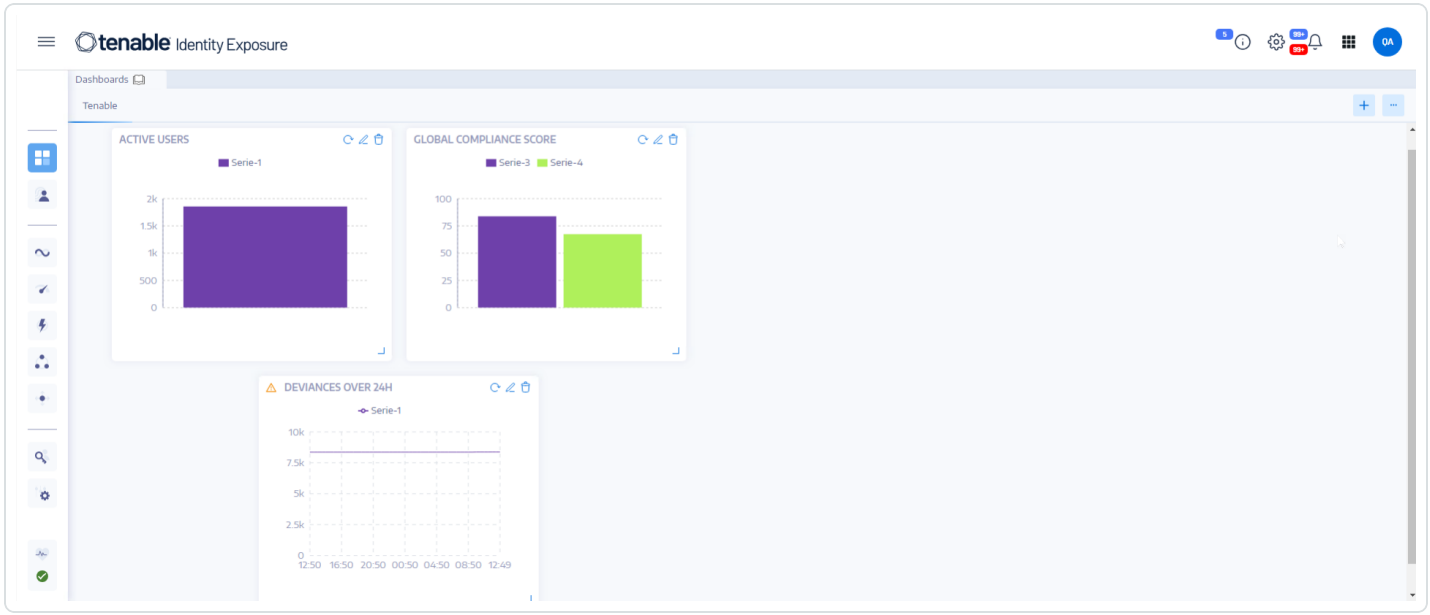
Après avoir affiché l'alerte, vous pouvez l'archiver.

1. Dans la liste des alertes du volet **Alertes**, cochez la case de l'alerte à archiver.
   - Si vous le souhaitez, vous pouvez cocher la case **n/n objets sélectionnés** au bas du volet pour sélectionner toutes les alertes simultanément.
2. Au bas du volet, cliquez sur **Sélectionner une action** > **Archiver**.
3. Cliquez sur **OK**.

Dashboards

Les dashboards vous permettent de visualiser des données et des tendances sur la sécurité de votre infrastructure Active Directory. Vous pouvez les personnaliser avec des widgets pour afficher des graphes et des compteurs selon vos besoins.

Le dashboard Tenable Identity Exposure fait office de centre de commande en temps réel pour la sécurité de l'infrastructure Active Directory (AD) de votre organisation. Il fournit un aperçu complet (une vue centralisée en temps réel) de votre paysage d'identité, mettant en évidence les vulnérabilités critiques et les vecteurs d'attaque potentiels pour permettre une atténuation proactive des risques.



Fonctionnalités clés du dashboard

- **Vue d'ensemble** : vérifiez en un clin d'œil l'état de la sécurité de votre infrastructure grâce à des métriques clés bien en vue telles que le score de conformité, les risques principaux et les tendances des activités utilisateur.
- **Informations détaillées en cascade** : approfondissez des domaines spécifiques à l'aide de widgets interactifs qui décomposent les facteurs de risque par sévérité, catégorie d'utilisateurs et d'autres critères pertinents.
- **Focus personnalisable** : créez des dashboards personnalisés en fonction de vos priorités, en utilisant des modèles prédéfinis ou en créant vos propres mises en page. Par exemple, pour créer un dashboard des erreurs de configuration les plus courantes par rapport à des IoE récurrents communs :

    - S'assurer de la cohérence de SDProp
    - Contrôleurs de domaine gérés par des utilisateurs mal intentionnés
    - Délégation Kerberos dangereuse
- **Surveillance en temps réel** : restez informé des menaces émergentes et des activités suspectes grâce à des mises à jour et des alertes en continu.
- **Informations exploitables** : profitez de recommandations pratiques en matière de remédiation, hiérarchisées en fonction de la sévérité et de l'impact potentiel.

Widgets

Dans les dashboards, les widgets permettent de visualiser vos données Active Directory sous forme d'histogrammes, de graphiques en courbes et de compteurs. Vous pouvez personnaliser les widgets pour afficher des informations spécifiques et les déplacer en les faisant glisser sur le dashboard.

Vous pouvez ajouter des widgets à un dashboard que vous venez de créer ou à un dashboard existant.

Pour ajouter un widget à un dashboard :

1. Dans Tenable Identity Exposure, cliquez sur  ou sur **Dashboards**. Cette page s'ouvre également par défaut dans Tenable Identity Exposure.
2. Sur le volet Dashboards, sélectionnez l'onglet Dashboard.
3. Vous pouvez effectuer l'une des opérations suivantes :
    - Si le dashboard est vide : cliquez sur **Ajouter des widgets**.
    - Si le dashboard contient déjà des widgets :  > **Ajouter un widget sur le dashboard actuel** dans l'angle supérieur droit.

      Le volet **Ajouter un widget** apparaît.

4. Cliquez sur une tuile pour sélectionner l'une des options suivantes :
    - Histogramme
    - Graphique linéaire
    - Compteur
5. Dans la zone **Nom du widget**, saisissez le nom du widget.
6. Sous **Configuration du widget**, dans la zone **Type de données**, cliquez sur la flèche dans la liste déroulante pour sélectionner l'une des options suivantes :
    - Nombre d'utilisateurs : nombre d'utilisateurs actifs pour le domaine.
    - Nombre d'éléments déviants : nombre de déviances ou de violations de sécurité détectées.
    - Score de conformité : score de 0 à 100 que Tenable Identity Exposure détermine en calculant le nombre de déviances détectées et leurs niveaux de sévérité.
    - Durée (pour les graphiques en courbes) : cliquez sur la flèche dans la liste déroulante pour sélectionner la durée à afficher.

7. Sous **Configuration des datasets** :

Configuration des datasets	
Statut (nombre d'utilisateurs)	Sélectionnez Actif, Inactif ou Tout.
Indicateurs	a. Cliquez sur **Indicateurs** pour sélectionner un ou plusieurs indicateurs. Le volet **Indicateurs d'exposition** apparaît. b. Sélectionnez un ou plusieurs indicateurs dans la liste. Vous pouvez aussi : ■ Saisir un nom d'indicateur dans la zone de recherche. ■ Sélectionnez tous les indicateurs. ■ Sélectionner tous les indicateurs d'un niveau de sévérité spécifique (critique, élevé, moyen ou faible). c. Cliquez sur **Filtrer sur la sélection**.
Domaines	a. Cliquez sur **Domaines** pour sélectionner un ou plusieurs domaines. Le volet **Forêts et domaines** apparaît. b. Sélectionnez un domaine dans la liste. Vous pouvez aussi : ■ Saisir un nom de domaine dans la zone de recherche. ■ Sélectionner tous les domaines. c. Cliquez sur **Filtrer sur la sélection**.

8. Dans la zone **Nom du dataset**, saisissez le nom du dataset.

9. Sélectionnez le domaine du widget.

   Vous pouvez aussi saisir un nom de domaine dans la zone de recherche.

10. Cliquez sur **Filtrer sur la sélection**.
11. Vous pouvez aussi cliquer sur **Ajouter un dataset** pour ajouter un autre dataset avec différentes options pour le widget.
12. Cliquez sur **Ajouter**.

    Un message confirme que Tenable Identity Exposure a ajouté le widget.

Pour modifier un widget :

1. Dans Tenable Identity Exposure, cliquez sur **Dashboards**.
2. Sélectionnez le dashboard qui contient le widget à modifier.
3. Sélectionnez le widget.
4. Cliquez sur l'icône dans l'angle supérieur droit du widget.

   Le volet **Modifier un widget** apparaît.

5. Modifiez selon vos besoins.
6. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour le widget.

Pour actualiser un widget :

1. Sélectionnez le widget.
2. Cliquez sur l'icône dans l'angle supérieur droit du widget.

   Le widget s'actualise.

Pour supprimer un widget :

1. Dans Tenable Identity Exposure, cliquez sur **Dashboards**.
2. Sélectionnez le dashboard qui contient le widget à supprimer.

3. Sélectionnez le widget.
4. Cliquez sur l'icône .

   Le volet Retirer un widget apparaît. Un message demande de confirmer la suppression.
5. Cliquez sur **OK**.

   Un message confirme que Tenable Identity Exposure a supprimé le widget du dashboard.

Voir aussi

- Dashboards

Centre d'exposition

Le **Centre d'exposition** est une fonctionnalité de Tenable Identity Exposure qui améliore la posture de sécurité des identités de votre organisation. Il identifie les faiblesses et les mauvaises configurations sur votre surface de risque d'identité, et couvre aussi bien les systèmes d'identité sous-jacents, tels qu'Entra ID, que les identités au sein de ces systèmes.

L'expérience utilisateur de cette fonctionnalité s'articule autour de trois concepts interdépendants : la **vue d'ensemble de la cyber-exposition**, les **instances d'exposition** et les **détections**. Tenable Research prend en charge ces concepts avec **un nouveau moteur de sécurité** et des indicateurs d'exposition (IoE) conçus spécialement pour optimiser leurs fonctionnalités.

- Similaire à la vue des indicateurs d'exposition (IoE) dans Tenable Identity Exposure, la **vue d'ensemble de la cyber-exposition** représente les faiblesses ou les mauvaises configurations potentielles que des attaquants pourraient exploiter. Il s'agit de descriptions générales de risques de sécurité, par exemple « comptes utilisateur inactifs » ou « autorisations d'accès mal configurées ». Les IoE mettent en évidence les zones d'exposition de manière proactive pour offrir aux organisations une vue complète de leur posture de sécurité.
- Les **instances d'exposition** sont des occurrences spécifiques de ces faiblesses générales. Par exemple, la faiblesse générale liée aux « comptes utilisateur inactifs » peut répondre à un scénario spécifique, tel que « comptes utilisateur inactifs depuis plus de 30 jours dans le service marketing ».
- Les **détections** correspondent aux résultats d'une analyse des instances d'exposition par rapport aux données réelles de diverses sources de données d'identité. Une détection

représente un problème de sécurité sur un asset impacté, identifié de manière unique par des attributs tels que l'utilisateur, le groupe et le rôle. Par exemple, si un compte utilisateur est inactif pendant une durée supérieure au seuil spécifié dans l'instance d'exposition, il sera signalé comme une détection.

Le processus commence par appliquer en continu une bibliothèque de faiblesses à vos fournisseurs d'identité par le biais de scans.

Tenable Research fournit les faiblesses par défaut et les met à jour en continu pour s'ajuster au paysage des menaces. Ces faiblesses, adaptées à vos besoins spécifiques dans les instances d'exposition, génèrent des détections, qui sont ensuite présentées avec un score de sévérité et des directives de remédiation. En tirant parti de cette fonctionnalité, Tenable Identity Exposure aide les organisations à atténuer de manière proactive les risques de sécurité.

Remarque : le Centre d'exposition ne présente que les faiblesses prises en charge par le nouveau moteur de sécurité. Les indicateurs d'exposition (IoE) générés par l'ancien moteur de sécurité n'apparaissent pas ici. Cependant, les IoE actuellement liés à Active Directory (AD) restent visibles sur la page Indicateurs d'exposition dans Tenable Identity Exposure.

Conditions préalables

- Pour utiliser le **Centre d'exposition**, vous devez activer la fonctionnalité dans les paramètres Tenable Identity Exposure.
- Voir Activation de la prise en charge de « Identités 360 », « Centre d'exposition » et « Microsoft Entra ID » pour obtenir des instructions.

Voir aussi

- Vue d'ensemble de la cyber-exposition
- Instances d'exposition

Vue d'ensemble de la cyber-exposition

Tenable Identity Exposure offre une visibilité complète sur les faiblesses et les mauvaises configurations de divers fournisseurs d'identité, notamment Active Directory (AD) et Entra ID.

En scannant et en identifiant en continu les faiblesses critiques dans les comptes avec privilèges, les stratégies de mots de passe, les configurations de délégation, etc., Tenable Identity Exposure permet aux organisations de combler les failles de sécurité de manière proactive.

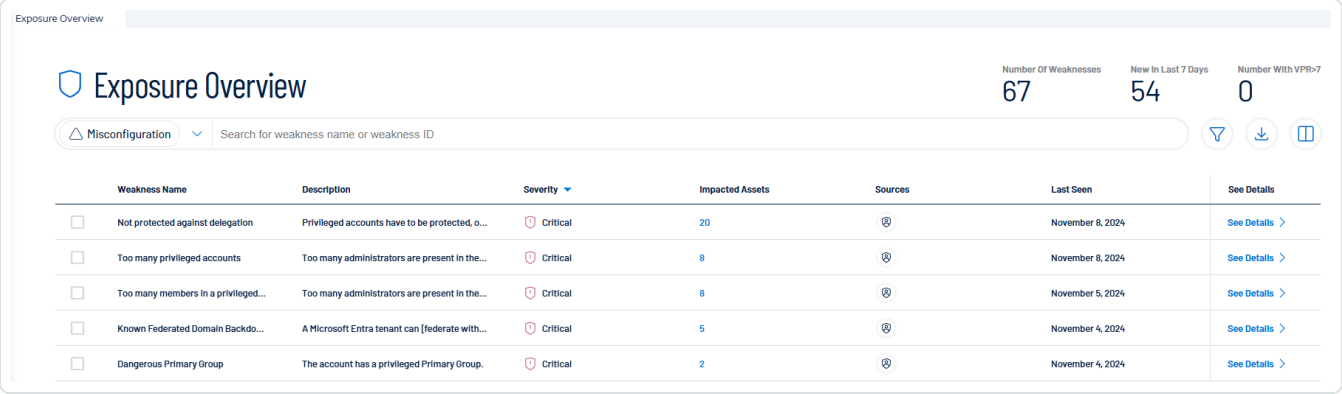
Cet aperçu vous permet de prioriser les problèmes en fonction de leur sévérité, des assets impactés et des détections récentes, garantissant une approche ciblée et efficace de la gestion de la sécurité des identités.

Pour accéder à la page **Vue d'ensemble de la cyber-exposition** :

1. Dans le volet de navigation de gauche de Tenable Identity Exposure, cliquez sur l'icône du Centre d'exposition .

2. Dans le sous-menu, cliquez sur **Vue d'ensemble de la cyber-exposition**.

   La page **Vue d'ensemble de la cyber-exposition** apparaît.



Informations d'en-tête

- **Nombre de faiblesses** : affiche le nombre total de faiblesses détectées.
- **Nouvelles au cours des 7 derniers jours** : met en évidence les nouvelles faiblesses détectées la semaine passée.

Liste des faiblesses

Les colonnes suivantes apparaissent dans la liste des faiblesses :

- **Nom de la faiblesse** : répertorie les faiblesses ou mauvaises configurations spécifiques détectées. Exemple : « Non protégé contre la délégation », « Nombre de membres privilégiés trop élevé », etc.
- **Description** : donne une brève explication du problème. Exemple : « Les comptes privilégiés doivent être protégés… », « Trop de comptes administrateurs sont présents… ».
- **Sévérité** : affiche la criticité de chaque faiblesse (critique, élevée, moyenne, faible).
- **Assets impactés** : affiche le nombre d'assets affectés par chaque faiblesse.
- **Sources** : les systèmes ou plateformes qui ont détecté les données. Ces données peuvent provenir de plusieurs produits.
- **Dernière détection** : affiche la dernière fois que chaque faiblesse a été détectée ou signalée. Exemple : « 10 septembre 2024 », « 29 septembre 2024 ».
- **Afficher les détails** : vous permet d'afficher des informations supplémentaires sur chaque faiblesse.

> **Conseil** : la flèche « Afficher les détails » vous redirige vers Tenable Inventory. Pour plus de détails sur une faiblesse spécifique, voir Weaknesses (Faiblesses) dans Tenable Inventory.

> **Remarque** : la fonctionnalité Vue d'ensemble de la cyber-exposition affiche actuellement des données liées aux faiblesses en fonction du **profil Tenable par défaut** et ne reflète pas automatiquement le **statut des déviances sur les objets AD que vous avez ajoutés à la liste blanche dans d'autres profils**.
>
> Par conséquent :
>
> - Si vous avez **ajouté un objet AD à la liste blanche** pour un indicateur d'exposition spécifique (p. ex., « Membre d'un groupe d'administrateurs natif »), **la Vue d'ensemble de la cyber-exposition le signalera toujours comme une faiblesse de sécurité si le profil par défaut l'a identifié comme déviant**.
> - Vous pouvez ainsi avoir l'impression que le problème n'a pas été résolu, même si l'objet a déjà été ajouté à la liste blanche sous un profil différent.
> - Si une mesure de remédiation (telle que la suppression de l'appartenance à un groupe) est prise sur la base des indications de la Vue d'ensemble de la cyber-exposition, l'objet disparaît de la vue. Mais si l'objet était déjà sur liste blanche ailleurs, il est possible que cette mesure ait été facultative.

Options de recherche, de filtrage, d'exportation et d'affichage des colonnes

Filtrer

Dans **Vue d'ensemble de la cyber-exposition**, une fonction de filtrage permet de limiter ou d'affiner les données affichées en appliquant des critères spécifiques.

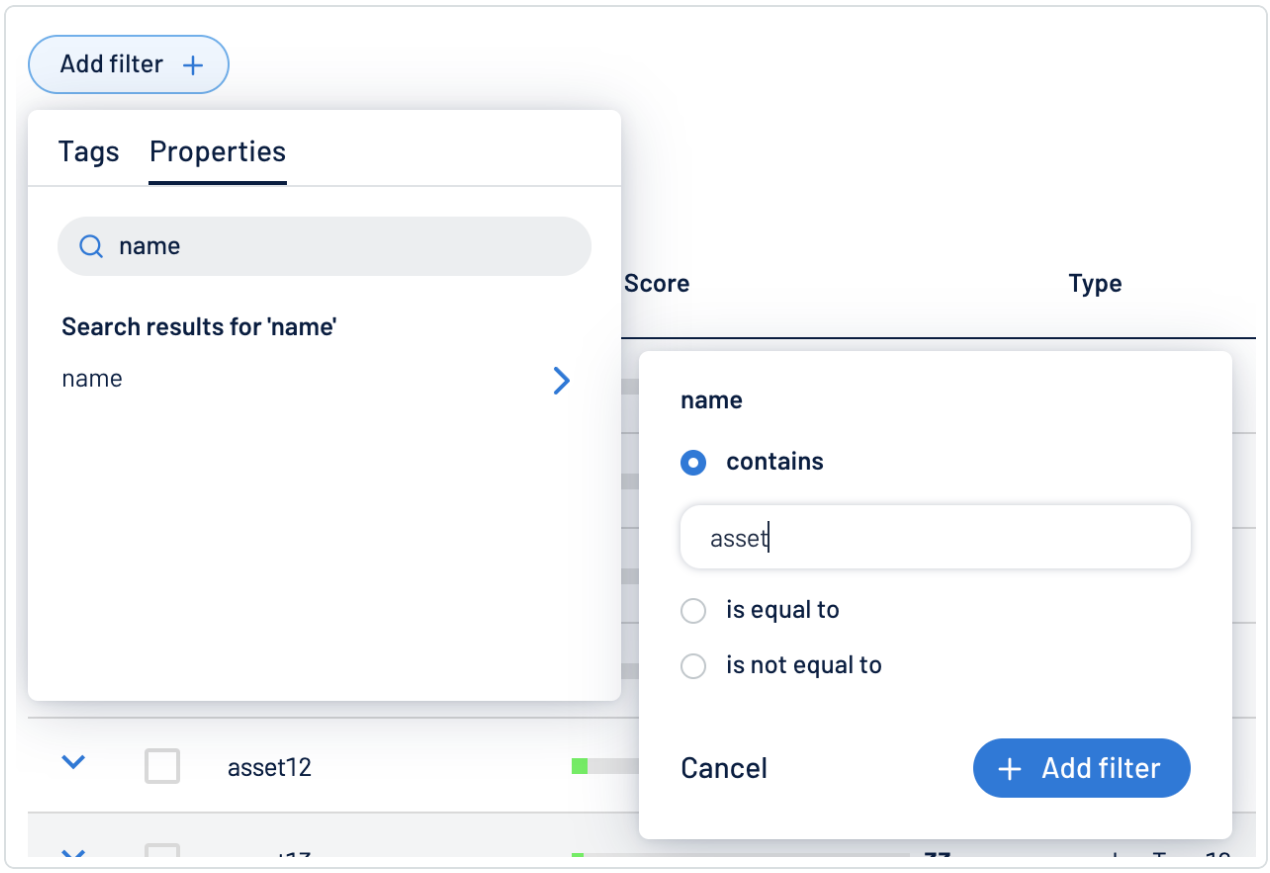
Pour appliquer un filtre à la liste des faiblesses :

1. Dans l'en-tête de la page **Vue d'ensemble de la cyber-exposition**, cliquez sur l'icône .

   Le bouton Ajouter un filtre apparaît.

2. Cliquez sur **Ajouter un filtre +**.

   Un menu apparaît.



3. Effectuez l'une des actions suivantes :
    - Pour effectuer une recherche par tag dans la liste des faiblesses, cliquez sur **Tags** (valable uniquement avec la licence Tenable One et géré dans Tenable Inventory).
    - Pour effectuer une recherche par propriété dans la liste des faiblesses, cliquez sur **Propriétés**.
4. Dans la zone de recherche, saisissez les critères de recherche que vous souhaitez appliquer.

    Tenable Inventory affiche une liste d'options en fonction de vos critères.
5. Cliquez sur le tag ou la propriété à utiliser pour filtrer la liste des faiblesses.

    Un menu apparaît.
6. Sélectionnez le mode d'application du filtre. Par exemple, si vous souhaitez rechercher une faiblesse dont le nom est « Weakness14 », sélectionnez le bouton radio « contient » et saisissez « Weakness14 » dans la zone de texte.
7. Cliquez sur **Ajouter un filtre**.

    Le filtre apparaît au-dessus de la liste des faiblesses.
8. Répétez ces étapes pour chaque filtre supplémentaire que vous souhaitez appliquer.
9. Cliquez sur **Appliquer les filtres**.

    La page filtre la liste des identités selon les critères désignés.

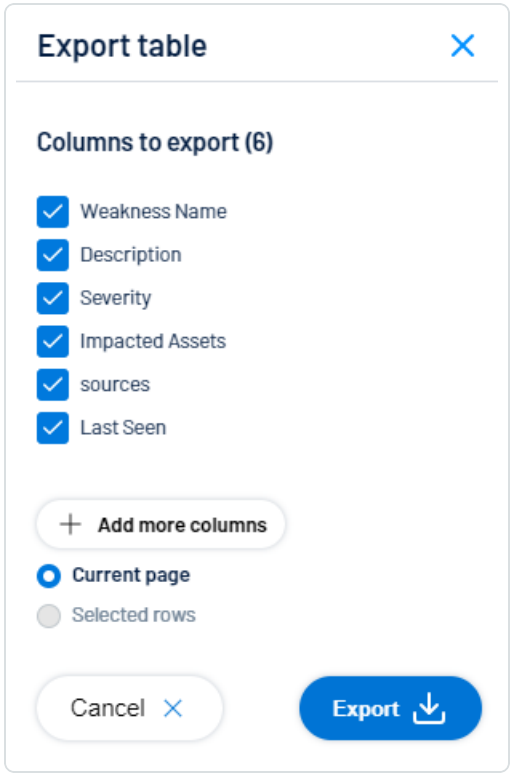
Exporter

Vous pouvez exporter les données affichées dans le tableau au format Excel.

Pour exporter des données :

1. Dans l'en-tête de la page **Vue d'ensemble de la cyber-exposition**, cliquez sur l'icône .
2. Dans la fenêtre Exporter le tableau, sélectionnez les colonnes à exporter. Vous avez la

possibilité d'exporter la page actuelle ou les lignes sélectionnées.



3. Cliquez sur **Exporter**.

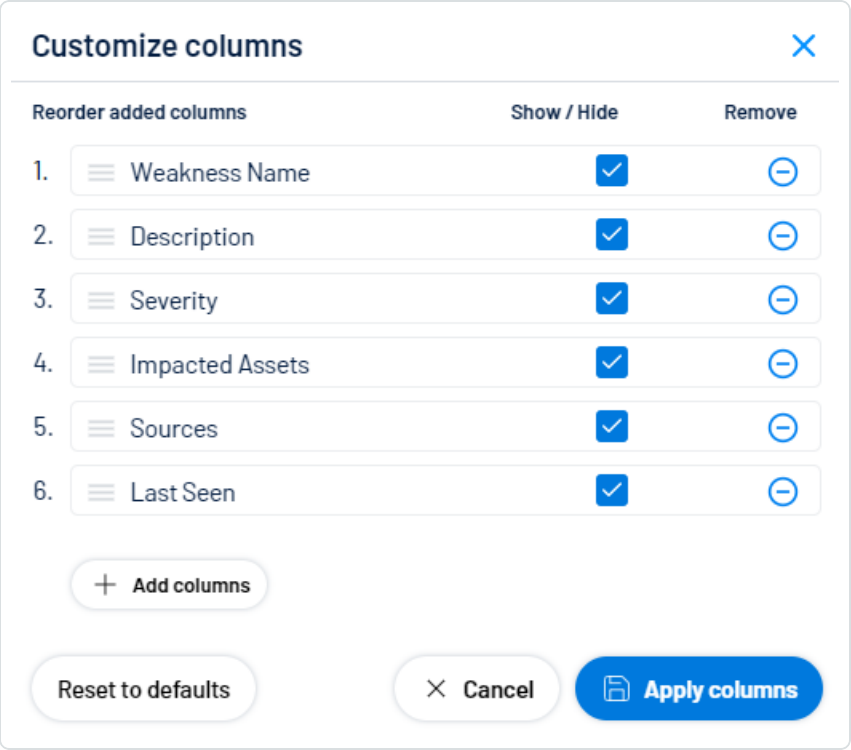
Personnaliser les colonnes

Vous pouvez ajouter, supprimer ou réorganiser des colonnes pour adapter l'affichage à vos préférences. Pour annuler les modifications, vous pouvez toujours rétablir les paramètres par défaut.

Pour personnaliser l'affichage des colonnes :

1. Dans l'en-tête de la page **Vue d'ensemble de la cyber-exposition**, cliquez sur .

   La fenêtre Personnaliser les colonnes apparaît.



2. Facultatif :
    - Dans la section **Réorganiser les colonnes ajoutées**, cliquez sur n'importe quel nom de colonne et faites-le glisser pour réorganiser les colonnes.
    - Dans la section **Afficher/Masquer**, cochez/décochez les cases pour afficher ou masquer des colonnes du tableau.
    - Dans la section **Retirer**, cliquez sur (-) pour supprimer définitivement une colonne du tableau.
    - Pour ajouter des colonnes au tableau, cliquez sur **Ajouter des colonnes**.

      La fenêtre **Ajouter des colonnes au tableau** apparaît.

        - (Facultatif) Utilisez la barre de recherche pour rechercher une propriété de colonne.

          La liste des propriétés de colonne est mise à jour en fonction de votre requête de recherche.
        - Cochez la case à côté des colonnes que vous souhaitez ajouter au tableau.

- Cliquez sur **Ajouter**.

  La colonne apparaît dans la fenêtre Personnaliser les colonnes.

3. Cliquez sur **Appliquer les colonnes**.

   Tenable enregistre les modifications apportées aux colonnes du tableau.

Affichage par défaut des colonnes

La disposition par défaut des colonnes met en avant les données clés tout en offrant une certaine flexibilité en matière de personnalisation.

- **Nom de la faiblesse**
- **Description**
- **Sévérité**
- **Assets impactés**
- **Sources**
- **Dernière détection**

Pour rétablir l'affichage par défaut des colonnes :

- Cliquez sur **Rétablir les réglages par défaut** pour réinitialiser toutes les colonnes à leurs valeurs par défaut.

Voir aussi

- Instances d'exposition

Instances d'exposition

La page **Instances d'exposition** affiche une liste des occurrences spécifiques de faiblesses identifiées.

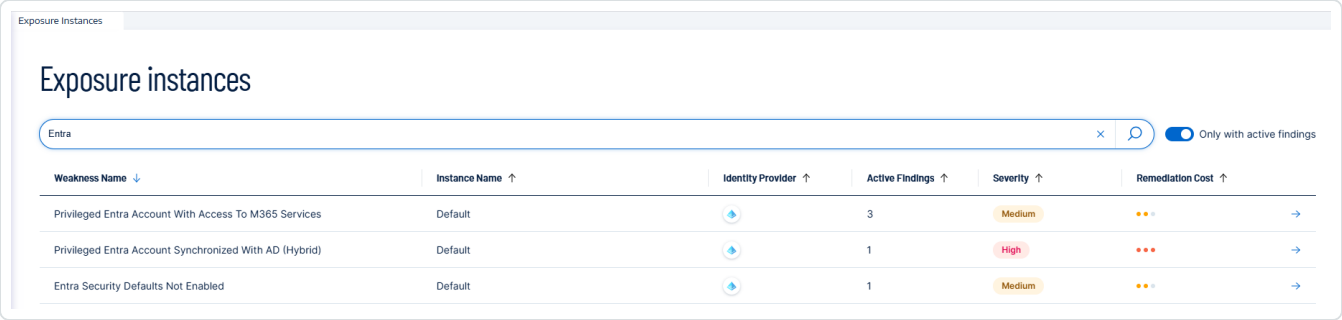
Pour accéder à la page **Instances d'exposition** :

1. Dans le volet de navigation de gauche de Tenable Identity Exposure, cliquez sur l'icône du Centre d'exposition

.

2. Dans le sous-menu, cliquez sur **Instances d'exposition**.

   La page **Instances d'exposition** s'affiche.



Informations générales

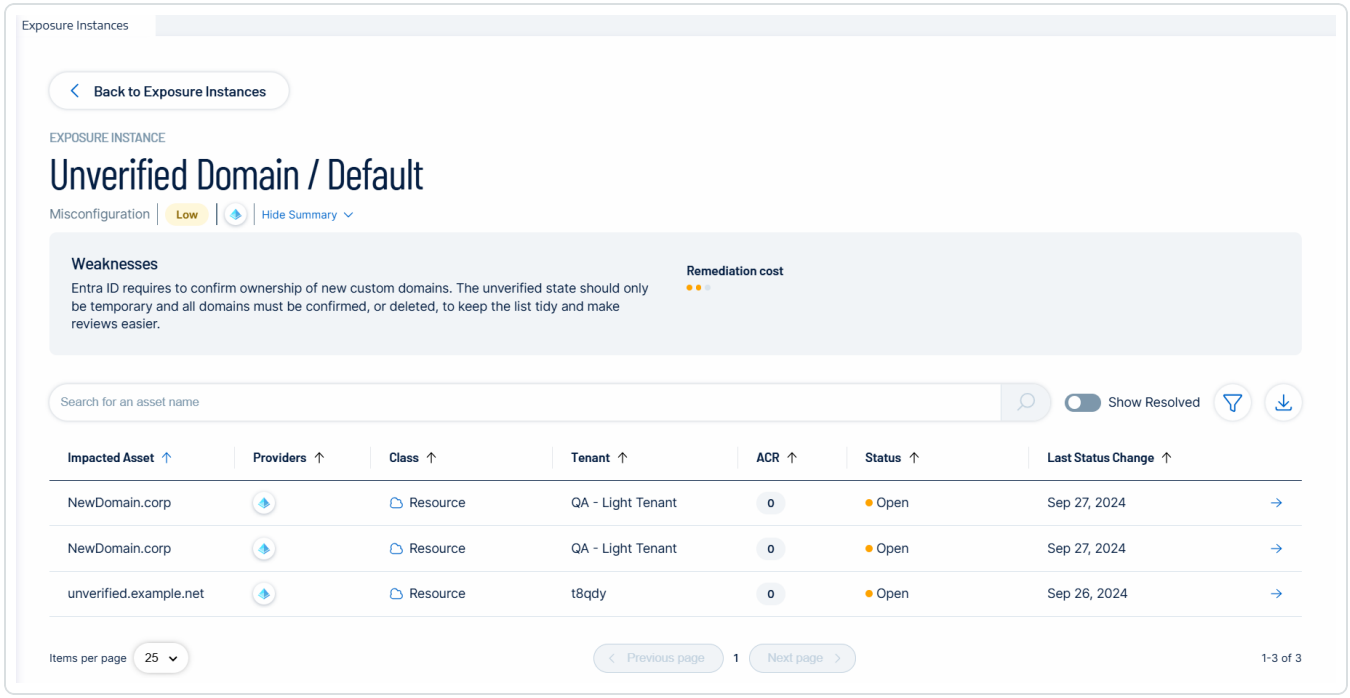
Cette page affiche un tableau répertoriant toutes les instances d'exposition accompagnées des informations correspondantes :

- **Nom de la faiblesse** : nom générique de la faiblesse
- **Nom de l'instance** : nom spécifique de cette instance
- **Fournisseur d'identité** : nom du fournisseur d'identité d'où proviennent les données
- **Nombre de détections actives**
- **Sévérité** : indique la criticité de cette faiblesse
- **Coût de la remédiation** : indique l'effort requis pour remédier à cette faiblesse (faible, moyen, élevé)

Informations détaillées

- Pour explorer plus en détail chaque instance d'exposition, cliquez sur la flèche à la fin de la ligne. Une autre page s'ouvre et affiche les informations suivantes pour chaque instance

d'exposition :



Informations d'en-tête

L'en-tête affiche les informations suivantes :

- Le type de faiblesse, tel qu'une mauvaise configuration, et le nom de l'instance (par défaut)
- La sévérité : la sévérité de la faiblesse (faible, moyenne ou élevée)
- La description de la faiblesse : une explication détaillée de la faiblesse et les raisons pour lesquelles elle pose un risque de sécurité.
- Une estimation du coût de la remédiation

Assets impactés

Les assets impactés sont les assets affectés par l'instance d'exposition, accompagnés des détails correspondants :

- Fournisseur
- Type d'asset

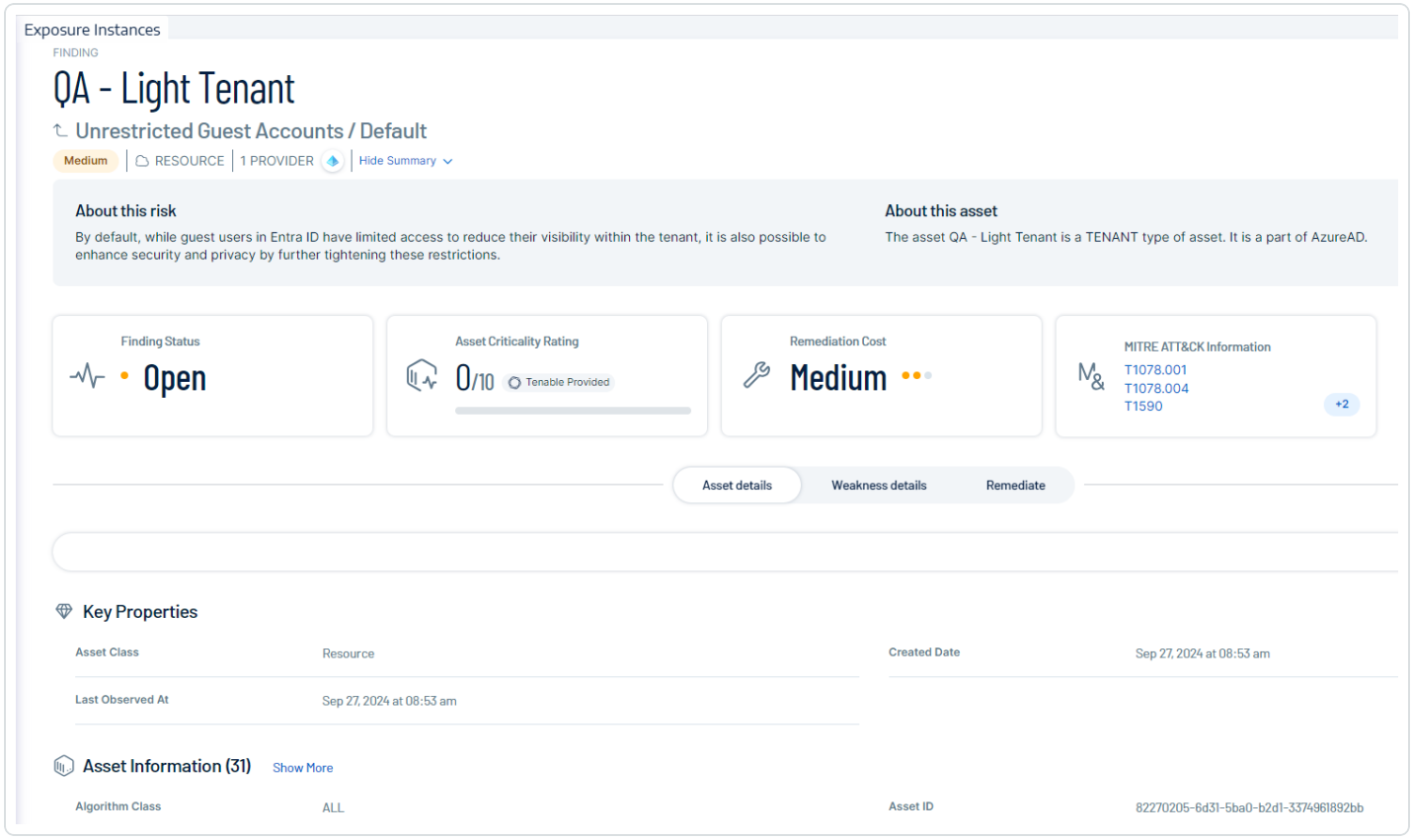
- Tenant : le terme « tenant » est utilisé de manière générique pour désigner les tenants (ou locataires) des fournisseurs d'identité (IDP), même si chaque IDP peut avoir un nom spécifique pour ce concept (par exemple, tenants Entra ID, domaine AD, etc.).
- Classement ACR (Asset Criticality Rating)
- Statut : ouverte, résolue ou réapparue
- Date du dernier changement de statut

Exclusions

Pour des informations complètes, voir Exclusions d'instances d'exposition.

Analyse des détections

Pour afficher la détection associée à l'asset impacté, cliquez sur la flèche à la fin de la ligne. Une autre page s'ouvre et affiche ces informations pour la détection :



Informations d'en-tête

L'en-tête de la page **Détection** affiche les informations suivantes :

- **Nom du tenant**
- Le **nom de la faiblesse** et le nom de l'instance d'exposition associée
- La **sévérité** : la sévérité de la faiblesse (faible, moyenne ou élevée)
- La **classe de l'asset** : la catégorie à laquelle l'asset appartient. Voir Asset Classes (Classes d'assets) pour plus d'informations.
- Le **fournisseur** : le fournisseur d'identité.
- Un **récapitulatif** de l'instance d'exposition
    - La section « À propos de ce risque » donne une brève description de cette faiblesse
    - La section « À propos de cet asset » indique le type d'asset (par exemple, « tenant ») et le fournisseur d'identité

Statuts des détections

Les détections peuvent afficher les statuts suivants :

> **Remarque** : par défaut, la page affiche uniquement les détections ouvertes et réapparues.

- **Ouverte** : ce statut indique un problème de sécurité actif qui nécessite une attention. La faiblesse a été détectée et n'a pas encore été résolue.
- **Résolue** : ce statut montre que la faiblesse précédemment identifiée a bien été résolue. Le problème de sécurité n'est plus actif.

  > **Conseil** : activez le curseur « Afficher les éléments résolus » pour afficher les détections résolues.

- **Réapparue** : ce statut apparaît lorsqu'un problème précédemment résolu a de nouveau été détecté. Cela peut indiquer que la solution était temporaire ou que le problème est réapparu.
- **Exclue** : ce statut apparaît lorsque vous appliquez un filtre affichant les assets impactés auxquels une exclusion a été appliquée.

Classement ACR (Asset Criticality Rating)

Tenable attribue un classement ACR à chaque asset de votre fournisseur d'identité, afin de représenter la criticité relative de l'asset sous la forme d'un entier de 1 à 10. Plus le classement ACR est élevé, plus la criticité est importante. Voir ACR (classement ACR) pour plus d'informations.

Coût de la remédiation

Le coût de la remédiation est une estimation de l'effort nécessaire pour résoudre une faiblesse spécifique, en tenant compte de la combinaison travail humain, complexité et frais potentiels.

Il est classé en trois niveaux :

- Faible : faiblesse relativement facile à résoudre, nécessitant un minimum de temps et de ressources.
- Moyen : faiblesse dont la résolution nécessite un effort modéré.
- Élevé : problèmes complexes dont la résolution peut nécessiter du temps, des ressources ou des changements importants.

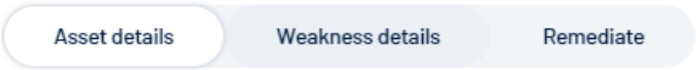
Cette classification permet de prioriser les problèmes à traiter en premier en fonction de leur sévérité et de l'effort requis pour les résoudre.

Informations MITRE ATT&CK

Techniques associées selon le cadre MITRE ATT&CK.

Détails des détections

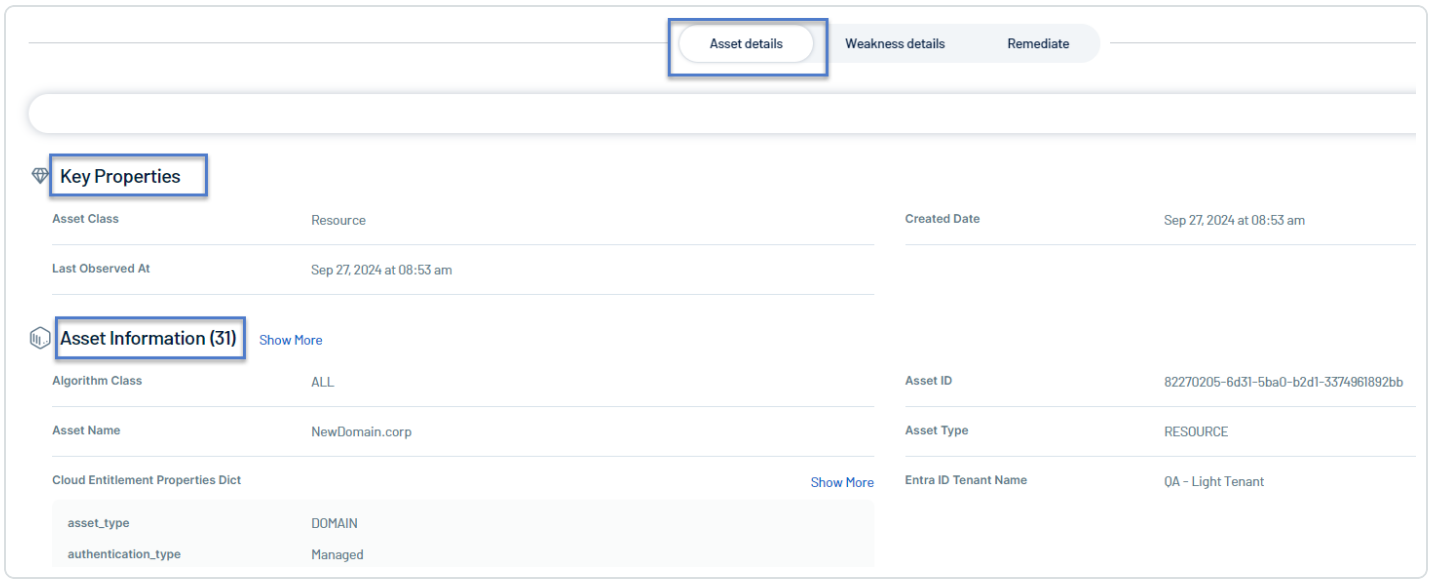
Sous l'en-tête, la page Détections affiche trois onglets pour mettre en évidence les informations suivantes :



- Cliquez sur un onglet pour afficher plus de détails.

Détails de l'asset

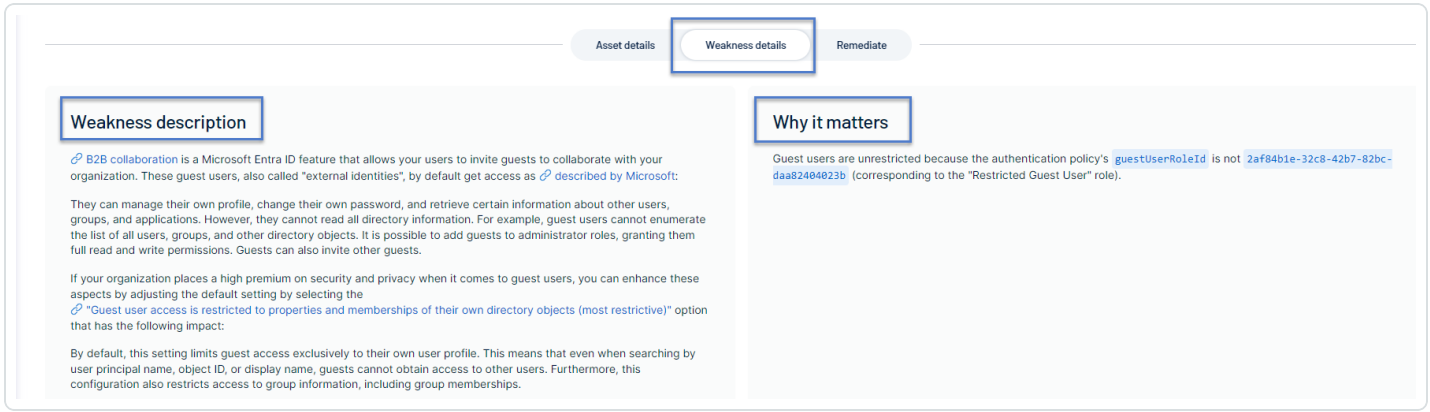
L'onglet « Détails de l'asset » est ouvert par défaut dans la page Détections.



Cette section fournit les informations suivantes :

- **Propriétés clés** – Cette section fournit des détails généraux sur l'asset, tels que sa classe. Elle affiche également la date de création de l'asset et la date de sa dernière observation.
- **Informations sur l'asset** – Cette section contient des attributs plus détaillés de l'asset, issus des informations du fournisseur d'identité.

Détails de la faiblesse

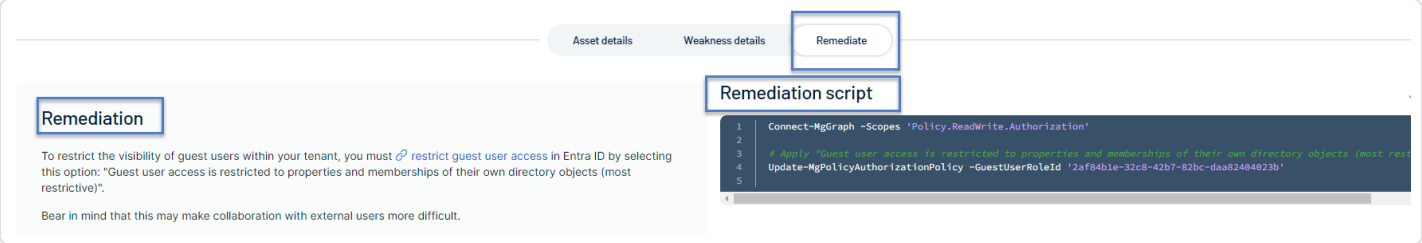


Cette section fournit les informations suivantes :

Description de la faiblesse – En termes simples, cette section explique pourquoi la faiblesse peut poser des risques de sécurité pour vous aider à comprendre et à résoudre les faiblesses.

Pourquoi c'est important : cette section identifie l'occurrence spécifique de cette faiblesse afin que vous puissiez concentrer vos efforts sur sa remédiation.

Remédiation



Cette section vous guide tout au long du processus de remédiation d'une faiblesse.

Directives de remédiation – Les directives textuelles fournissent des instructions pas à pas sur le traitement de la faiblesse identifiée. Ces directives incluent généralement :

- Des instructions détaillées sur la façon de corriger la faiblesse.
- De bonnes pratiques pour prévenir des problèmes similaires à l'avenir.
- Des liens vers de la documentation pertinente ou des ressources supplémentaires.

Scripts de remédiation – Pour certaines détections, des scripts de remédiation automatisés peuvent être disponibles.

> **Remarque** : si aucun script n'est disponible, cela peut être dû au fait que le produit ne peut pas automatiser la remédiation, ou que la remédiation automatique exigerait la mise en œuvre de changements organisationnels dépassant le cadre d'une simple correction technique. Dans ce cas, un message vous indique que seule la remédiation manuelle est possible pour cette détection, et vous devez suivre les directives textuelles.

Avant d'exécuter le script :

- Examinez son contenu pour comprendre les modifications qu'il apportera.
- Adaptez-le à votre environnement si nécessaire.
- Testez le script dans un environnement de pré-production si possible.
- Assurez-vous de disposer des autorisations nécessaires pour exécuter le script.

Conseil : bien que les scripts de remédiation puissent faire gagner du temps, faites toujours preuve de prudence et assurez-vous de comprendre les implications de toute modification automatisée de votre environnement.

Pour exécuter le script de remédiation :

Vous pouvez soit ouvrir une console PowerShell, coller le script de remédiation et l'exécuter directement, soit, si vous préférez, télécharger le script au format .ps1 pour l'exécuter.

1. Recherchez le bouton « Télécharger le script » dans l'onglet Remédiation.
2. Cliquez sur ce bouton pour télécharger le script de remédiation.
3. Exécutez le fichier comme n'importe quel script PowerShell.

Options de recherche, de filtrage et d'exportation

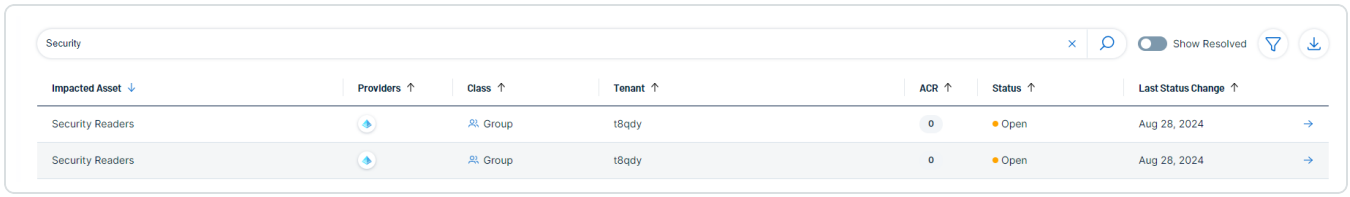
Rechercher

- Vous pouvez rechercher une instance spécifique dans la liste des instances d'exposition par **nom de faiblesse**, **nom d'instance** ou **sévérité**.
  - Dans la zone de recherche, saisissez un terme de recherche (par exemple, « Entra »). La liste affiche toutes les instances qui correspondent aux critères de recherche.



- Vous pouvez rechercher des assets impactés spécifiques dans l'instance d'exposition.

- Dans la zone de recherche, saisissez un **nom d'asset** (par exemple, « Sécurité »). La liste affiche toutes les instances qui correspondent aux critères de recherche.



Filtrer

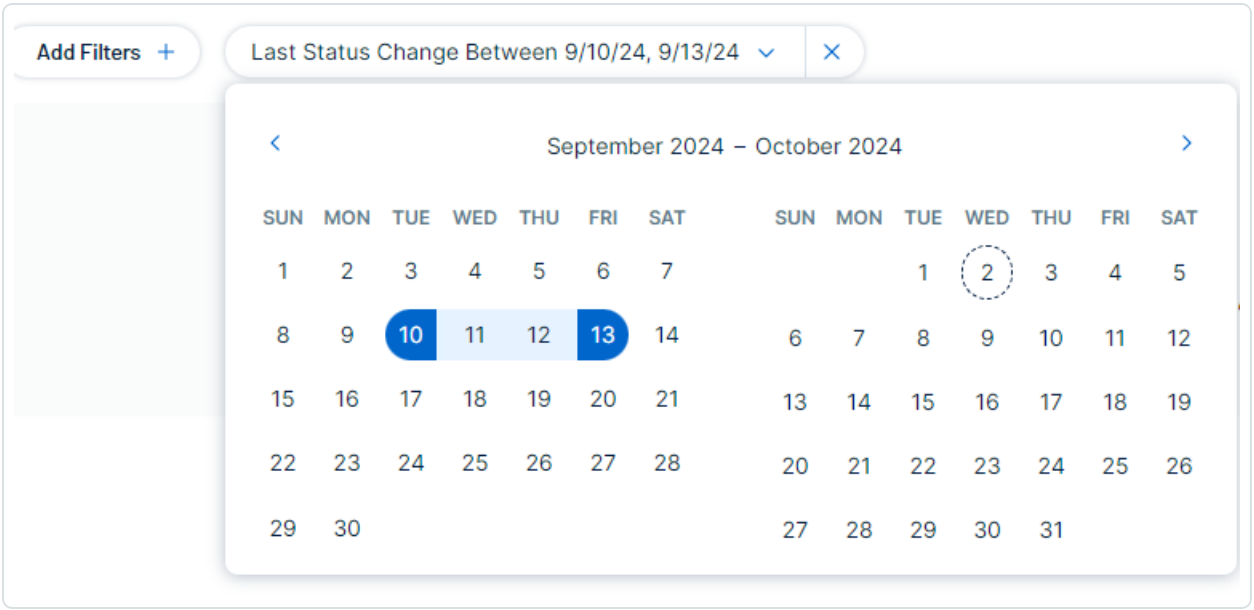
Pour filtrer la liste des faiblesses :

1. Cliquez sur l'icône .

   Le bouton « Ajouter un filtre » apparaît.

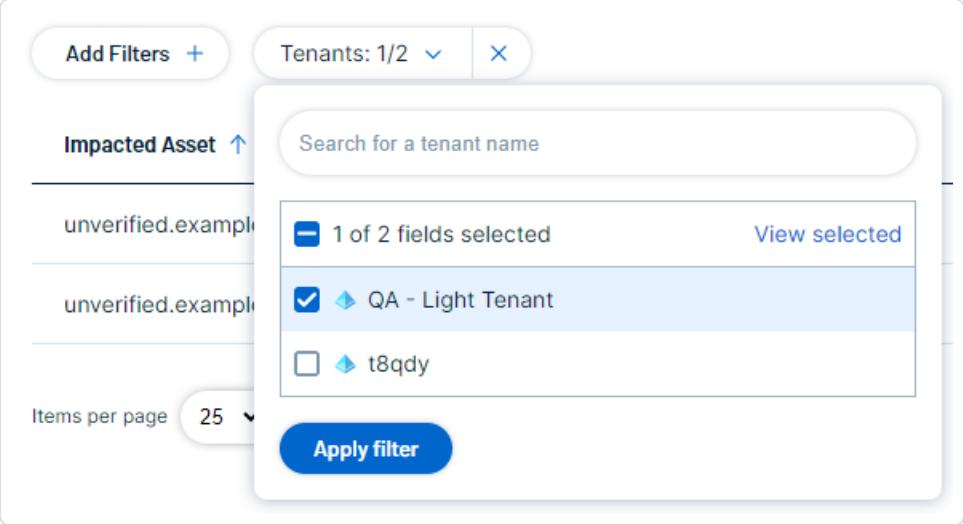
2. Cliquez sur « Ajouter un filtre ». Les options de filtrage suivantes sont disponibles :

   - Par « Dernier changement de statut » : sélectionnez une date dans le sélecteur de date.



   - Par « Tenant » : sélectionnez le nom du tenant. Vous pouvez également rechercher un

locataire spécifique dans la zone de recherche et cliquer sur **Afficher la sélection**.



3. Cliquez sur **Appliquer le filtre**.

Exporter

Vous pouvez exporter la liste des assets impactés par une instance d'exposition au format Excel.

Pour exporter :

- Sur la page des instances d'exposition, cliquez sur l'icône .

Voir aussi

- Vue d'ensemble de la cyber-exposition

Exclusions d'instances d'exposition

Personnalisez vos scans de sécurité grâce aux exclusions d'assets

Toutes les alertes de sécurité ne requièrent pas une action de votre part et tous les assets signalés ne sont pas nécessairement exposés à un risque. Dans certains cas, les systèmes sont configurés de manière à déclencher des alertes, même en l'absence de menace réelle. Cela peut créer du bruit inutile dans vos rapports de sécurité et détourner votre attention des problèmes qui comptent vraiment.

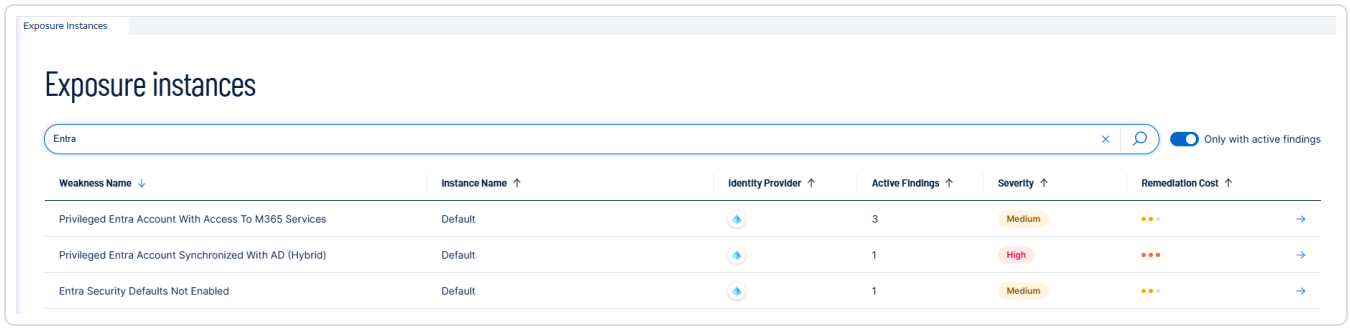
Pour vous aider à vous concentrer sur ce qui compte vraiment, la fonctionnalité **Exclusions** vous permet d'exclure (ou de mettre sur liste d'autorisation) des assets spécifiques afin qu'ils ne soient pas signalés comme affectant certaines faiblesses. L'exclusion des assets sûrs vous permet de contrôler davantage les résultats de vos scans, afin que vos rapports soient clairs, pertinents et exploitables.

Pour accéder à la page Exclusions :

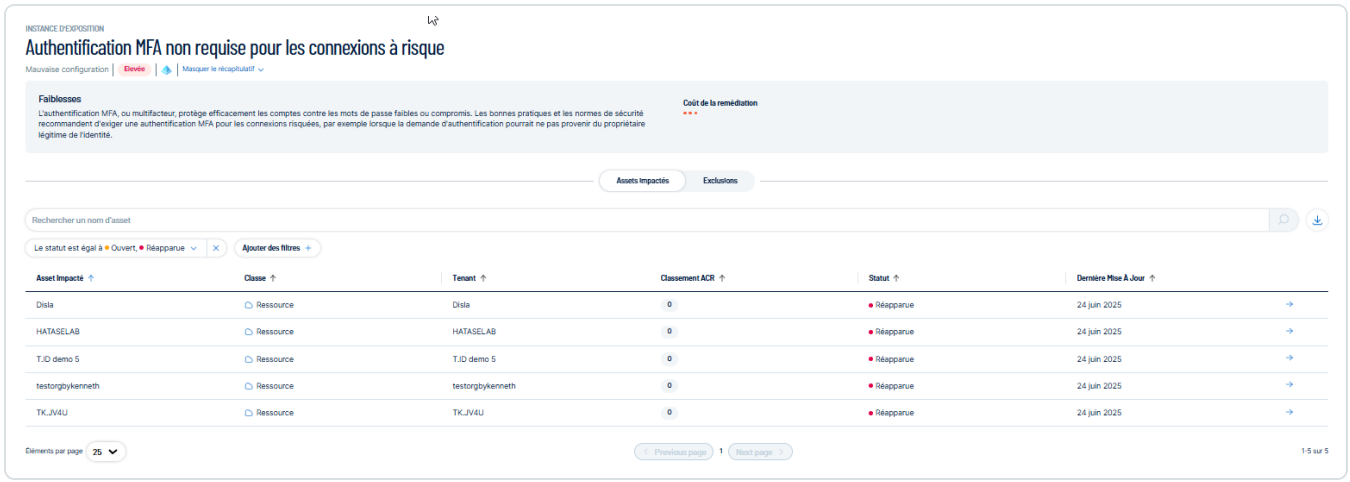
1. Dans le volet de navigation de gauche de Tenable Identity Exposure, cliquez sur l'icône du Centre d'exposition .

2. Dans le sous-menu, cliquez sur **Instances d'exposition**.

   La page **Instances d'exposition** s'affiche.



3. Pour explorer plus en détail chaque instance d'exposition, cliquez sur la flèche à la fin de la ligne. Une autre page s'ouvre et affiche les informations suivantes pour chaque instance d'exposition :



4. Cliquez sur l'onglet **Exclusions**.

   Une page s'ouvre pour afficher une liste des éventuelles exclusions pour cette instance.

Pour créer une exclusion :

1. Cliquez sur **Créer une exclusion**.

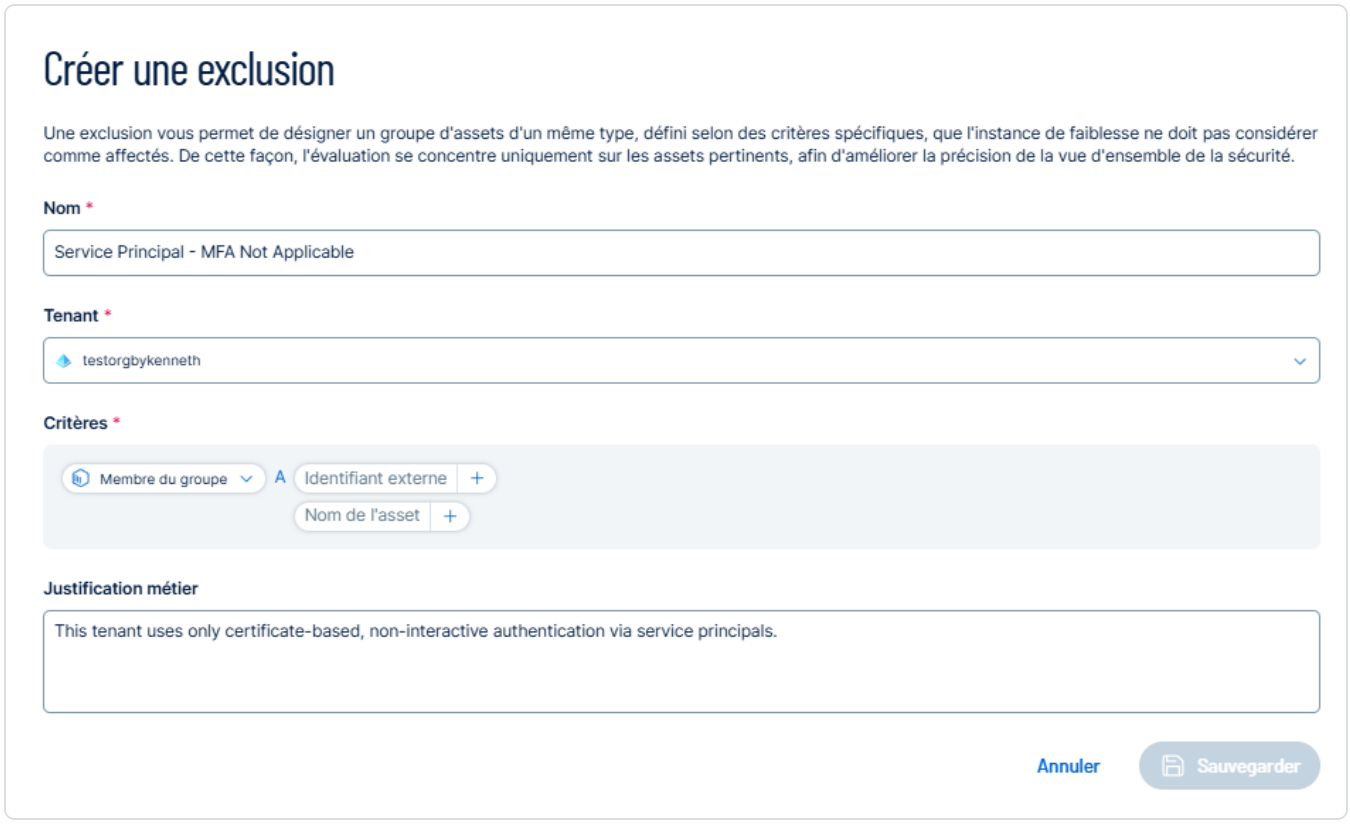
   La fenêtre **Créer une exclusion** s'ouvre.

2. Fournissez les informations suivantes :

Nom	Saisissez un nom intuitif pour l'exclusion.	
Tenant	Cliquez sur la flèche pour afficher la liste déroulante des tenants disponibles et sélectionnez-en un.	
Critères	Selon le type de faiblesse, les informations et les critères associés diffèrent.	
	◦ Dans le menu déroulant **Type d'asset**, sélectionnez le type d'asset à exclure : ◦ Cliquez sur **+** à côté du nom de l'attribut et attribuez des valeurs qui identifient l'asset à exclure. Tenable Identity Exposure propose des valeurs suggérées correspondant à l'asset impacté que vous avez sélectionné. ◦ Cliquez sur **Sélectionner**.	
	Type d'asset	**Attributs**
	Tenant	Nom d'asset, Identifiant externe
	Rôle privilégié	Nom d'asset, Identifiant externe, le Rôle est Privilégié

	Compte	Connexion au compte, Statut du compte, Classement ACR, Nom de l'asset, Identifiant de sécurité Entra ID, Identifiant externe, Indicateur MFA, Type d'utilisateur
	Utilisateur	
Justification métier	Saisissez une description de cette exclusion pour y apporter du contexte.	

Cliquez sur **Enregistrer** pour créer l'exclusion.

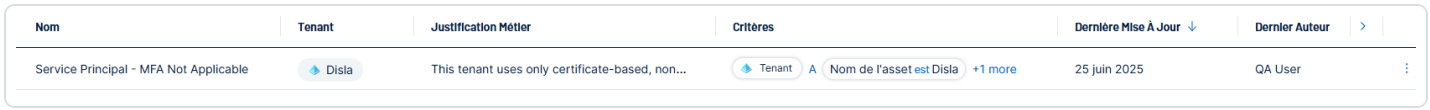


Un message apparaît indiquant que Tenable Identity Exposure a créé l'exclusion et qu'elle sera prise en compte lors de la prochaine analyse de sécurité.

Remarque : la nouvelle exclusion n'est pas appliquée immédiatement. Par conséquent, le statut des assets exclus n'est mis à jour qu'une fois le scan suivant effectué.

Pour afficher les exclusions :

La liste **Exclusions** est triée en plaçant en haut l'élément mis à jour le plus récemment. Par conséquent, toute nouvelle exclusion que vous créez apparaît en premier.



Nom	Description
Nom	Affiche le nom donné à l'exclusion.
Tenant	Tenant associé à l'asset impacté dans l'exclusion
Justification métier	Motif de l'exclusion
Critères	Affiche les critères et les attributs de l'exclusion sous forme de capsules qui sont automatiquement redimensionnées en fonction de la largeur des colonnes. Si les attributs ne sont pas tous visibles, cliquez sur **plus** pour ouvrir le panneau de droite et afficher les détails complets de l'exclusion, chaque capsule représentant un critère ou un attribut de l'exclusion. En cliquant sur une capsule dans ce panneau, vous affichez une liste dans laquelle vous pouvez rechercher les valeurs qu'elle contient, ce qui est pratique lorsque les valeurs sont masquées en raison d'un manque d'espace.
Dernière mise à jour	Date de la création ou de la dernière mise à jour de l'exclusion.
Dernier auteur	Nom de la partie qui a créé ou mis à jour l'exclusion.
⋮	Menu contextuel permettant de modifier ou de supprimer une exclusion.

Pour modifier une exclusion :

1. Sélectionnez l'exclusion dans la liste et cliquez sur le menu contextuel ⋮ à la fin de la ligne.
2. Sélectionnez **Supprimer**.

   La fenêtre **Modifier une exclusion** s'ouvre.

3. Modifiez les informations nécessaires. Reportez-vous à la procédure pour créer une exclusion.
4. Cliquez sur **Enregistrer**.

   Un message apparaît pour indiquer que l'exclusion a bien été mise à jour et que le prochain scan en tiendra compte.

Pour supprimer une exclusion :

1. Sélectionnez l'exclusion dans la liste et cliquez sur le menu contextuel ⋮ à la fin de la ligne.

   Un message demande de confirmer la suppression. Cette action est irréversible.
2. Cliquez sur **Supprimer une exclusion**.

   Un message apparaît pour indiquer que l'exclusion a bien été supprimée et que le prochain scan en tiendra compte.

Identités 360 — Gestion complète du risque d'identité

Identités 360 est une nouvelle fonctionnalité de Tenable Identity Exposure centrée sur les identités, qui fournit un inventaire riche et exhaustif de chaque identité sur la surface de risque de l'organisation.

Cette fonctionnalité unifie les identités dans tout Active Directory et Entra ID et permet de les classifier selon leur niveau de risque, de sorte que vous pouvez classer les identités dans votre organisation des plus risquées aux moins risquées.

De plus, **Identités 360** permet aux utilisateurs d'acquérir une compréhension approfondie de chaque identité à travers différents prismes contextuels tels que les comptes, les faiblesses et les appareils associés à une identité donnée pour obtenir un tableau complet de cette identité.

Fonctions clés

- **Vue unifiée des identités** — « Identités 360 » regroupe les identités de plusieurs fournisseurs d'identité, en commençant par Active Directory et Entra ID.

- **Classement basé sur le risque** – Tirant parti d'analyses avancées, « Identités 360 » vous permet de classer les identités de votre organisation des plus risquées aux moins risquées. Cette priorisation permet aux équipes de sécurité de concentrer leurs efforts sur ce qui compte le plus, de manière à optimiser l'allocation des ressources et améliorer la posture de sécurité globale.
- **Informations contextuelles sur les identités** – Vous pouvez acquérir une compréhension approfondie de chaque identité à travers différents prismes contextuels :
    - Comptes associés
    - Faiblesses identifiées
    - Appareils connectés
    - Privilèges d'accès
    - Modèles d'activité

  Cette approche aux multiples facettes permet d'obtenir un tableau complet de chaque identité pour profiter d'évaluations des risques plus précises et de mesures de sécurité ciblées.
- **Renseignements exploitables** – En consolidant les informations d'identité provenant de sources disparates, « Identités 360 » fournit des données exploitables qui offrent de nombreuses possibilités aux équipes de sécurité :
    - Identification et correction des vulnérabilités associées aux identités à haut risque
    - Mise en œuvre de stratégies de contrôle d'accès plus efficaces
    - Détection et réponse plus rapides aux menaces internes potentielles
    - Simplification des rapports et des audits de conformité

En centralisant la gestion du risque d'identité et en fournissant une vue holistique du paysage d'identité de votre organisation, **Identités 360** permet de réduire la surface d'attaque, d'améliorer l'efficacité opérationnelle et de renforcer votre posture de sécurité globale.

Qu'est-ce qu'une identité ?

Une **identité** est la représentation numérique d'une entité humaine (ou non humaine).

- De qui il s'agit (nom, poste, service, etc.)
- Ce à quoi elle peut accéder (fichiers, systèmes, données)
- Comment elle interagit avec le monde numérique de votre organisation

Un **compte**, en revanche, n'est qu'une partie d'une identité. Il s'agit d'une clé qui permet à la personne de se connecter à un système ou service spécifique. Par exemple, une personne peut posséder un compte de messagerie professionnel, un compte de base de données client et un compte d'outil de gestion de projet : tous ces éléments constituent différentes parties de son identité numérique globale.

En examinant l'identité dans son ensemble plutôt que simplement les comptes individuels, « Identités 360 » vous donne un tableau plus complet de la présence numérique de chaque personne et des risques potentiels.

Données de la fonctionnalité « Identités 360 »

Identités 360 exploite les données de la plateforme Tenable, offrant à Tenable Identity Exposure un accès sans précédent aux données pour évaluer la posture de sécurité de votre organisation.

Dans l'écosystème Tenable, les entités sont appelées « assets ». Tenable Identity Exposure continue de mettre en évidence les vulnérabilités associées à ces assets tout en révélant leurs relations à travers des pages d'assets détaillées.

Remarque : lors de la visualisation des propriétés d'un asset, certains champs peuvent s'afficher avec une casse incorrecte (tout en minuscules, par exemple) par rapport à leur format d'origine dans le fournisseur d'identité (IDP).

Remarque : la fonctionnalité Vue d'ensemble de la cyber-exposition affiche actuellement des données liées aux faiblesses en fonction du **profil Tenable par défaut** et ne reflète pas automatiquement le **statut des déviances sur les objets AD que vous avez ajoutés à la liste blanche dans d'autres profils**.

Par conséquent :

- Si vous avez **ajouté un objet AD à la liste blanche** pour un indicateur d'exposition spécifique (p. ex., « Membre d'un groupe d'administrateurs natif »), **la Vue d'ensemble de la cyber-exposition le signalera toujours comme une faiblesse de sécurité si le profil par défaut l'a identifié comme déviant**.

- Vous pouvez ainsi avoir l'impression que le problème n'a pas été résolu, même si l'objet a déjà été ajouté à la liste blanche sous un profil différent.
- Si une mesure de remédiation (telle que la suppression de l'appartenance à un groupe) est prise sur la base des indications de la Vue d'ensemble de la cyber-exposition, l'objet disparaît de la vue. Mais si l'objet était déjà sur liste blanche ailleurs, il est possible que cette mesure ait été facultative.

Collecte d'identités

Identités 360 consolide les comptes d'IDP sous une entité « Personne » unifiée. Pour déterminer si elle doit associer des comptes, la fonctionnalité **Identités 360** compare plusieurs attributs tels que les adresses e-mail de compte et les noms principaux d'utilisateur (UPN).

Tenable priorise les correspondances de haute qualité pour empêcher les associations erronées, même si, de ce fait, il lui arrive parfois de manquer des correspondances qui semblent évidentes pour un observateur humain. Par exemple, Tenable exclut les noms et prénoms de la correspondance, car la forte probabilité d'homonymes dans les grandes organisations augmente considérablement le risque de faux positifs.

Remarque : lorsque l'IDP supprime le dernier compte associé à une personne, l'interface utilisateur Tenable Identity Exposure peut mettre jusqu'à 12 heures pour supprimer l'asset « Personne » correspondant. **Identités 360** peut également afficher des relations dupliquées entre une personne et les comptes associés.

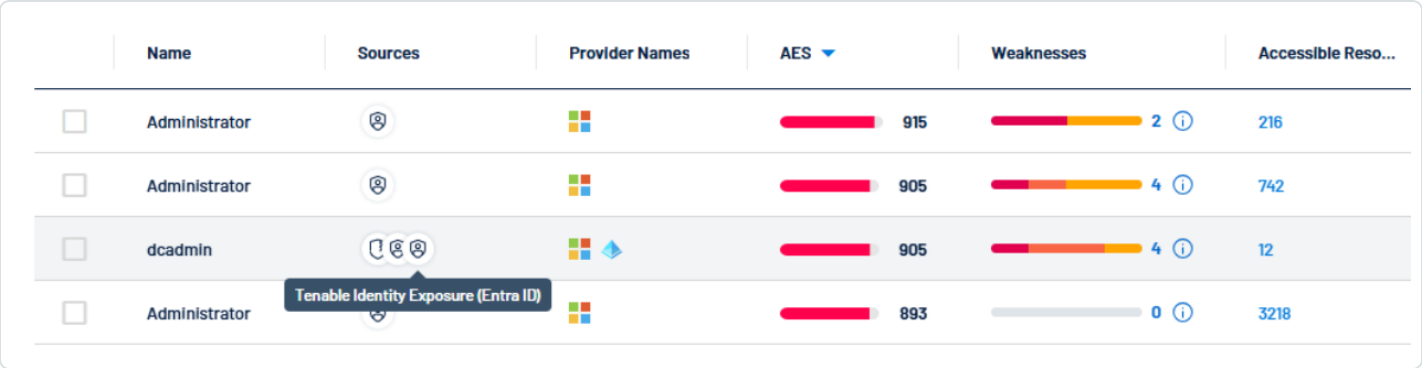
Tenant, domaine et organisation IDP

Tenable utilise le terme « tenant » pour englober divers concepts associés à l'IDP, notamment « tenant » (par exemple, dans Microsoft Entra ID), « organisation » (par exemple, dans Okta) et « domaine » (par exemple, dans Microsoft Active Directory).

Pour plus d'informations sur la façon dont Tenable identifie les tenant d'objets IDP, voir Comprendre l'appartenance à un tenant.

Assets et sources de données multi-produits

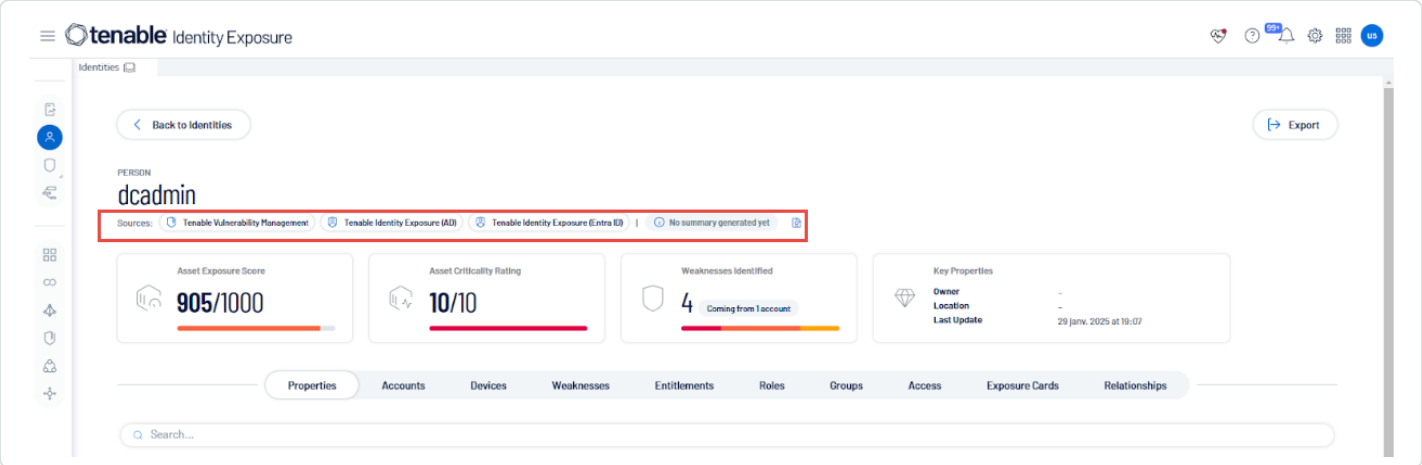
Identités - Bilan complet fournit une vue complète de toutes les données liées aux identités au sein de l'écosystème Tenable. Cela inclut les données Tenable Identity Exposure, les données de sécurité cloud et même les résultats de scan Nessus. Le produit Tenable spécifique qui a collecté chaque ensemble de données est désigné comme sa « source ».



La vue inclut également le type de données disponibles, correspondant par exemple au nom de l'IdP : Active Directory, Entra ID ou AWS. Ces informations apparaissent dans la colonne « Nom des fournisseurs ». Les champs « Source » et « Nom des fournisseurs » prennent en charge le filtrage et le tri, et chacun peut contenir plusieurs valeurs.

Données multi-produits (sources de données)

Identités - Bilan complet affiche toutes les données qui concernent les identités et sont disponibles au sein de l'écosystème Tenable. Un asset donné peut avoir une ou plusieurs sources, ce qui signifie qu'il peut être observé par un ou plusieurs produits Tenable. Tenable Identity Exposure présente les données directement collectées par Tenable Identity Exposure, ainsi que les données provenant de sources complémentaires.



Sources possibles :

License requise	Prérequis de configuration	Sources des assets	Valeur
Tenable Identity Exposure ou Tenable One	• Un domaine Active Directory (AD) dans Tenable Identity Exposure • Données envoyées à la plateforme cloud de Tenable	Tenable Identity Exposure (AD)	Données AD complètes
Tenable Identity Exposure ou Tenable One	• Un tenant Microsoft Entra ID (MEID) dans Tenable Identity Exposure	MEID Tenable Identity Exposure	Données MEID complètes
Tenable One	• Un fournisseur d'identité de Tenable dans Tenable Cloud Security	Tenable Cloud Security	Données d'IdP supplémentaires dans Identités - Bilan complet : AWS, Okta, GCI, OneLogin et PingIdentity. Les données seront limitées aux comptes IDP dont les adresses e-mails sont renseignées dans l'IDP.
Tenable One	• Un scan Nessus	Tenable	Mappage de

	utilisant le plug-in 171956 - Windows Enumerate Accounts. Pour plus de détails sur les scans, voir Scans Overview (Vue d'ensemble des scans) dans le Guide de l'utilisateur Tenable Vulnerability Management.	Vulnerability Management	comptes Active Directory (AD) et Entra ID, avec les appareils qui utilisent ces comptes.

Conditions préalables

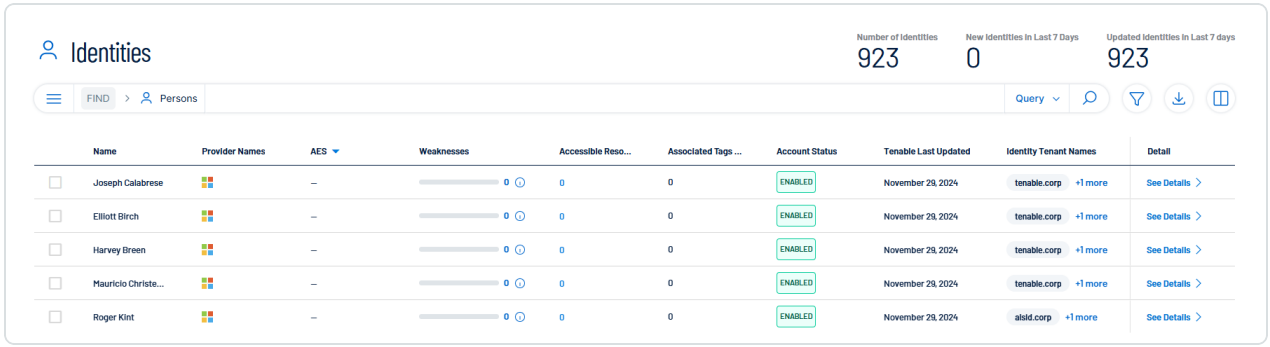
- Pour utiliser **Identités 360**, vous devez activer la prise en charge de la fonctionnalité dans les paramètres de Tenable Identity Exposure.
- Voir Activation de la prise en charge de « Identités 360 », « Centre d'exposition » et « Microsoft Entra ID » pour obtenir des instructions.

Accéder à la vue d'ensemble des identités

Pour ouvrir la page **Vue d'ensemble des identités** :

- Dans Tenable Identity Exposure, cliquez sur dans la barre de navigation de gauche.

  La page **Vue d'ensemble des identités** apparaît et affiche un dashboard permettant de gérer et de surveiller les identités au sein du système d'une organisation.



Principaux éléments

Ce dashboard vous permet d'afficher, de rechercher et de gérer des informations sur les identités, en mettant l'accent sur des métriques de sécurité telles que les faiblesses et l'exposition aux attaques. Il fournit à la fois un aperçu général (dans l'en-tête) et des informations détaillées pour chaque identité sous forme de tableau.

- **Métriques clés**
  - Nombre d'identités
  - Nouvelles identités au cours des 7 derniers jours
  - Identités mises à jour au cours des 7 derniers jours
- **Navigation et recherche**
  - Barre de recherche pour les requêtes d'identités
  - Options de requête, de filtrage, d'exportation et de personnalisation des colonnes

    Pour des informations complètes sur l'utilisation de cette fonction de recherche, voir le Global Search Quick Reference (Guide de référence rapide de la recherche globale, en anglais).
- **Tableau de données** répertoriant tous les assets d'identité de vos fournisseurs d'identité (IDP). Cette vue se concentre spécifiquement sur les assets de type identité, contrairement à Tenable One qui affiche tous les types d'assets. Chaque ligne représente une identité unique accompagnée de ces informations (affichage par défaut des colonnes) :
  - Nom, fournisseurs, score AES (Asset Exposure Score), faiblesses, ressources accessibles, tags associés, statut du compte, dernière mise à jour, noms des tenants d'identité et détails
- **Visualisation des données**
  - Histogrammes ou indicateurs dans les colonnes « Score AES » et « Faiblesses » fournissant une représentation visuelle des données
- **Indicateurs de statut**
  - Tag « ACTIVÉ/DÉSACTIVÉ » dans la colonne « Statut du compte »

Comparaison avec l'inventaire Tenable Exposure Management

L'interface d'**Identités 360** présente une apparence et des fonctionnalités similaires à celles de la page **Inventaire**de Tenable Exposure Management, avec des adaptations spécifiques pour la gestion des identités. La disposition et de nombreuses fonctionnalités vous seront familières si vous utilisez déjà Tenable Exposure Management.

Pour plus d'informations, voir le Tenable One Exposure Management Platform Deployment Guide (Guide de déploiement de la Plateforme de gestion de l'exposition Tenable One, en anglais).

Voir aussi

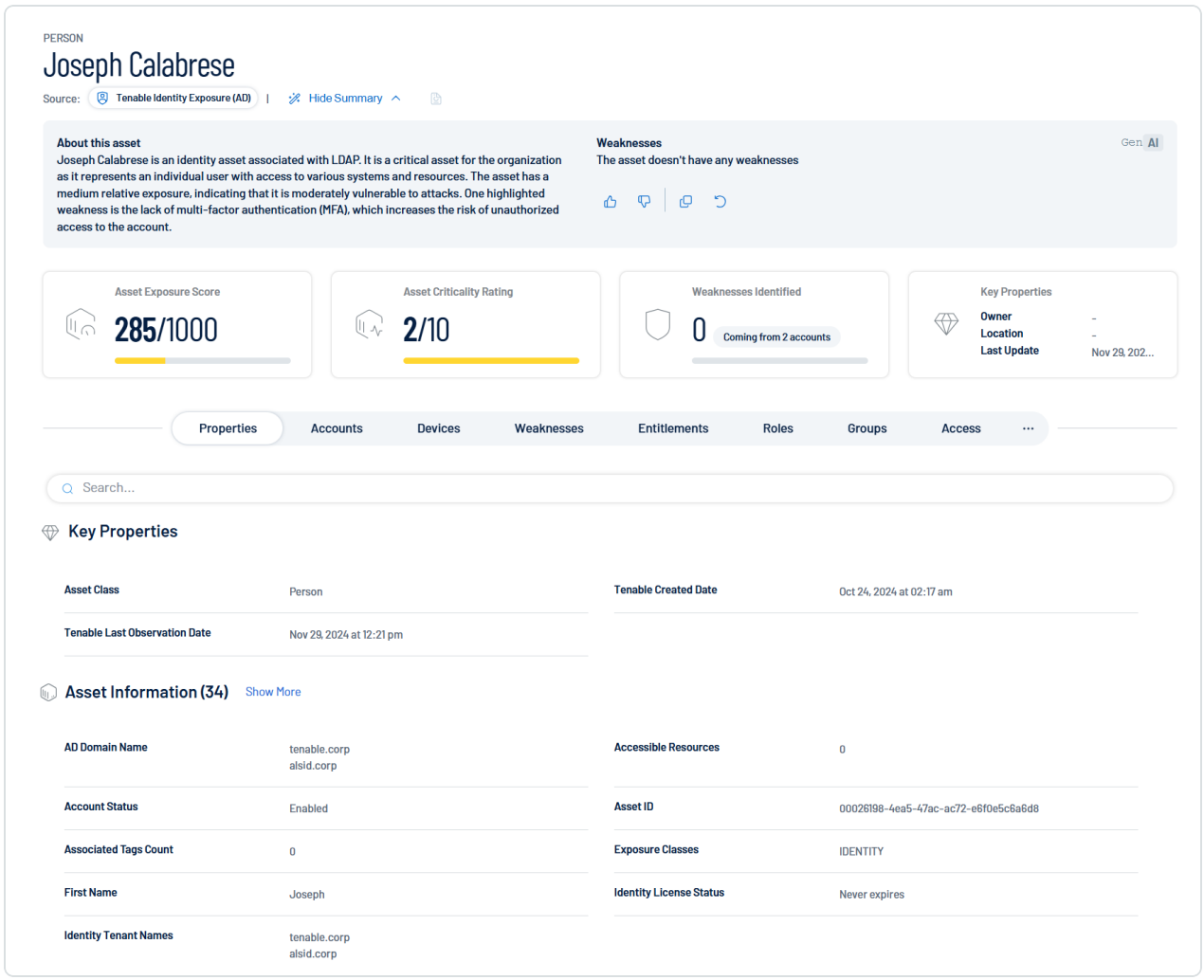
- Comprendre l'appartenance à un tenant

Détails sur l'identité

La page des **détails sur l'identité** se concentre sur une identité particulière et fournit une vue complète de son empreinte numérique, de ses droits d'accès, de ses vulnérabilités potentielles et de sa posture de sécurité globale au sein de l'écosystème informatique d'une organisation.

Pour accéder à la page :

- Sur la page **Vue d'ensemble des identités**, cliquez sur **Afficher les détails** à la fin de la ligne contenant le nom de la personne dans le tableau.



En-tête et section supérieure

- **Nom de l'identité** : affiche le nom de l'identité.
- Icônes **Personne** et **Source** : précise l'association de l'identité à des sources spécifiques. En passant le pointeur de la souris sur l'icône Source, vous découvrirez le nom du fournisseur d'identité.
- **Récapitulatif** : récapitulatif détaillé de l'identité et des faiblesses détectées pour cette identité.

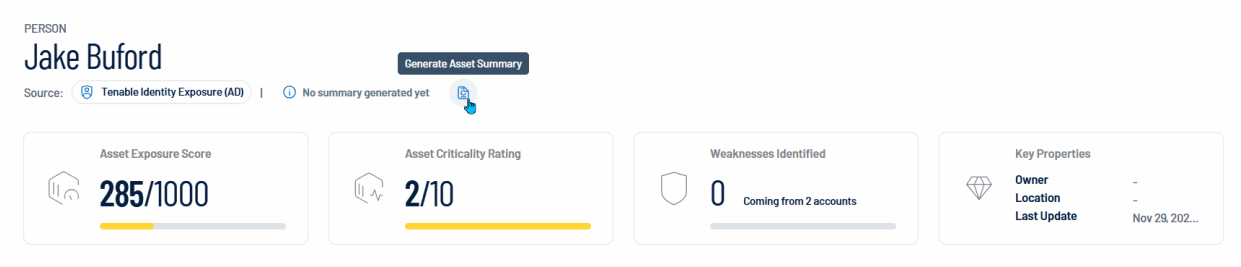
Générer et afficher un récapitulatif IA de l'asset :

Tenable Identity Exposure vous permet de générer un récapitulatif d'une identité à l'aide de l'IA. Les récapitulatifs sont générés au niveau du conteneur et ne s'appliquent qu'aux identités sous licence au sein de votre conteneur.

Remarque : Tenable Identity Exposure limite la génération de récapitulatifs à 100 par heure, avec un maximum de 1 000 récapitulatifs par jour.

Effectuez l'une des actions suivantes :

- Si c'est la première fois que vous générez un récapitulatif IA au sujet de cet asset, cliquez sur le bouton à côté de **Aucun récapitulatif n'a encore été généré**.



  Tenable Identity Exposure utilise l'IA pour générer un récapitulatif de l'asset, en incluant les détails généraux et les spécificités des faiblesses de l'asset.

- Pour générer à nouveau un récapitulatif IA existant pour l'asset, cliquez sur **Afficher le récapitulatif** et, en bas du panneau de récapitulatif, cliquez sur le bouton .

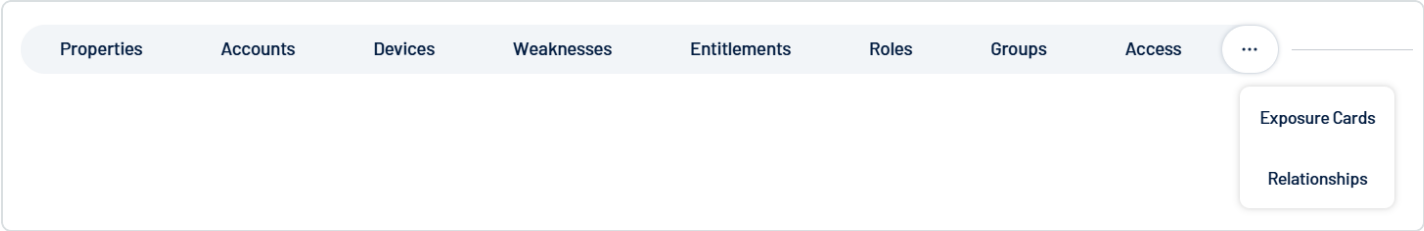
  Tenable Identity Exposure regénère le récapitulatif IA pour l'identité.

Conseil : cliquez sur le bouton pour copier le récapitulatif directement dans votre presse-papiers. Vous pouvez également évaluer l'utilité du récapitulatif en cliquant sur ou , afin de contribuer à améliorer la qualité du contenu généré par l'IA dans Tenable Identity Exposure à l'avenir.

- **Score AES (Asset Exposure Score)** : quantifie l'exposition de l'identité en matière de sécurité, un score maximal de 1 000 représentant le niveau d'exposition le plus élevé.
- **Classement ACR (Asset Criticality Rating)** : reflète l'importance de l'identité au sein de l'organisation, notée sur une échelle de 1 à 10, 10 représentant la criticité la plus élevée.
- **Faiblesses identifiées** : affiche le nombre de faiblesses ou de failles de sécurité identifiées pour cette identité spécifique.
- **Propriétés clés** : répertorie des informations clés, notamment le propriétaire, l'emplacement et la date de la dernière mise à jour de cette identité.

Onglets d'en-tête

Sous l'en-tête, des onglets spécifiques fournissent des informations détaillées propres à leur catégorie. Consultez les descriptions détaillées de chaque onglet dans la section ci-dessous.

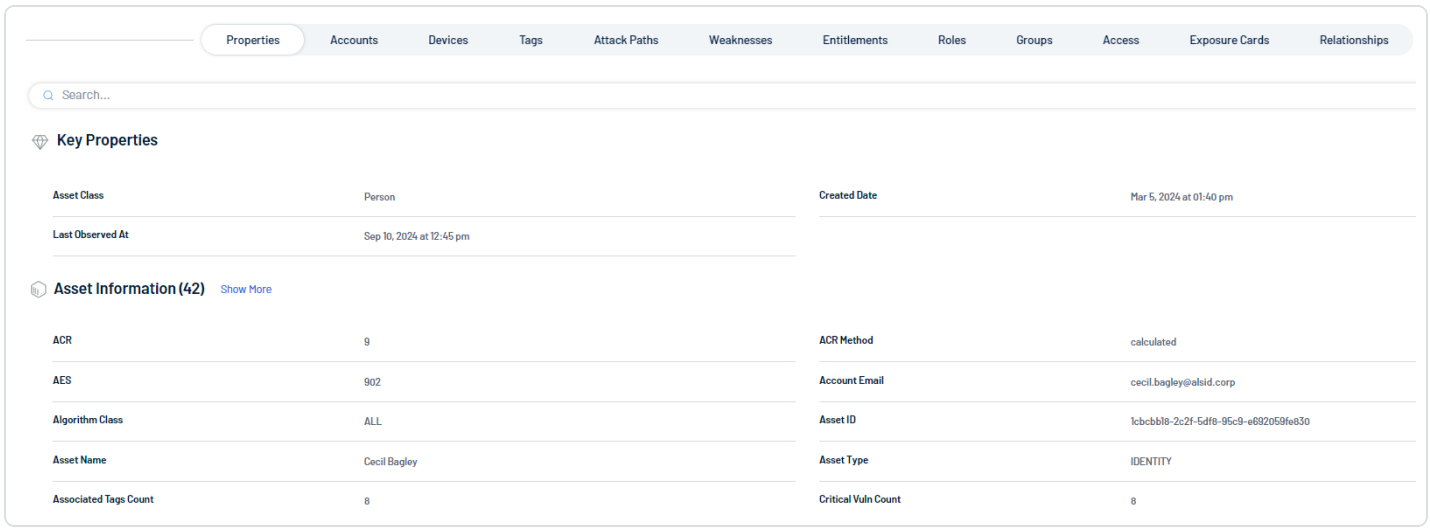


- **Propriétés** : informations de base et attributs de l'identité.
- **Comptes** : compte et profil réseau associés à l'identité.
- **Appareils** : appareils électroniques associés à l'identité.
- **Faiblesses** : vulnérabilités ou risques de sécurité spécifiques.
- **Droits d'accès** : autorisations ou droit d'accès spécifiques accordés à une identité au sein des systèmes informatiques d'une organisation.
- **Rôles** : ensemble de droits d'accès regroupés par fonctions, responsabilités ou postes au sein de l'organisation.
- **Groupes** : unités d'organisation ou équipes auxquelles l'identité appartient.
- **Accès** : aperçu des ressources ou des systèmes auxquels cette identité peut accéder.
- **Fiches d'exposition** : récapitulatifs des niveaux d'exposition aux risques.
- **Relations** : connexions à d'autres identités ou entités.

Lorsqu'elle est disponible, l'option « Afficher les détails » permet d'afficher des informations plus précises dans Tenable Inventory.

Propriétés

La vue par défaut affiche l'onglet « Propriétés ».



Propriétés clés

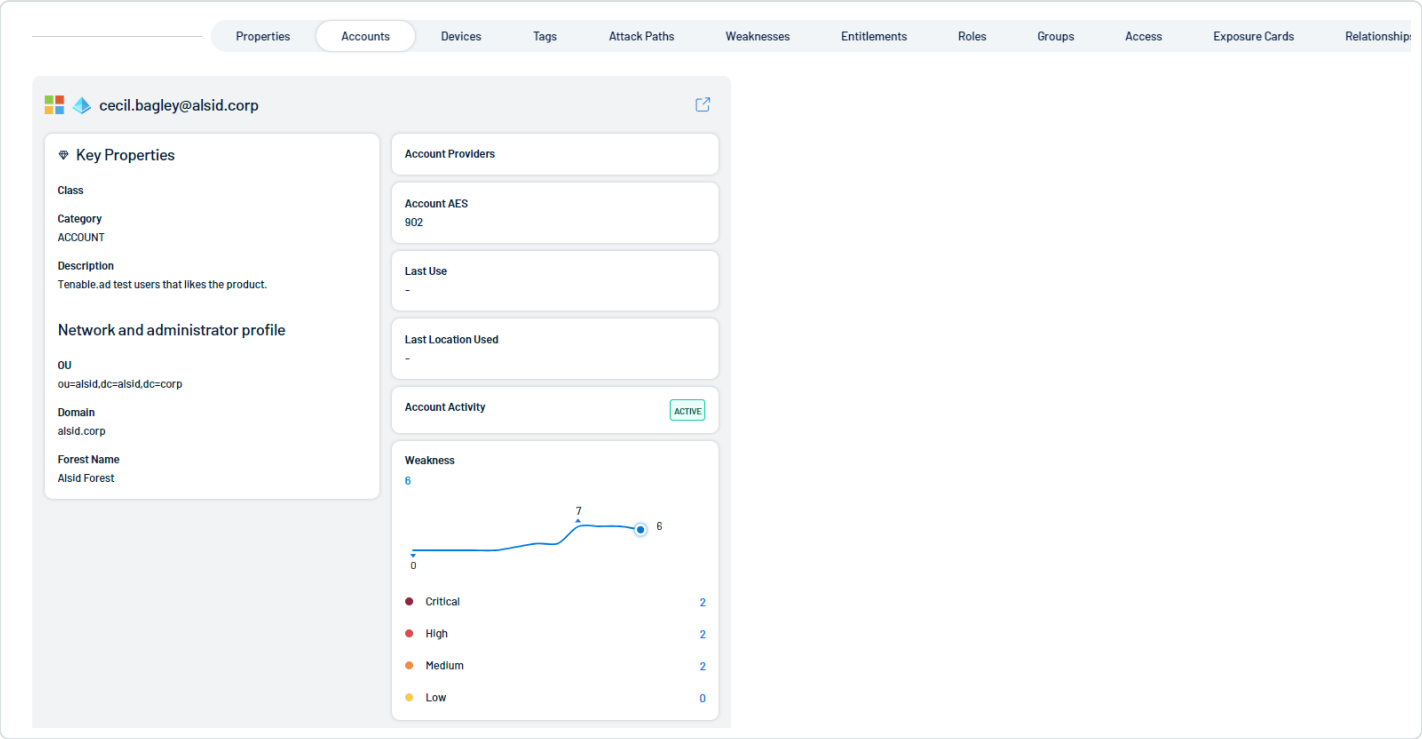
Récapitulatif des attributs les plus essentiels liés à l'asset ou à l'identité. Cela inclut généralement des détails importants tels que la classe de l'asset, la date/heure de la dernière observation et d'autres informations essentielles qui donnent un aperçu du statut de l'entité.

Informations sur l'asset

Liste détaillée des propriétés spécifiques associées à l'asset ou à l'identité. Il peut s'agir d'identifiants techniques tels que le classement ACR, le score AES, le nom de l'asset, l'adresse e-mail, la date de création, etc. Ces informations fournissent une vue complète des caractéristiques et des métadonnées liées à l'entité.

Comptes

La section « Comptes » fournit des informations détaillées sur le compte et le profil réseau associés à l'identité.



Propriétés clés

Contient des détails essentiels tels que la classe de compte (type d'asset), la catégorie (par exemple, COMPTE) et une description de l'objectif ou du rôle du compte. La section « Profil réseau et administrateur » met en évidence des détails techniques, tels que l'unité d'organisation (UO), le domaine et le nom de la forêt.

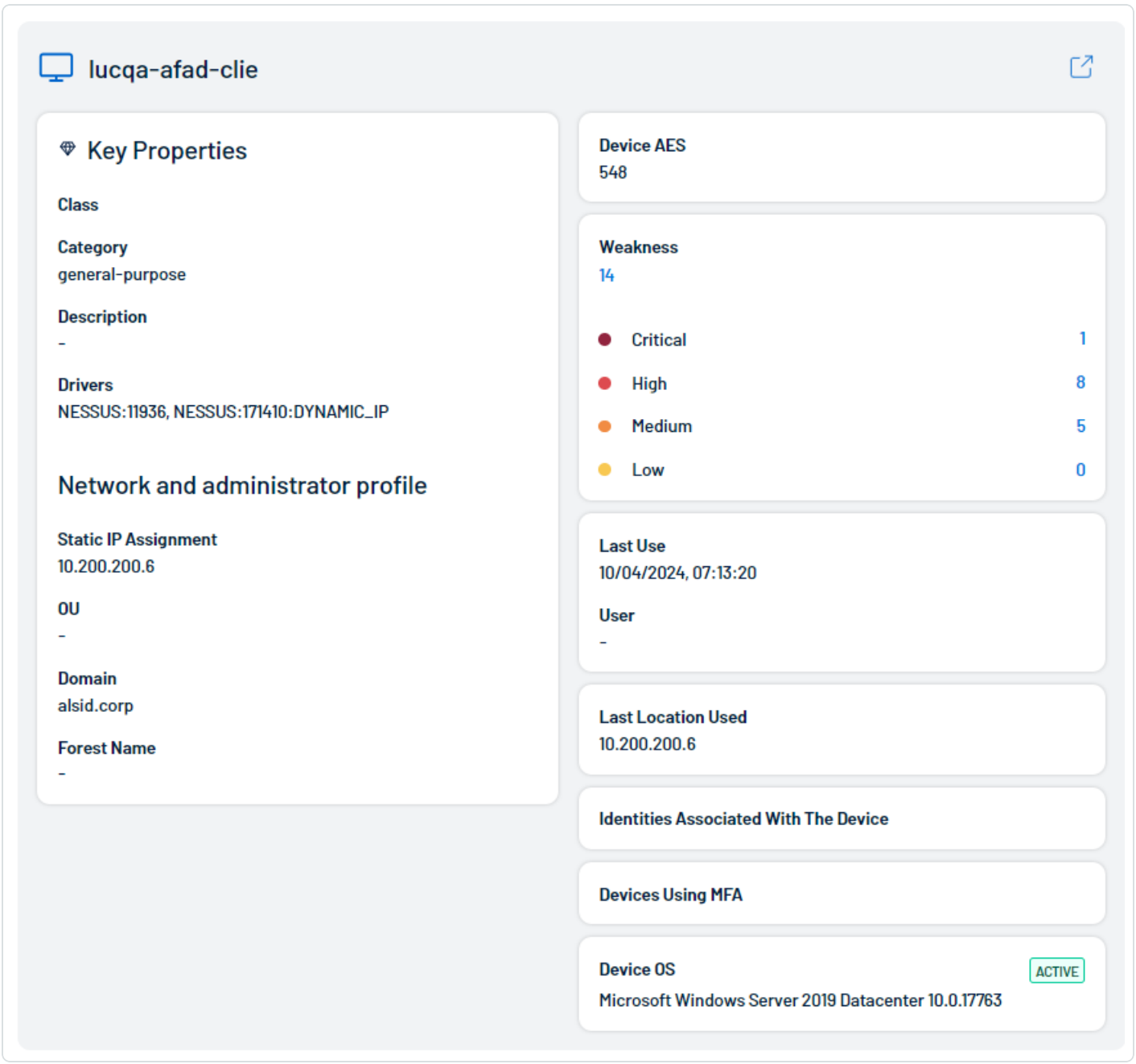
Faiblesse

Affiche une représentation graphique du nombre de faiblesses détectées, classées par sévérité (critique, élevée, moyenne et faible). Le graphique fournit une courbe de tendance indiquant la progression des faiblesses au fil du temps.

Appareils

Un appareil est généralement un composant physique ou virtuel qui peut se connecter à un réseau, communiquer avec d'autres appareils et accomplir des fonctions ou des tâches spécifiques associées à l'identité.

Pour voir les appareils de cette personne, utilisez d'abord Tenable Vulnerability Management afin d'effectuer un scan des machines sur lesquelles elle se connecte.



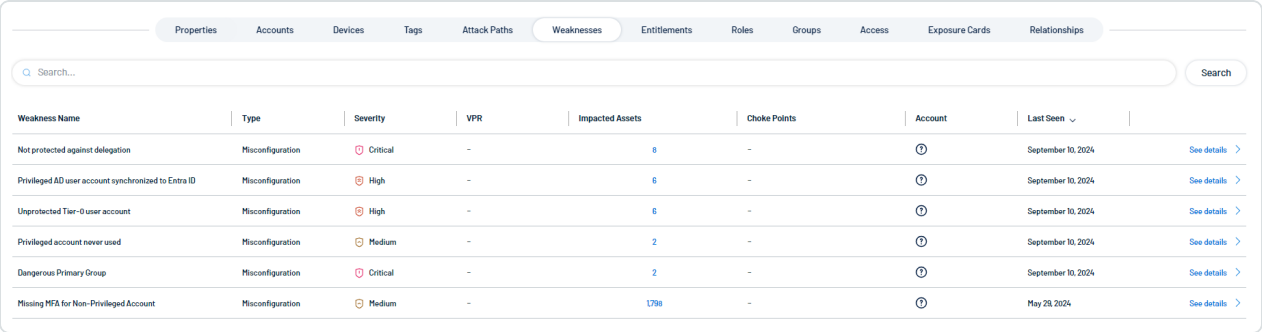
Sur chaque tuile, vous pouvez afficher les informations suivantes concernant l'appareil :

- **Propriétés clés** :
  - **Classe** – La classe d'assets associée à l'appareil.
  - **Catégorie** – La catégorie associée à l'appareil, par exemple, **general-purpose** (à usage général).

    - **Description** – Lorsque cela est possible, la description de l'appareil.
    - **Pilotes** – La liste des pilotes installés sur l'appareil.
- **Profil réseau et administrateur** :
    - **Attribution d'adresse IP statique** – L'adresse IP statique associée à l'appareil.
    - **UO** – L'unité d'organisation (UO) associée à l'appareil.
    - **Domaine** – Le domaine associé à l'appareil. Pour plus d'informations, voir Domaines dans le *Guide de l'utilisateur Tenable Identity Exposure*.
    - **Nom de la forêt** – Le nom de la forêt associée à l'appareil. Pour plus d'informations, voir Forêts dans le *Guide de l'utilisateur Tenable Identity Exposure*.
- **Score AES de l'appareil** – Le score AES global associé à l'appareil. Pour plus d'informations, voir Tenable Inventory Metrics (Métriques Tenable Inventory).
- **Faiblesse** – Représentation graphique des faiblesses de l'appareil. Cette section comprend un graphique en courbes et un décompte individuel de chaque faiblesse et de sa criticité.

Faiblesses

- Une **faiblesse** est une instance qui indique la présence de vulnérabilités ou de failles de sécurité associées à cette identité ou à ses comptes.
- Une **vulnérabilité** est une faiblesse technique présente dans des produits ou des systèmes d'information, et qui peut être exploitée pour perturber ou dégrader les activités économiques et sociales.
- Un **indicateur d'exposition** (IoE) est une signature de détection qui identifie les expositions de sécurité potentielles liées à l'identité au sein de votre environnement.
- Un **score de risque** est une métrique complète qui évalue les risques liés aux identités à l'échelle de votre organisation, en tenant compte de divers éléments tels que les faiblesses, les droits d'accès et d'autres indicateurs liés à la sécurité, afin de fournir une évaluation globale des menaces potentielles.



Conseil : pour accéder à des données plus détaillées sur les faiblesses, cliquez sur « Afficher les détails » afin d'accéder à la page Weakness Details (Détails de la faiblesse) de Tenable Inventory.

Remarque : cette page est actuellement réservée aux utilisateurs titulaires d'une licence Tenable One.

La tuile contient les informations suivantes :

- **Nom** : la vulnérabilité ou la faiblesse identifiée.
- **Type** : la catégorie ou la classification de la vulnérabilité, par exemple « mauvaise configuration ».
- **Sévérité** : mesure la criticité de la faiblesse, de faible à critique, et détermine l'impact potentiel en cas d'exploitation.
- **VPR** : le classement VPR (Vulnerability Priority Rating) est un score ou classement indiquant l'urgence de traiter la faiblesse en fonction de son exploitabilité et de ses dommages potentiels. Voir Vulnerability Priority Rating (Classement VPR [Vulnerability Priority Rating]).
- **Assets impactés** : répertorie les systèmes, les applications et les données qui pourraient être affectés si la faiblesse est exploitée.
- **Points d'étranglement** : zones potentielles du système où vous pouvez concentrer les efforts d'atténuation pour limiter les dommages ou la propagation d'une attaque.
- **Compte** : le compte associé à la faiblesse ou à la vulnérabilité identifiée.
- **Dernière détection** : la date ou l'heure à laquelle la vulnérabilité a été détectée pour la dernière fois.

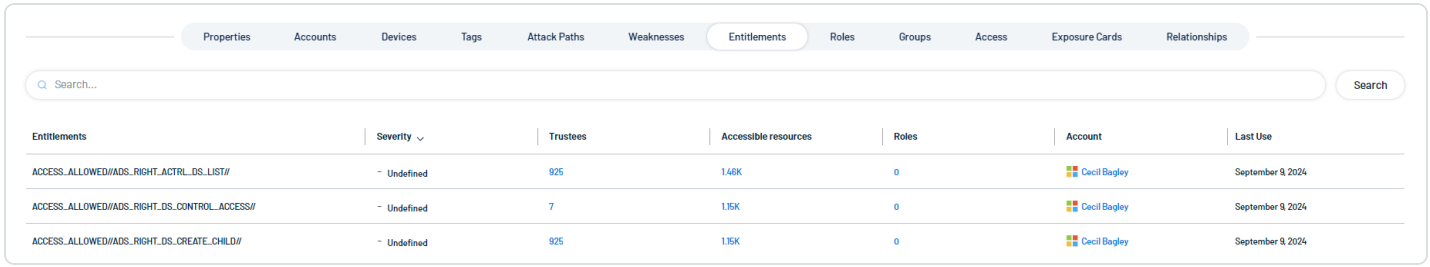
Remarque : la fonctionnalité Identités - Bilan complet affiche actuellement des données liées aux faiblesses en fonction du **profil Tenable par défaut** et ne reflète pas automatiquement le **statut des déviances sur les objets AD que vous avez ajoutés à la liste blanche dans d'autres profils**.

Par conséquent :

- Si vous avez **ajouté un objet AD à la liste blanche** pour un indicateur d'exposition spécifique (p. ex., « Membre d'un groupe d'administrateurs natif »), **Identités - Bilan complet le signalera toujours comme une faiblesse de sécurité si le profil par défaut l'a identifié comme déviant**.
- Vous pouvez ainsi avoir l'impression que le problème n'a pas été résolu, même si l'objet a déjà été ajouté à la liste blanche sous un profil différent.
- Si une mesure de remédiation (telle que la suppression de l'appartenance à un groupe) est prise sur la base des indications d'Identités - Bilan complet, l'objet disparaît de la vue. Mais si l'objet était déjà sur liste blanche ailleurs, il est possible que cette mesure ait été facultative.

Droits d'accès

Un **droit d'accès** est une autorisation spécifique accordée à une identité au sein des systèmes informatiques d'une organisation. Il représente le niveau granulaire du contrôle d'accès et définit avec exactitude les actions qu'une identité peut accomplir sur une ressource particulière.



La tuile contient les informations suivantes :

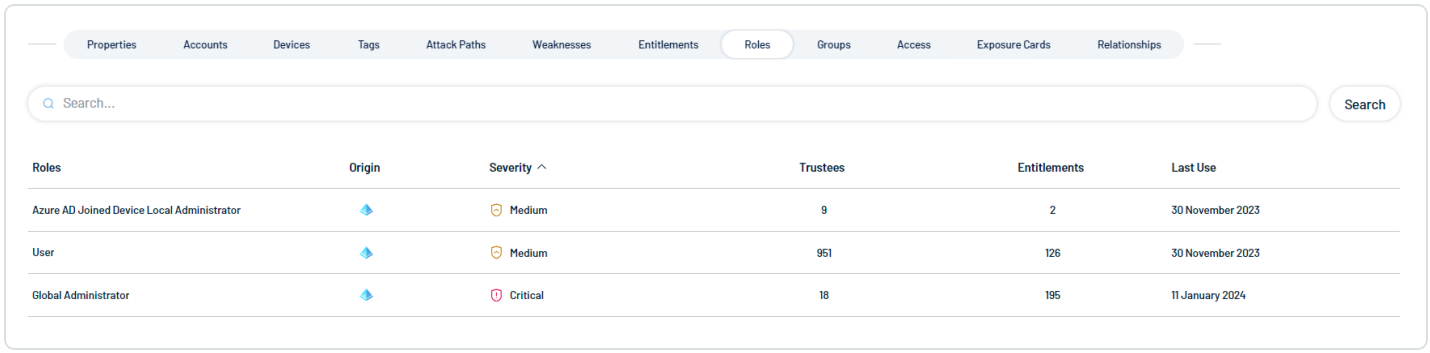
- **Droit d'accès** : répertorie les autorisations ou droits d'accès spécifiques accordés aux comptes, tels que « ACCESS_ALLOWED » avec des autorisations détaillées. Il peut s'agir des autorisations définies au sein d'un système comme Active Directory.
- **Sévérité** : affiche le niveau de criticité ou de risque associé à chaque droit d'accès. Dans ce cas, la sévérité est marquée comme « Indéfinie », ce qui suggère qu'aucune catégorisation de risque spécifique ne s'applique.

- **Assets ayant donné leur approbation** : indique le nombre d'utilisateurs ou de comptes (assets ayant donné leur approbation) auxquels ces droits ou autorisations ont été accordés.
- **Ressources accessibles** : affiche le nombre de ressources (telles que des fichiers, des dossiers, des systèmes, etc.) accessibles via le droit d'accès accordé.
- **Rôles** : affiche le nombre de rôles liés à ce droit d'accès spécifique.
- **Compte** : spécifie l'utilisateur ou le compte associé à ces droits d'accès. Par exemple, « Cecil Bagley » est répertorié comme titulaire de compte pour les autorisations affichées.
- **Dernière utilisation** : indique la dernière date à laquelle ces droits d'accès ont été utilisés, c'est-à-dire la date à laquelle le compte a accédé aux ressources pour la dernière fois à l'aide des autorisations spécifiques.

Rôles

Un **rôle** est un ensemble de droits d'accès regroupés par fonctions, responsabilités ou postes au sein de l'organisation. Les rôles offrent un moyen de gérer plus efficacement les droits d'accès en attribuant un ensemble de droits d'accès prédéfinis à plusieurs utilisateurs qui partagent des fonctions similaires.

La tuile **Rôles** affiche tous les rôles attribués à l'identité. Par exemple, si cette identité a des rôles attribués dans Microsoft Entra ID, leurs détails apparaissent ici.



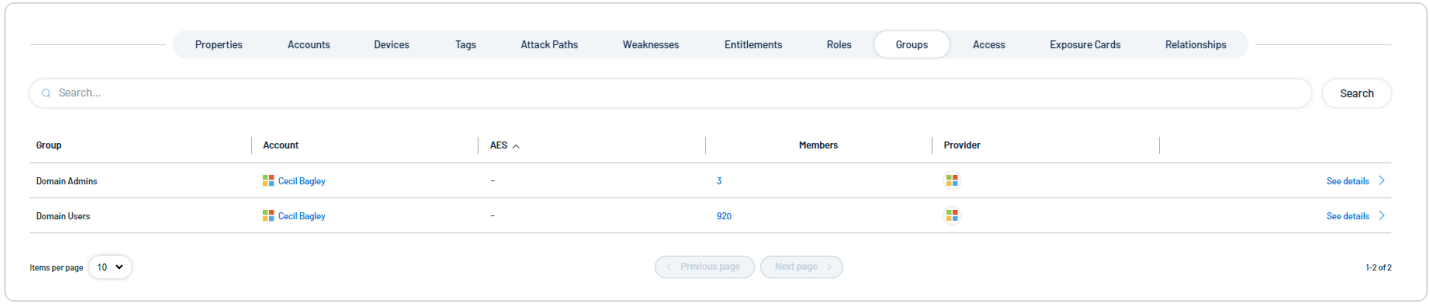
La tuile contient les informations suivantes :

- **Rôles** – Nom du rôle attribué à l'identité.
- **Origine** – Icône indiquant le fournisseur d'origine du compte.
- **Sévérité** – Sévérité globale de l'asset, par exemple, **Critique**.

- **Assets ayant donné leur approbation** – Nombre d'assets ayant donné leur approbation associés au rôle de l'identité.
- **Droits d'accès** – Nombre de droits d'accès accordés au rôle.
- **Dernière utilisation** – Date à laquelle le rôle a été utilisé pour la dernière fois sur l'asset.

Groupes

Les groupes sont des unités collectives ou des équipes auxquelles cette identité appartient au sein de l'organisation.

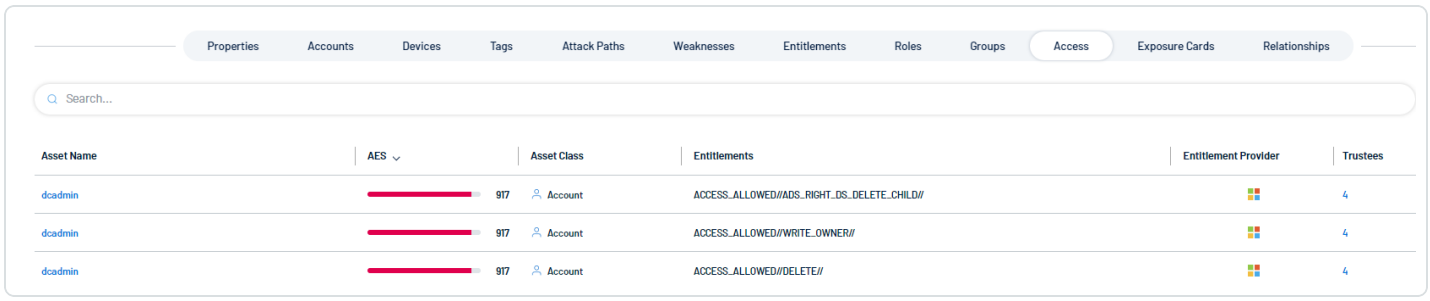


La tuile contient les informations suivantes :

- **Groupe** : nom du groupe auquel les utilisateurs ou les comptes appartiennent (par exemple, « Administrateurs du domaine » ou « Utilisateurs du domaine »).
- **Compte** : compte lié à un utilisateur ou une entité spécifique (dans ce cas, « Cecil Bagley »). Il peut s'agir de l'administrateur ou de l'utilisateur qui gère le groupe.
- **Score AES** (Asset Exposure Score) : Tenable calcule un score AES dynamique pour chaque asset de votre réseau, afin de représenter l'exposition relative de l'asset sous la forme d'un entier compris entre 0 et 1 000. Plus le score AES est élevé, plus l'exposition est importante. Pour plus d'informations, voir Tenable Inventory Metrics (Métriques Tenable Inventory).
- **Membres** : nombre de membres dans chaque groupe (par exemple, 3 membres dans « Administrateurs du domaine » et 920 membres dans « Utilisateurs du domaine »).
- **Fournisseur** : fournisseur d'identité source des informations du compte ou du groupe.

Accès

Cet onglet donne un aperçu des ressources ou des systèmes auxquels cette identité peut accéder.



La tuile contient les informations suivantes :

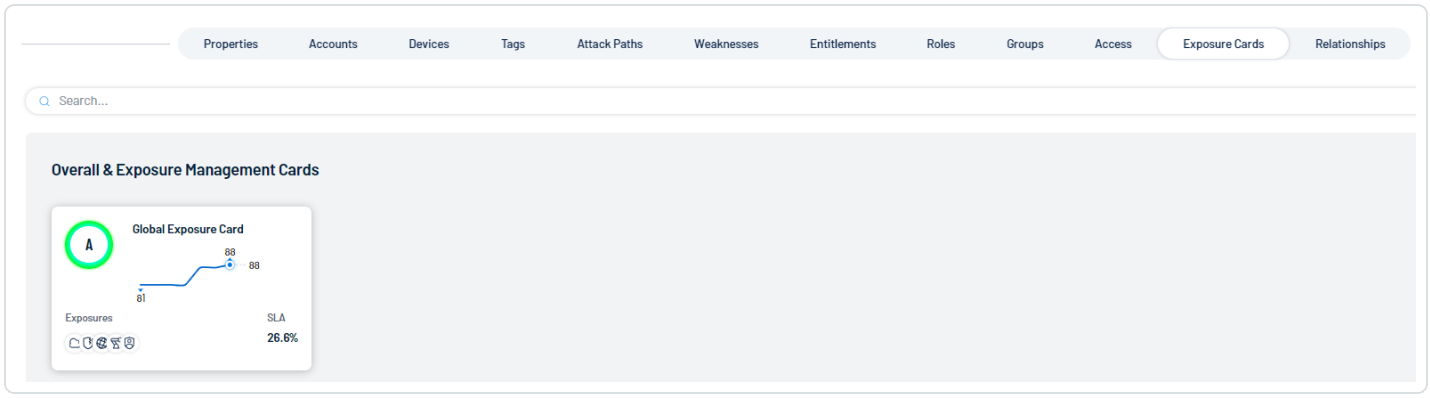
- **Nom de l'asset** : répertorie les noms des assets ou des comptes gérés (par exemple, « dcadmin ») associés à l'identité.
- **Score AES** (Asset Exposure Score) : Tenable calcule un score AES dynamique pour chaque asset de votre réseau, afin de représenter l'exposition relative de l'asset sous la forme d'un entier compris entre 0 et 1 000. Plus le score AES est élevé, plus l'exposition est importante. Il s'agit d'une valeur numérique, ici 917, accompagnée d'une barre graphique représentant une mesure relative de la sécurité ou de l'accès. Pour plus d'informations, voir Tenable Inventory Metrics (Métriques Tenable Inventory).
- **Classe de l'asset** : indique le type d'asset qui, dans ce cas, est étiqueté comme « Compte ». Les assets répertoriés sont des comptes utilisateur ou système.
- **Droits d'accès** : décrit les autorisations ou les droits accordés à l'asset. Par exemple, des droits d'accès tels que ACCESS_ALLOWED//ADS_RIGHT_DS_DELETE_CHILD//, WRITE_OWNER// et DELETE// définissent les autorisations spécifiques associées à chaque asset.
- **Fournisseur de droits d'accès** : spécifie la source ou le service fournissant ces droits d'accès.
- **Assets ayant donné leur approbation** : affiche le nombre d'assets ayant donné leur approbation associés à l'asset, représentant des individus ou des groupes qui ont le contrôle ou sont responsables de l'asset (4 assets ayant donné leur approbation sont affichés pour chaque ligne).

Fiche d'exposition

Une fiche d'exposition représente les données entrantes provenant de vos tags et sources de données configurés. Elle regroupe et normalise les données pour vous permettre de visualiser votre Score CES (Cyber Exposure Score) (CES) ainsi que d'autres métriques. Les utilisateurs peuvent créer des fiches personnalisées ou utiliser les fiches fournies par Tenable pour obtenir des

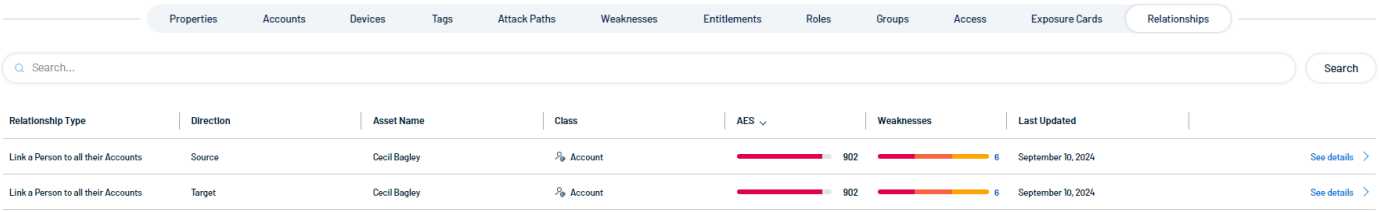
informations et des conseils sur les domaines qui nécessitent le plus leur attention.

- Cliquez sur n'importe quelle fiche pour accéder directement à Lumin Exposure View avec les données de fiche sélectionnées affichées par défaut.



Relations

La section **Relations** affiche une liste de tous les assets ayant une relation connue avec l'identité actuelle dont vous consultez les détails.



La tuile contient les informations suivantes :

- **Type de relation** – Type de relation entre les deux identités.
- **Direction** – Indique si l'identité associée est la source ou la cible de la relation.
- **Nom de l'asset** – Identifiant de l'asset de l'identité associée.
- **Classe de l'asset** – Indique le type d'asset qui, dans ce cas, est étiqueté comme « Compte ».
- **Score AES** (Asset Exposure Score) : Tenable calcule un score AES dynamique pour chaque asset de votre réseau, afin de représenter l'exposition relative de l'asset sous la forme d'un entier compris entre 0 et 1 000. Pour plus d'informations, voir Tenable Inventory Metrics (Métriques Tenable Inventory).

- **Faiblesses** – Faiblesses associées à l'asset.
- **Dernière mise à jour** – Date à laquelle un scan a identifié l'asset pour la dernière fois.

Fondamentaux d'« Identités 360 »

Identités 360 propose des outils robustes pour gérer et analyser les données d'identité de votre organisation, afin de vous permettre de prendre des décisions de sécurité éclairées.

Rechercher

Identités 360 propose trois options de recherche puissantes pour vous aider à trouver les informations exactes dont vous avez besoin :

- **Générateur de requêtes de recherche globale**
  - Permet des recherches complexes et précises à l'aide de propriétés spécifiques et de requêtes relationnelles
  - Idéal pour les utilisateurs expérimentés et l'analyse détaillée
  - Exemple : trouver tous les comptes membres des « identités dont les comptes appartiennent à un groupe spécifique » ou des « identités disposant de droits d'accès à haut risque ayant fait l'objet d'un accès au cours des 30 derniers jours ».
  - Avantages : vous permet d'effectuer des recherches précises à plusieurs niveaux pour identifier exactement les données dont vous avez besoin.

  Pour des informations complètes sur l'utilisation de ce générateur de requêtes, voir le Global Search Quick Reference Guide (Guide de référence rapide de la recherche globale, en anglais).
- **Recherche avec traitement automatique du langage naturel (NLP)**
  - Saisissez simplement votre demande en langage clair
  - Le système interprète intelligemment votre intention et la convertit en une requête structurée
  - Exemple : « Montre-moi tous les comptes utilisateur inactifs du service marketing »

- Avantages : convivial, ne nécessite aucune connaissance de la syntaxe des requêtes, idéal pour les recherches ponctuelles rapides

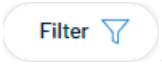
- **Recherche simple**
  - Recherche textuelle simple et rapide pour des résultats immédiats
  - Parfaite pour trouver des identités spécifiques et pour les simples consultations
  - Exemple : saisir un nom comme « John Smith » ou un identifiant d'employé
  - Avantages : instantanée, idéale pour les opérations quotidiennes et les vérifications rapides

Chaque type de recherche répond à différents besoins et scénarios utilisateur, de l'analyse de données complexe aux recherches d'identités rapides. Vous pouvez choisir la méthode de recherche la plus appropriée en fonction de la tâche en cours, de votre expertise technique et de la complexité des informations que vous recherchez.

Filtrer

Dans **Identités 360**, une fonction de filtrage permet de limiter ou d'affiner les données affichées en appliquant des critères spécifiques.

Pour appliquer un filtre :

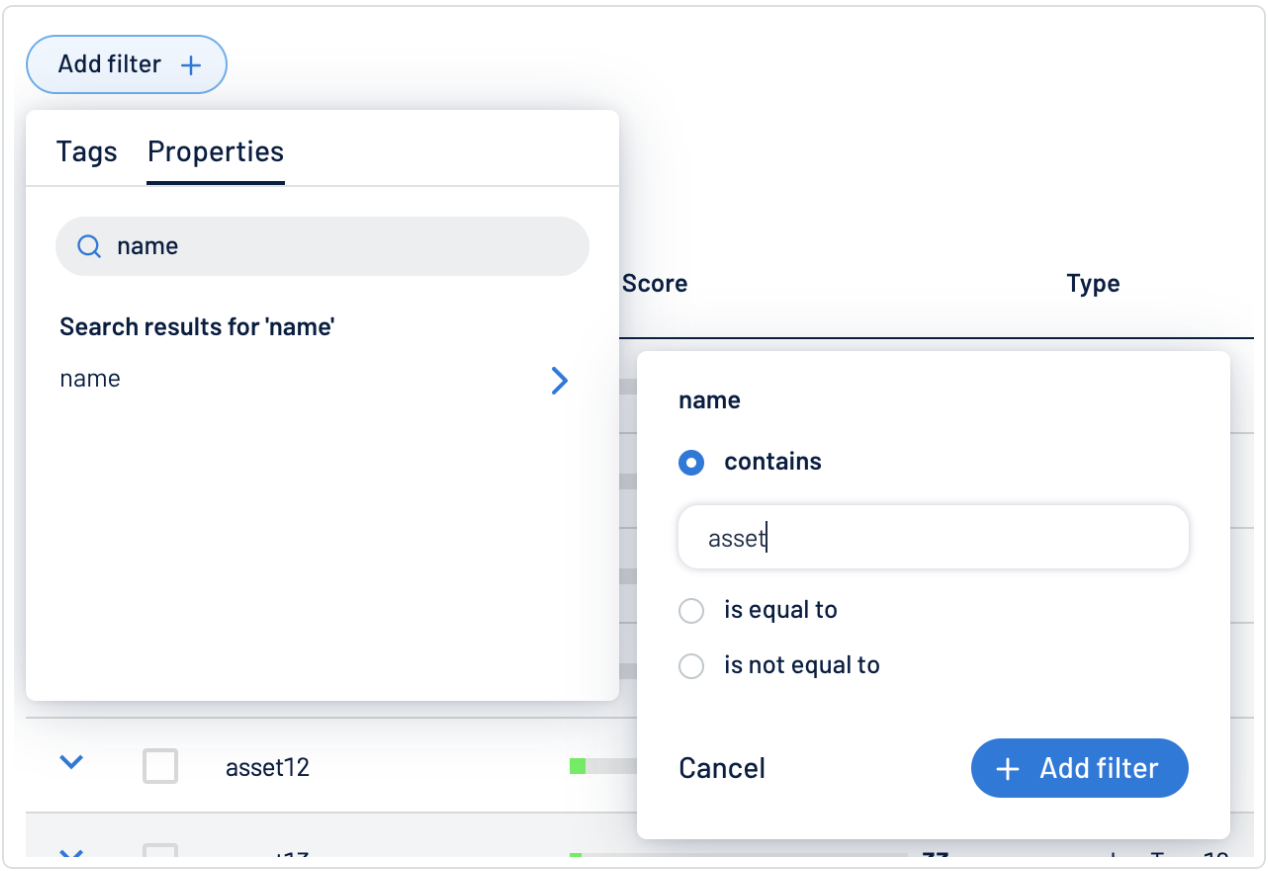
1. Dans l'en-tête de la page Identités, cliquez sur 

.

   Le bouton Ajouter un filtre apparaît.

2. Cliquez sur **Ajouter un filtre +**.

   Un menu apparaît.



3. Effectuez l'une des actions suivantes :
   - Pour effectuer une recherche par tag dans la liste des assets, cliquez sur **Tags** (valable uniquement avec la licence Tenable One et géré dans Tenable Inventory.)
   - Pour effectuer une recherche par propriété d'asset dans la liste des assets, cliquez sur **Propriétés**.
4. Dans la zone de recherche, saisissez les critères de recherche que vous souhaitez appliquer à la liste des assets.

   Tenable Inventory affiche une liste d'options en fonction de vos critères.
5. Cliquez sur le tag ou la propriété à utiliser pour filtrer la liste des assets.

   Un menu apparaît.
6. Sélectionnez le mode d'application du filtre. Par exemple, si vous souhaitez rechercher un asset dont le nom est « Asset14 », sélectionnez le bouton radio « contient » et saisissez « Asset14 » dans la zone de texte.

7. Cliquez sur **Ajouter un filtre**.

   Le filtre apparaît au-dessus de la liste des assets.

8. Répétez ces étapes pour chaque filtre supplémentaire que vous souhaitez appliquer.
9. Cliquez sur **Appliquer les filtres**.

   La page filtre la liste des identités selon les critères désignés.

Exporter

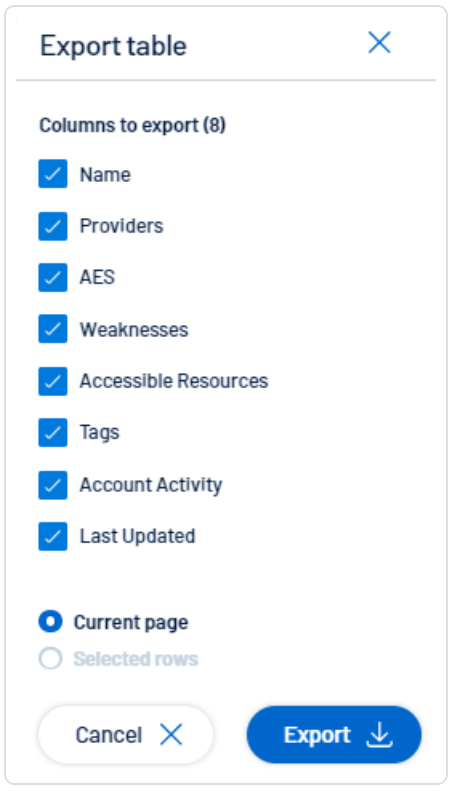
Vous pouvez exporter les données affichées dans le tableau au format Excel.

> **Remarque** : chaque onglet de la vue détaillée de l'identité propose sa propre option d'exportation, vous permettant d'extraire des ensembles de données plus ciblés.

Pour exporter des données :

1. Dans l'en-tête de la page Identités, cliquez sur l'icône .
2. Dans la fenêtre Exporter le tableau, sélectionnez les colonnes à exporter. Vous avez la

possibilité d'exporter la page actuelle ou les lignes sélectionnées.



3. Cliquez sur **Exporter**.

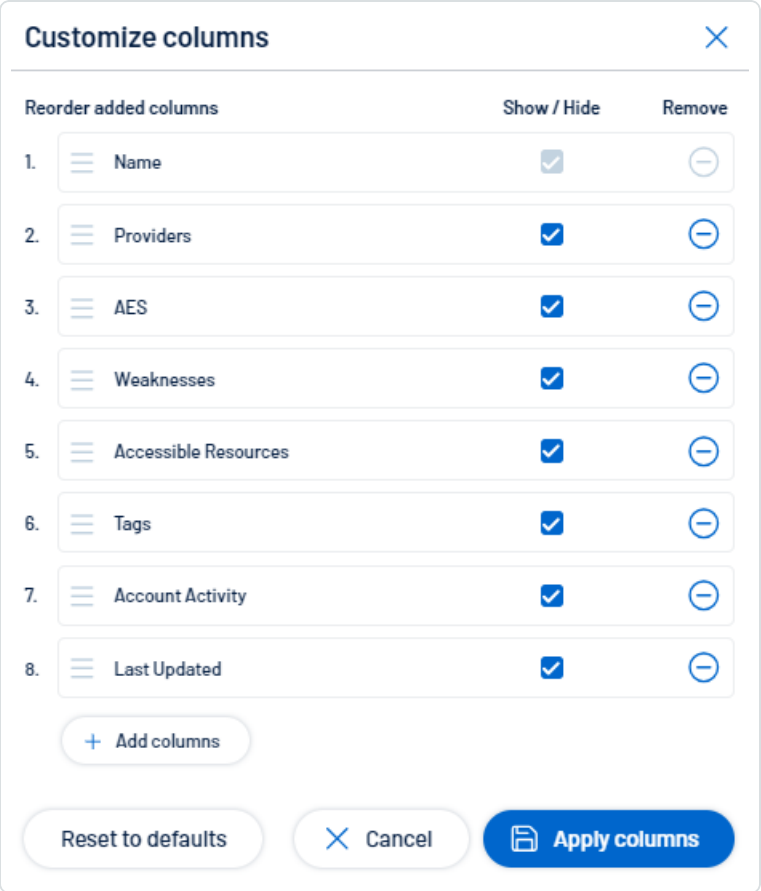
Personnaliser les colonnes

Vous pouvez ajouter, supprimer ou réorganiser des colonnes pour adapter l'affichage à vos préférences. Pour annuler les modifications, vous pouvez toujours rétablir les paramètres par défaut.

Pour personnaliser l'affichage des colonnes :

1. Dans l'en-tête de la page Identités, cliquez sur .

   La fenêtre Personnaliser les colonnes apparaît.



2. Facultatif :
    - Dans la section **Réorganiser les colonnes ajoutées**, cliquez sur n'importe quel nom de colonne et faites-le glisser pour réorganiser les colonnes.
    - Dans la section **Afficher/Masquer**, cochez/décochez les cases pour afficher ou masquer des colonnes du tableau.
    - Dans la section **Retirer**, cliquez sur le bouton pour supprimer définitivement une colonne du tableau.
    - Pour ajouter des colonnes au tableau, cliquez sur **Ajouter des colonnes**.

      La fenêtre **Ajouter des colonnes au tableau** apparaît.

        - (Facultatif) Utilisez la barre de recherche pour rechercher une propriété de colonne.

La liste des propriétés de colonne est mise à jour en fonction de votre requête de recherche.

- Cochez la case à côté des colonnes que vous souhaitez ajouter au tableau.
- Cliquez sur Ajouter.

  La colonne apparaît dans la fenêtre Personnaliser les colonnes.

3. Cliquez sur **Appliquer les colonnes**.

   Tenable enregistre les modifications apportées aux colonnes du tableau.

Affichage par défaut des colonnes

La disposition par défaut des colonnes met en avant les données clés tout en offrant une certaine flexibilité en matière de personnalisation.

- **Nom** – Champ obligatoire qui ne peut pas être masqué ni supprimé, car il sert d'identifiant principal pour chaque élément.
- **Fournisseurs** – Affiche le service ou la plateforme associés à l'élément.
- **AES** – Affiche le score AES (Score AES (Asset Exposure Score)).
- **Faiblesses** – Met en évidence les vulnérabilités ou les problèmes détectés pour les éléments répertoriés.
- **Ressources accessibles** – Affiche les ressources accessibles par le compte ou l'entité.
- **Tags** – Étiquettes ou métadonnées associées à chaque élément pour faciliter la catégorisation.
- **Activité du compte** – Journaux ou métriques liées à l'activité des comptes.
- **Dernière mise à jour** – Affiche la date la plus récente à laquelle l'élément a été mis à jour.

Pour rétablir l'affichage par défaut des colonnes :

- Cliquez sur **Rétablir les réglages par défaut** pour réinitialiser toutes les colonnes à leurs valeurs par défaut.

Comprendre l'appartenance à un tenant

L'appartenance à un tenant représente un lien unidirectionnel entre deux types d'assets au sein de l'écosystème d'un fournisseur d'identité :

1. **Un asset du fournisseur d'identité**, comme un compte utilisateur, un groupe ou une ressource.
2. **L'asset « tenant »**, qui représente l'entité ou le domaine plus large englobant l'asset. La nature du « tenant » dépend du fournisseur d'identité spécifique.

Cette appartenance permet d'identifier les relations entre les assets et leurs tenants, offrant ainsi un aperçu de l'organisation et de la hiérarchie des assets.

Lier des assets à un tenant

Dans le cas d'Active Directory (AD), les assets sont liés à leur tenant (domaine AD) à l'aide du **nom distinctif (DN)** de l'asset. Le DN fournit des informations hiérarchiques sur l'emplacement de l'asset au sein de la structure d'annuaire qui sont utilisées pour déterminer le tenant.

Identification du tenant

Lorsqu'un asset correspond à un objet AD (par exemple, un utilisateur ou un groupe), son tenant est identifié à l'aide des étapes suivantes :

- Extraction du **nom distinctif** de l'asset.
- Identification du tenant à partir des entrées de **composant de domaine (DC)** dans le DN.

Exemple

- DN de l'asset : `CN=UserA,CN=Users,DC=tenable,DC=corp`
- Tenant : `DC=tenable,DC=corp` (représentant le domaine AD).

Cas spéciaux : compréhension des liens de domaines racines de forêt

Dans certains cas, la relation entre un asset Active Directory (AD) et son tenant (domaine) peut ne pas suivre la structure attendue en raison de la façon dont AD gère certains objets. Cette section explique ces « cas spéciaux » plus en détail pour plus de clarté.

Que sont les domaines racines de forêt ?

Les forêts Active Directory sont constituées d'un ou plusieurs domaines organisés hiérarchiquement. Le **domaine racine de forêt** est le domaine le plus élevé de cette hiérarchie ; il englobe tous les autres domaines de la forêt. Certains objets au sein d'AD font référence au domaine racine de forêt dans leurs noms distinctifs, même s'ils appartiennent à un domaine différent. Ce comportement peut affecter l'identification des tenants.

Comment les cas spéciaux se produisent-ils ?

Lors de l'identification d'un tenant à partir du nom distinctif (DN) d'un asset, les composants de domaine (DC=...) indiquent généralement le domaine de l'asset. Cependant, il existe des exceptions :

1. **Objets de configuration à l'échelle de la forêt**
    - Certains objets AD sont liés à des configurations ou à des paramètres qui s'appliquent à l'ensemble de la forêt plutôt qu'à un domaine spécifique.
    - Ces objets ont des noms distinctifs se terminant par :
        - `CN=Configuration,DC=...`
    - De tels objets sont liés au **domaine racine de forêt** et non à leur domaine « réel ».

    #### Exemple

    - DN : `CN=Configuration,DC=forestRoot,DC=com`
    - Tenant : le **domaine racine de forêt** (`DC=forestRoot,DC=com`).
2. **Zones DNS de forêt**
    - Certains objets gèrent des zones DNS partagées sur l'ensemble de la forêt. Leurs noms distinctifs se terminent par :
        - `DC=ForestDnsZones,DC=...`
    - Ces objets sont associés au **domaine racine de forêt**, et non à leur domaine spécifique.

    #### Exemple

    - DN : `DC=ForestDnsZones,DC=forestRoot,DC=com`
    - Tenant : le **domaine racine de forêt** (`DC=forestRoot,DC=com`).

Pourquoi c'est important

Il est essentiel de comprendre ces cas spéciaux pour interpréter avec précision l'**appartenance à un tenant**. Les implications sont multiples :

1. **Le tenant identifié peut être différent de celui attendu**
    - Un objet semblant appartenir à un domaine spécifique peut en fait être lié au domaine racine de forêt.
    - Les objets dans les contextes d'attribution de noms « **Configuration** » ou « **ForestDnsZones** » sont liés au **domaine racine de forêt** en raison de leur portée à l'échelle de la forêt.
2. **Clarifications de la hiérarchie et de la portée**
    - Les objets liés au domaine racine de forêt ont généralement un champ d'application plus vaste, car ils gèrent ou représentent les paramètres au niveau de la forêt.
3. **Utilisation dans la résolution des problèmes et l'audit**
    - Une mauvaise interprétation de ces cas peut conduire à des erreurs lors de l'audit des structures de domaine ou de la résolution des problèmes liés à l'identité.

En comprenant ces nuances, vous pouvez interpréter en toute confiance les détections et garantir la précision des tâches d'audit et de résolution des problèmes.

Pourquoi Tenable Identity Explorer a choisi « tenant » comme nom de conteneur racine

Ce nom générique et non spécifique à l'IdP désigne le conteneur racine de chaque fournisseur d'identité (IdP). Il est conçu pour fonctionner sur différents systèmes, tels que les « tenants Entra » et les « domaines AD ».

Le terme « **tenant** » a été choisi car il est largement intelligible dans le contexte de la gestion des identités, neutre sur toutes les plateformes et déjà aligné sur des normes existantes telles que Microsoft Entra. Cela garantit la clarté, la cohérence et la flexibilité de la gestion de diverses implémentations d'IdP.

Trail Flow

Le Trail Flow de Tenable Identity Exposure affiche la surveillance et l'analyse en temps réel des événements qui affectent votre infrastructure AD. Il permet d'identifier les vulnérabilités critiques et les mesures correctives recommandées.

Dans la page **Trail Flow**, vous pouvez remonter dans le temps et charger des événements antérieurs ou rechercher des événements spécifiques. Vous pouvez également utiliser sa zone de recherche en haut de la page pour rechercher des menaces et détecter des modèles malveillants.

Le Trail Flow suit les événements suivants :

- **Modifications d'utilisateurs et de groupes** : inclut la création, la suppression et la modification de comptes et de groupes.
- **Modifications d'autorisations** : inclut les modifications apportées aux contrôles d'accès sur des objets tels que des fichiers, des dossiers et des imprimantes.
- **Ajustements de la configuration système** : implique les modifications des stratégies de groupe (GPO) et d'autres paramètres critiques.
- **Activités suspectes** : inclut les tentatives non autorisées, les élévations de privilèges et d'autres événements qui déclenchent des signaux d'alerte.

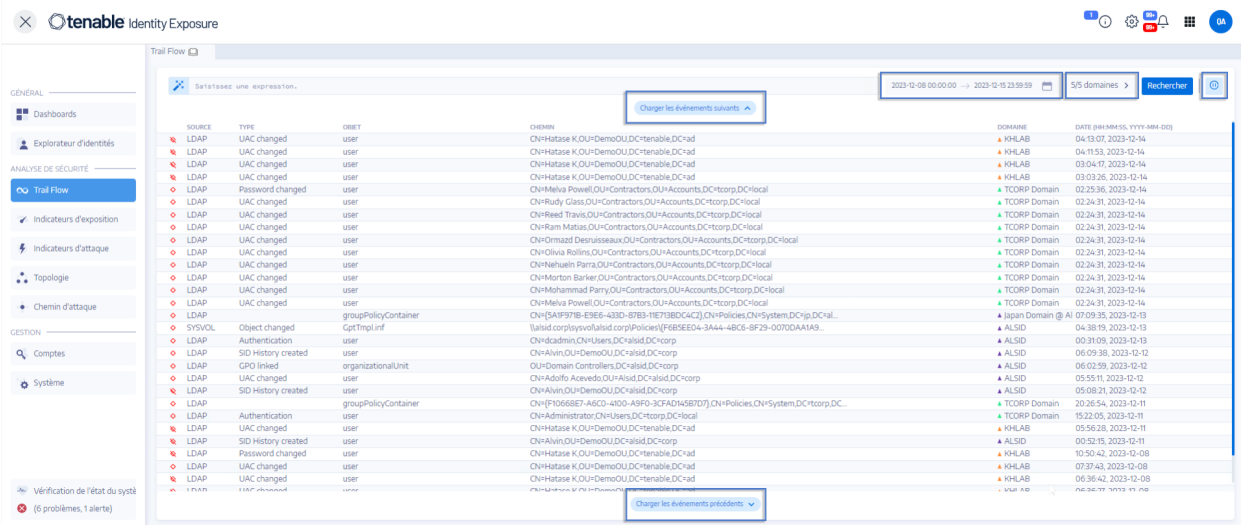
Tenable Identity Exposure propose les fonctionnalités suivantes pour exploiter les données du Trail Flow :

- **Recherche et filtrage** : navigation simple dans le flux d'événements à l'aide de mots-clés ou de critères spécifiques, permettant ainsi de concentrer l'attention sur des activités pertinentes tout en minimisant le bruit superflu.
- **Informations détaillées sur les événements** : chaque entrée d'événement fournit des détails exhaustifs qui incluent l'objet affecté, l'utilisateur responsable de la modification, le protocole utilisé et les indicateurs d'exposition (IoE) associés.
- **Relations visualisées** : les relations entre les événements sont représentées graphiquement pour éclairer la manière dont des activités, apparemment indépendantes les unes des autres, peuvent contribuer à une campagne d'attaque plus large.

Pour accéder au Trail Flow :

- Dans Tenable Identity Exposure, cliquez sur **Trail Flow** dans la barre de navigation sur la partie gauche.

  La page Trail Flow apparaît avec une liste d'événements. Pour plus d'informations, voir Tableau Trail Flow.



Pour sélectionner une période :

Pour sélectionner un domaine :

Pour afficher un événement :

Pour suspendre Trail Flow et le redémarrer :

Pour charger les événements suivants ou précédents :

Tableau Trail Flow

Tenable Identity Exposure répertorie en continu les événements de votre architecture Active Directory dans le tableau Trail Flow à mesure qu'ils se produisent. Il contient les informations suivantes :

Informations	Description

Source	Indique l'origine d'une modification d'ordre sécurité dans vos infrastructures AD. Il existe deux sources possibles : • Protocole LDAP (Lightweight Directory Access Protocol) utilisé pour communiquer avec votre infrastructur AD. • Protocole SMB (Server Message Block) utilisé pour partager des fichiers, des imprimantes, etc. **Tenable Identity Exposure** analyse en profondeur le trafic LDAP et SMB sur votre réseau pour détecter les anomalies et les menaces potentielles. **Remarque** : Active Directory (AD) permet aux administrateurs de créer des stratégies de groupe qui contrôlent les paramètres déployés dans les comptes des utilisateurs et des machines. La stratégie de groupe (GPO) stocke ces paramètres de contrôle. Le dossier SYSVOL stocke les fichiers GPO sur le contrôleur de domaine. Il est important de surveiller le contenu des GPO pour la sécurité de votre infrastructure AD, car chaque membre du domaine peut les appliquer ou les exécuter avec un haut niveau de privilèges.
Type	Affiche les éléments caractéristiques d'un événement tels que : • ACL modifiée • SPN modifié • Membre supprimé • Nouveau membre • Nouvelle relation d'approbation • Type de fichier inconnu ajouté • Nouvel objet • Objet supprimé • Mot de passe mis à jour • UAC modifié

	• Nouvelle GPO liée • Lien de GPO supprimé • Changement de propriétaire • Fichier renommé • SPN créé • Échec de réinitialisation de l'authentification • Échec de l'authentification
Objet	Indique la classe ou l'extension de fichier associée à un objet AD. Vous pouvez rechercher un objet d'annuaire (utilisateur, ordinateur, etc.) ou un fichier avec une extension spécifique (ini, XML, csv).
Chemin d'accès	Indique le chemin complet vers un objet AD pour identifier l'emplacement unique de l'objet dans l'infrastructure AD.
Annuaire	Indique l'annuaire d'où provient la modification de votre infrastructure AD.
Date	Indique la date de l'événement.

Lancer une recherche dans Trail Flow à l'aide de l'assistant

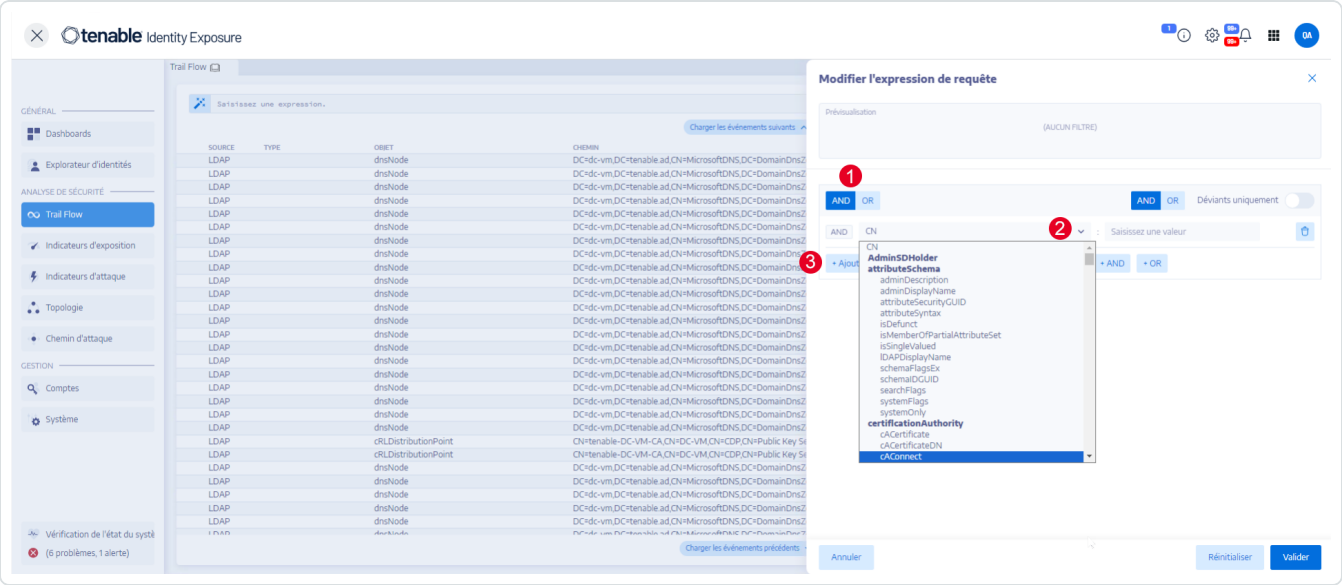
L'assistant de recherche vous permet de créer et de combiner des expressions de requête.

- Lorsque vous utilisez des expressions fréquentes dans la zone de recherche, vous pouvez les ajouter à une liste de favoris pour les réutiliser ultérieurement.
- Lorsque vous saisissez une expression dans la zone de recherche, Tenable Identity Exposure enregistre l'expression dans son volet Historique pour que vous puissiez la réutiliser.

Pour effectuer une recherche à l'aide de l'assistant :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez sur l'icône .

   Le volet **Modifier l'expression de requête** apparaît. Pour plus d'informations, voir Personnaliser les requêtes Trail Flow.



3. Pour définir l'expression de la requête dans le panneau, cliquez sur le bouton de l'opérateur **AND** ou **OR** (1) pour l'appliquer à la première condition.
4. Sélectionnez un attribut dans le menu déroulant et saisissez sa valeur (2).
5. Effectuez l'une des opérations suivantes :
    - Pour ajouter un attribut, cliquez sur **+ Ajouter une nouvelle règle** (3).
    - Pour ajouter une autre condition, cliquez sur **Ajouter une nouvelle condition** et sur l'opérateur **+AND** ou **+OR**. Sélectionnez un attribut dans le menu déroulant et saisissez sa valeur.
    - Pour limiter la recherche aux objets déviants, cliquez sur le bouton **Déviants uniquement**. Sélectionnez l'opérateur **+AND** ou **+OR** pour ajouter la condition à la requête.
    - Pour supprimer une condition ou une règle, cliquez sur l'icône .
6. Cliquez sur **Valider** pour lancer la recherche ou sur **Réinitialiser** pour modifier vos expressions de requête.

Voir aussi

- Recherche manuelle dans Trail Flow
- Lancer une recherche dans Trail Flow à l'aide de l'assistant
- Personnaliser les requêtes Trail Flow
- Ajouter des requêtes aux favoris
- Historique des requêtes

Recherche manuelle dans Trail Flow

Pour filtrer les événements qui correspondent à des chaînes de caractères ou à des modèles spécifiques, vous pouvez saisir une expression dans la zone de recherche afin d'affiner les résultats à l'aide des opérateurs booléens *****, **AND** et **OR**. Vous pouvez encapsuler des instructions **OR** avec des parenthèses pour modifier la priorité de recherche. La recherche identifie une valeur spécifique dans un attribut Active Directory.

Pour effectuer une recherche manuelle dans Trail Flow :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Dans la zone de recherche, saisissez une expression de requête.
3. Vous pouvez filtrer les résultats de la recherche comme suit :
    - Cliquez dans la zone **Calendrier** pour sélectionner une date de début et une date de fin.
    - Cliquez sur **n/n domaines** pour sélectionner des forêts et des domaines.
4. Cliquez sur **Rechercher**.

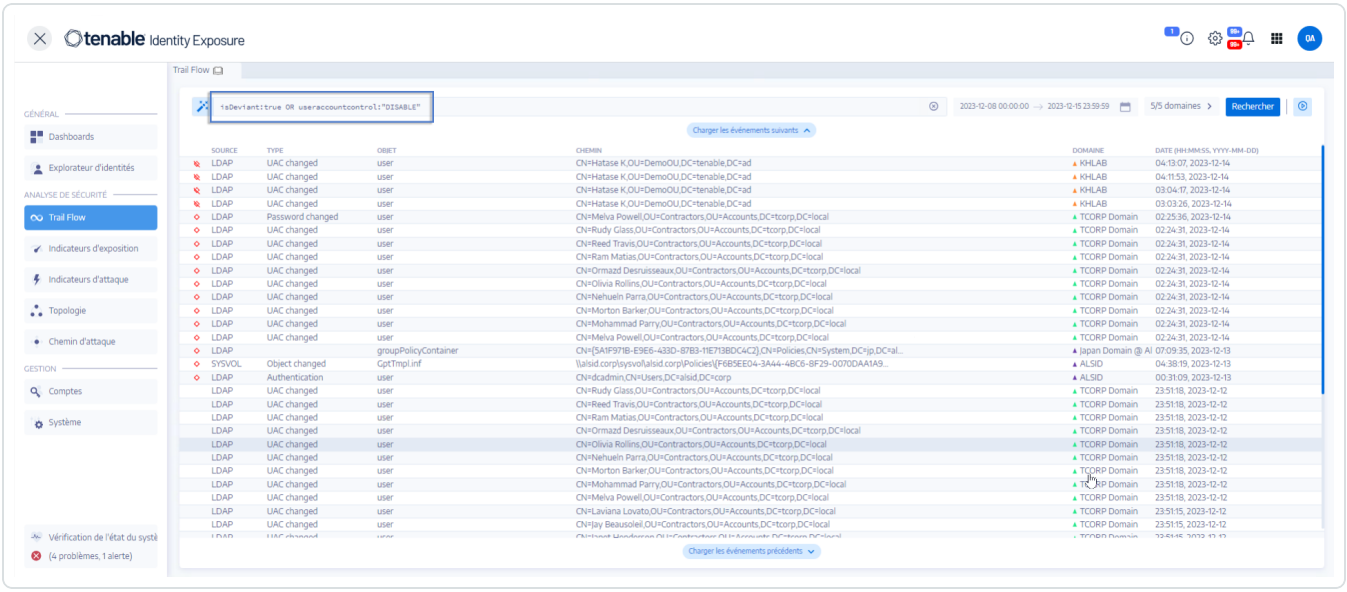
    Tenable Identity Exposure met à jour la liste avec les résultats correspondant à vos critères de recherche.

Conseil : pour effectuer une recherche à l'aide d'autres critères, vous pouvez Lancer une recherche dans Trail Flow à l'aide de l'assistant

Exemple :

L'exemple suivant recherche ce qui suit :

- Comptes utilisateur désactivés pouvant mettre en danger les infrastructures AD surveillées.
- Activités suspectes et utilisation anormale de compte.

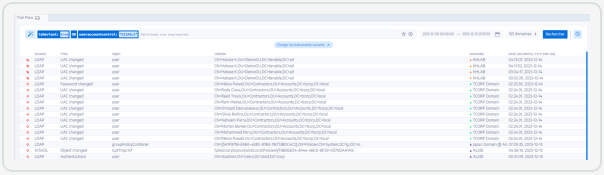


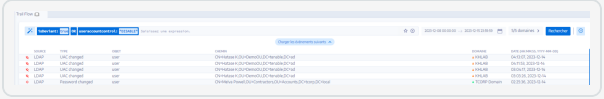
Personnaliser les requêtes Trail Flow

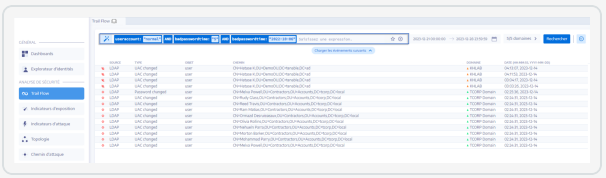
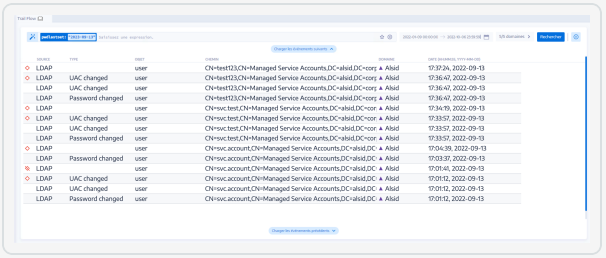
Le Trail Flow permet d'étendre les fonctionnalités Tenable Identity Exposure au-delà de la surveillance par défaut des indicateurs d'exposition et des indicateurs d'attaque. Vous pouvez créer des requêtes personnalisées pour récupérer rapidement des données et également utiliser la requête comme une alerte personnalisée que Tenable Identity Exposure peut envoyer à votre système de gestion des informations et des événements de sécurité (SIEM).

Les exemples suivants montrent des requêtes personnalisées pratiques dans Tenable Identity Exposure.

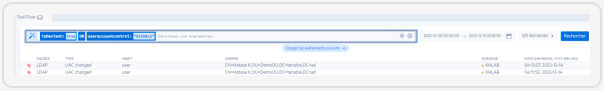
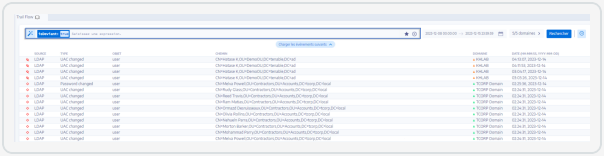
Cas d'utilisation	Description
Fichiers binaires de démarrage et d'arrêt de GPO et surveillance du chemin d'accès SYSVOL global	Surveille les scripts dans le chemin d'initialisation de l'amorçage et/ou le chemin d'accès de réplication SYSVOL global. Les attaquants utilisent généralement ces scripts pour tromper les services AD natifs, afin de faire proliférer rapidement les ransomwares dans un environnement. • **Scripts dans la requête de chemin de**

	démarrage :
	
	`globalpath: "sysvol" AND types: "Scriptsini"`
	
	Remarque : ici, `types` fait référence à l'attribut d'objet et non pas à l'en-tête de colonne.
	
	• **Requête de surveillance SYSVOL** :
	
	`globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")`
	
	

Modifications de la configuration d'une GPO	Surveille les modifications apportées aux configurations des GPO. Les attaquants utilisent généralement cette méthode pour rétrograder les paramètres de sécurité, afin de faciliter la persistance et/ou la prise de contrôle de compte. • **Requête de surveillance de GPO :** `gptini-displayname:"New Group Policy Object" AND changetype:"Changed"` 
Échec de l'authentification et de la réinitialisation du mot de passe	Surveille les tentatives d'authentification qui ont échoué à plusieurs reprises et qui ont abouti à un verrouillage,

	ce qui peut constituer un signal d'alerte annonciateur de tentatives d'attaque par force brute.
	
	Remarque : vous devez définir la stratégie de verrouillage et les variables de date/heure. Pour plus d'informations, voir Authentification à l'aide d'un compte Tenable Identity Exposure.
	
	• **Échec de la requête d'authentification :**
	
	`useraccountcontrol:"Normal" AND badpwdcount:"<ACCOUNT_LOCKOUT_THRESHOLD>" AND badpasswordtime:"<DATE_TIME_STAMP>"`
	
	
	
	• **Requête de réinitialisation du mot de passe :**
	
	`pwdlastset:"<DATE_TIME_STAMP"`
	
	

Autorisations d'objet ajoutées, supprimées ou modifiées	Surveille les modifications non autorisées des droits de l'ACL et des groupes d'autorisations d'objets associés. Les attaquants abusent de cette méthode pour élever les autorisations. **Remarque** : vous devez définir la variable date/heure.

	• **Requête d'autorisations d'objet :** `ntsecuritydescriptor:0 AND whenchanged:"DATE_TIME_STAMP"` 
Modifications apportées aux administrateurs entraînant une déviance	Les groupes d'administration intégrés et les groupes personnalisés sont des groupes sensibles qui nécessitent de surveiller attentivement les déviances ou les modifications de configuration pouvant introduire des risques. Cette requête permet d'examiner rapidement les modifications récentes qui auraient pu affecter négativement les paramètres de sécurité au sein du groupe d'administrateurs. • **Modifications apportées à la requête Admins :** `isDeviant:true AND cn:"admins"` 

Voir aussi

- Recherche manuelle dans Trail Flow
- Lancer une recherche dans Trail Flow à l'aide de l'assistant
- Ajouter des requêtes aux favoris
- Historique des requêtes
- Cas d'utilisation du Trail Flow

Ajouter des requêtes aux favoris

Lorsque vous utilisez fréquemment des expressions de requête, vous pouvez les ajouter à une liste de favoris personnalisés pour les réutiliser.

Pour ajouter une expression de requête à vos favoris :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez sur l'icône  en regard de la zone de recherche.

   Le volet **Modifier l'expression de requête** apparaît.
3. Dans la zone de recherche, saisissez une expression de requête.
4. Cliquez sur l'icône  en regard de la zone de recherche.

   La boîte **Ajouter à vos favoris** apparaît.
5. Dans la zone **Choisir un dossier**, cliquez sur la flèche déroulante pour sélectionner un dossier dans la liste.
6. (Facultatif) Cliquez sur le curseur **Créer un dossier** pour activer **Oui**. Dans la zone **Nom du dossier**, saisissez le nom du dossier de favoris.
7. Dans la zone **Nom du favori**, saisissez le nom du favori.
8. Cliquez sur **Ajouter**.

   Un message confirme que Tenable Identity Exposure a ajouté le favori à la liste.

Pour utiliser un favori d'expression de requête :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez dans la zone de recherche.

   Les onglets **Historique** et **Favoris** apparaissent sous la zone de recherche.
3. Cliquez sur l'onglet **Favoris**.

   La liste des favoris apparaît.
4. Cliquez sur le favori pour le sélectionner.

   Tenable Identity Exposure charge l'expression de requête et lance la recherche.

Pour gérer vos favoris :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez dans la zone de recherche.

   Les onglets **Historique** et **Favoris** apparaissent sous la zone de recherche.
3. Cliquez sur l'onglet **Favoris**.

   La liste des favoris apparaît.
4. Cliquez sur **Gérer vos favoris**.

   Le volet **Favoris** apparaît.
5. Effectuez l'une des opérations suivantes :
   - Rechercher un favori :
     a. Saisissez le nom du favori dans la zone de recherche.
     b. Sélectionnez un dossier dans la liste déroulante.
   - Modifier le nom d'un favori ou d'un dossier de favoris :
     a. Cliquez sur l'icône  du favori ou du dossier de favoris.
     b. Dans la zone **Nom du favori** ou **Nom du dossier**, saisissez un nouveau nom de favori ou de dossier de favoris.
     c. Cliquez sur **Modifier**.

        Un message confirme que Tenable Identity Exposure a mis à jour le nom du favori ou du dossier.
   - Supprimer un favori du dossier de favoris :
     - Cliquez sur l'icône  du favori ou du dossier de favoris.

Voir aussi

- Recherche manuelle dans Trail Flow
- Lancer une recherche dans Trail Flow à l'aide de l'assistant
- Personnaliser les requêtes Trail Flow
- Historique des requêtes
- Cas d'utilisation du Trail Flow

Historique des requêtes

Lorsque vous saisissez une expression dans la zone de recherche, Tenable Identity Exposure enregistre l'expression dans son volet **Historique** pour que vous puissiez la réutiliser.

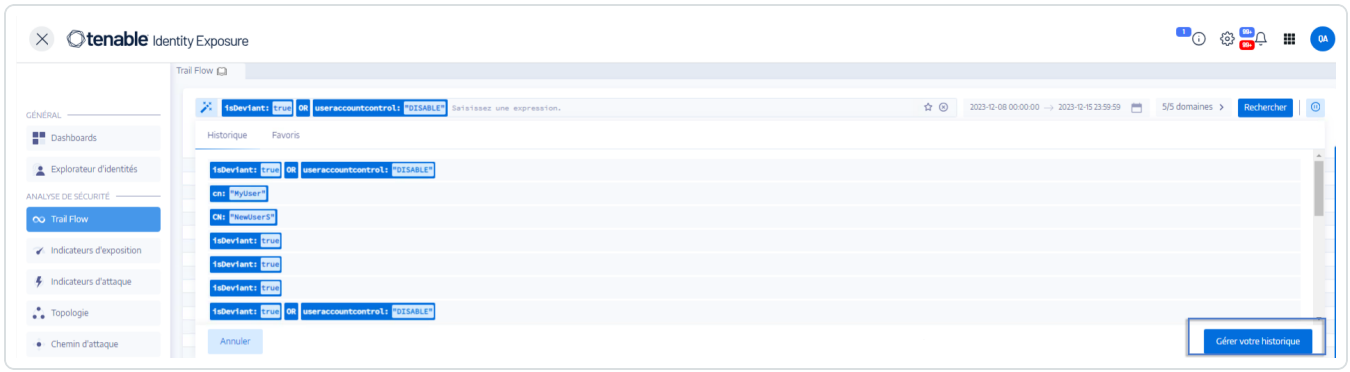
Pour utiliser une expression de requête de l'historique :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez dans la zone de recherche.

   Les onglets **Historique** et **Favoris** apparaissent sous la zone de recherche.
3. Cliquez sur l'onglet **Historique**.

   La liste des expressions de requête apparaît.
4. Cliquez pour sélectionner une expression de requête à utiliser.

   Tenable Identity Exposure charge l'expression de requête et lance la recherche.



Pour gérer l'historique de vos expressions de requête :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez dans la zone de recherche.

   Les onglets **Historique** et **Favoris** apparaissent sous la zone de recherche.
3. Cliquez sur l'onglet **Historique**.

   La liste des expressions de requête apparaît.
4. Cliquez sur **Gérer votre historique**.

   Le volet **Historique** apparaît.
5. Effectuez l'une des opérations suivantes :
   - Pour rechercher une expression de requête :
     a. Dans la zone de recherche, saisissez une expression de requête.
     b. Cliquez dans la zone de calendrier pour sélectionner une date de début et une date de fin.
     c. Cliquez sur **Rechercher**.
   - Pour utiliser une expression de requête dans l'historique :
     - Cliquez sur l'icône .
   - Pour supprimer toutes les expressions de requête de l'historique :
     a. Cliquez sur **Effacer la sélection**.

        Un message demande de confirmer la suppression.
     b. Cliquez sur **Confirmer**.

Voir aussi

- Recherche manuelle dans Trail Flow
- Lancer une recherche dans Trail Flow à l'aide de l'assistant
- Personnaliser les requêtes Trail Flow

- Ajouter des requêtes aux favoris
- Cas d'utilisation du Trail Flow

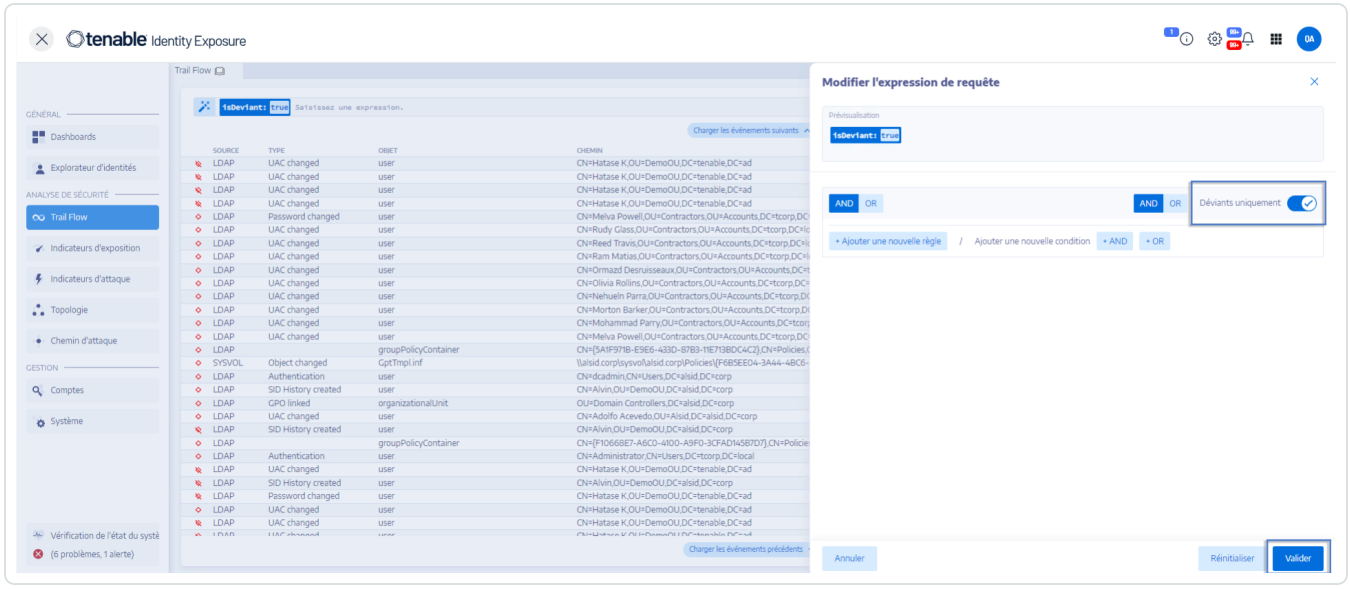
Afficher les événements déviants

Dans le tableau Trail Flow, vous pouvez vous concentrer directement sur les événements déviants.

Pour afficher uniquement les événements déviants :

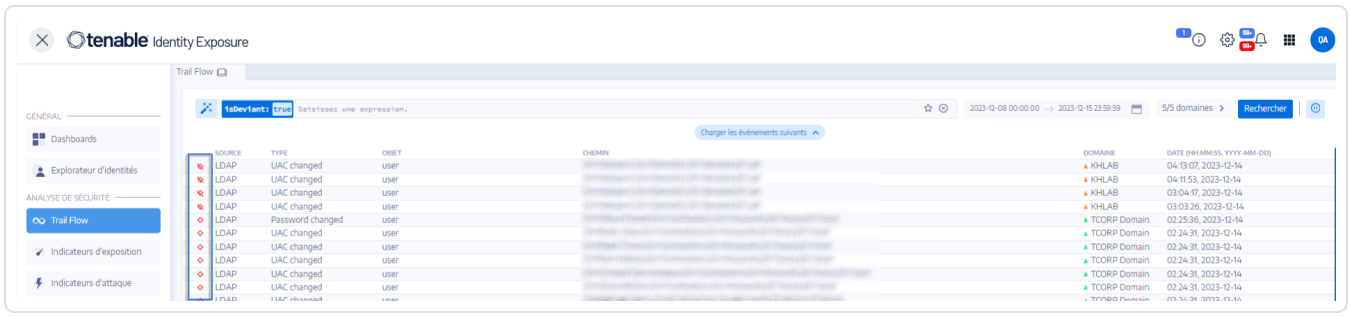
1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez sur l'icône en regard de la zone de recherche.

   Le volet **Modifier l'expression de requête** apparaît.



3. Cliquez sur le curseur **Déviants uniquement** pour n'afficher que les événements déviants.
4. Cliquez sur **Valider**.

   Tenable Identity Exposure met à jour le tableau Trail Flow et affiche une liste d'événements avec un losange rouge à côté de la source.



Dans ces commandes :

- Trail Flow a détecté une déviance dans le profil de sécurité Tenable Identity Exposure.
- Trail Flow a détecté une déviance dans d'autres profils de sécurité.
- Les changements ont résolu la déviance.

Détails d'un événement

Le flux de suivi (Trail Flow) dans Tenable Identity Exposure fournit des informations détaillées sur chaque événement qui affecte votre infrastructure Active Directory (AD). Les détails d'un événement permettent d'examiner les informations techniques et de prendre les mesures correctives requises par le niveau de sévérité de l'indicateur d'exposition (IoE).

Pour afficher les détails d'un événement :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez pour sélectionner une entrée dans le tableau Trail Flow.

   Le volet **Détails de l'événement** apparaît.

IoE, événement et objet déviant

- Un **indicateur d'exposition** (IoE) décrit une menace qui affecte l'infrastructure AD. Les IoE de Tenable Identity Exposure évaluent les niveaux de sécurité après avoir reçu un événement en temps réel. Les IoE peuvent inclure plusieurs vulnérabilités techniques. Ils fournissent des informations sur les vulnérabilités détectées, les objets déviants associés et des recommandations en termes d'actions correctives.

- Un **événement** indique une modification de la sécurité qui peut apparaître dans une infrastructure AD. Il peut s'agir d'un changement de mot de passe, de la création d'un utilisateur, de la création ou de la modification d'une GPO, de la création d'un droit délégué, etc. Un événement peut rendre non conforme un IoE conforme.
- Un **objet déviant** est un élément technique, seul ou associé à un autre objet déviant, qui permet au vecteur d'attaque de l'IoE de fonctionner. Pour plus d'informations, voir Indicateurs d'exposition.

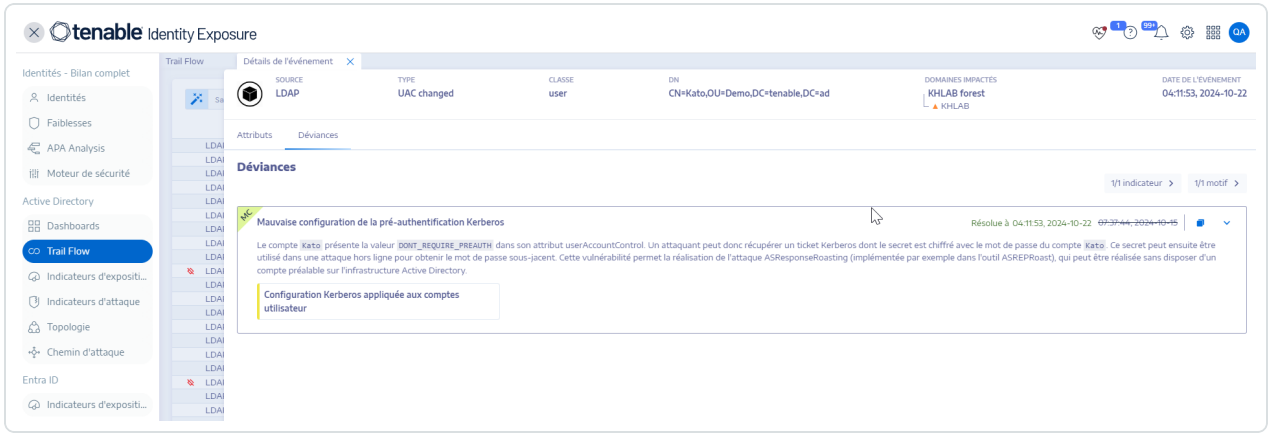


Tableau des attributs

Le tableau Attributs contient les colonnes suivantes :

Colonne	Description
Attributs	Indique les attributs de l'objet AD associé à l'événement que vous avez sélectionné dans le tableau Trail Flow. Les attributs décrivent les caractéristiques de l'objet. Plusieurs attributs peuvent décrire un seul objet AD.
Valeur à l'événement	Indique la valeur de l'attribut au moment de l'événement.
Valeur actuelle	Indique la valeur de l'attribut dans l'infrastructure AD au moment où vous le visualisez.

Conseil : pour afficher la valeur de l'attribut avant l'occurrence de l'événement, survolez le point bleu à gauche (le cas échéant).

Pour rechercher un attribut :

- Dans le volet **Détails de l'événement**, saisissez une chaîne dans la zone de recherche.

  Tenable Identity Exposure réduit la liste aux attributs correspondant à la chaîne de recherche.

Pour plus d'informations, voir Changements d'attribut.

Déviances

Si un événement du Trail Flow contient des déviances, le volet Détails de l'événement les affiche également pour vous permettre d'accéder à la source du problème.

Tenable Identity Exposure lie une déviance à un objet racine et peut l'associer à plusieurs attributs incriminants. Lorsque vous résolvez l'un de ces attributs, Tenable Identity Exposure résout la déviance sur l'objet racine. Il crée ensuite une nouvelle déviance pour l'objet racine, en gardant le même motif mais en incluant uniquement les attributs non résolus.

Par exemple, Tenable Identity Exposure lie une déviance à l'objet **A** pour un motif unique qui se connecte à plusieurs objets associés (**B**, **C**et **D**). Lorsque vous résolvez l'attribut incriminant sur l'objet **C**, Tenable Identity Exposure résout la déviance sur l'objet **A**. Il crée ensuite une nouvelle déviance pour l'objet **A**, en la liant au même motif mais en incluant uniquement les objets **B** et **D**.

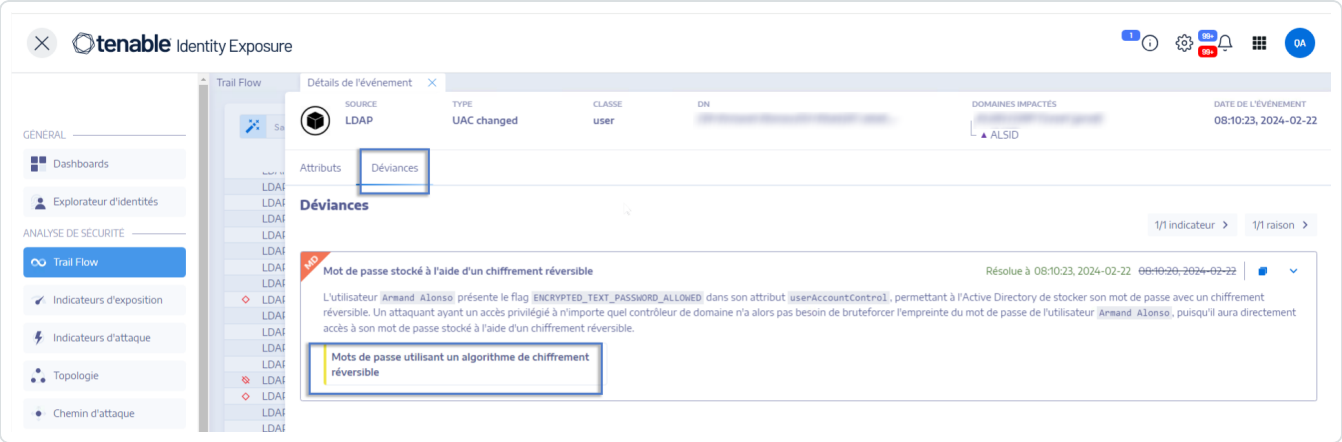
Au cours de ce processus, Tenable Identity Exposure peut générer un événement Trail Flow qui affiche plusieurs déviances comme étant résolues et rouvertes au même horodatage.

Pour afficher les déviances :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez pour sélectionner une entrée dans le tableau Trail Flow.

   Le volet **Détails de l'événement** apparaît.
3. Cliquez sur l'onglet **Déviances**.

   Tenable Identity Exposure affiche la liste des déviances et les IoE qui les ont déclenchées.



Pour accéder aux détails de l'IoE :

1. Dans l'onglet **Déviances**, cliquez sur la tuile IoE sous la raison de la déviance.

   Le volet **Détails de l'indicateur** apparaît avec la liste des objets déviants et les informations suivantes :

   - Nom de l'IoE
   - Sévérité de l'IoE (critique, élevée, moyenne, faible)
   - Statut de l'IoE
   - Horodatage de la dernière détection

2. Cliquez sur l'un des onglets suivants :

   - **Informations** : contient les ressources internes et externes sur l'IoE.
   - **Détails de la vulnérabilité** : fournit des explications sur la faille détectée dans votre infrastructure AD.
   - **Objets déviants** : contient des détails techniques et une zone de recherche pour filtrer les objets.
   - **Recommandations** : contient des conseils sur la façon de résoudre le problème.

Changements d'attribut

Lorsque la valeur d'un attribut change, un point bleu figure avant la colonne **Attribut** dans le Trail Flow.

Pour afficher le changement d'attribut :

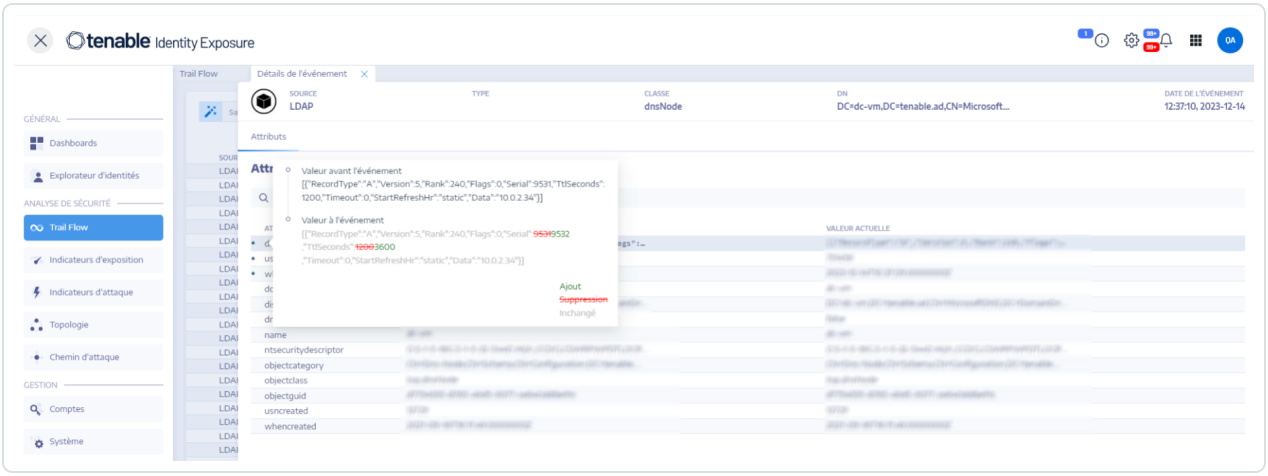
1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** dans la barre de navigation sur la partie gauche.

   La page **Trail Flow** apparaît avec une liste d'événements.

2. Survolez le point bleu devant la ligne d'événement pour afficher les modifications.

   La couleur de l'étiquette **Valeur à l'événement** dépend des modifications appliquées à l'attribut :

   - Vert – **Ajout**
   - Rouge – **Suppression**
   - Gris – **Inchangé**



Attribut « ntsecuritydescriptor »

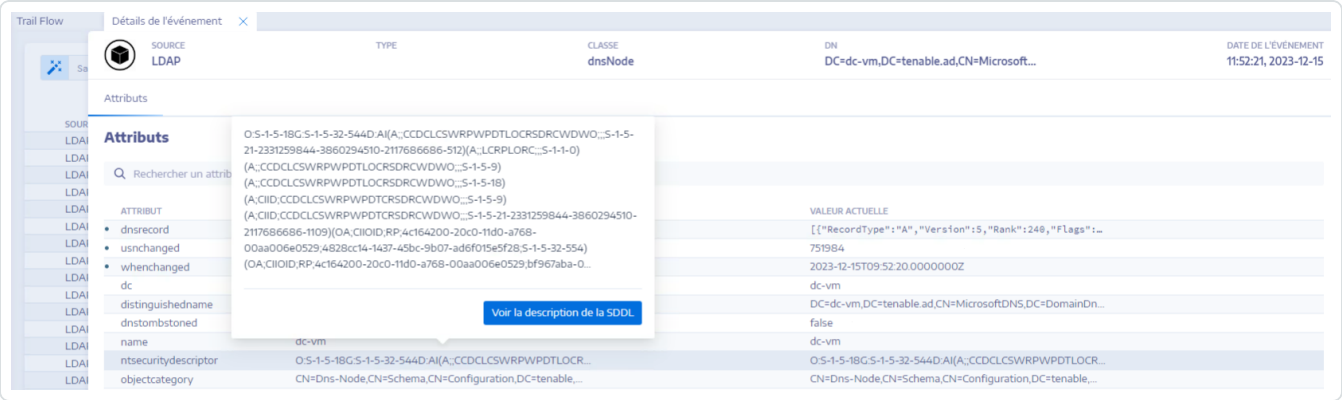
Un descripteur de sécurité est une structure de données qui contient des informations de sécurité sur un objet AD, telles que sa propriété et ses autorisations. Pour plus d'informations, voir la documentation en ligne de Microsoft.

Pour afficher les informations du descripteur de sécurité d'un objet :

1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez pour sélectionner une entrée dans le tableau Trail Flow.

Le volet **Détails de l'événement** apparaît.

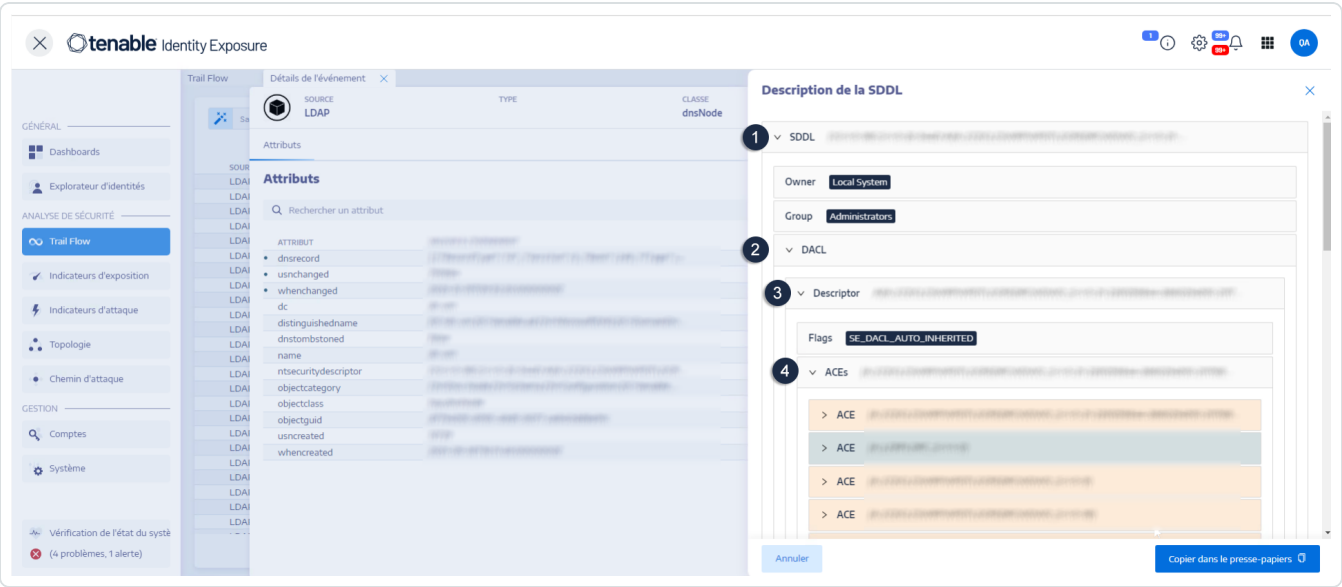
3. Survolez l'entrée d'attribut `ntsecuritydescriptor` avec la souris (colonne Valeur à l'événement ou Valeur actuelle) **.



4. Cliquez sur **Voir la description de la SDDL**.

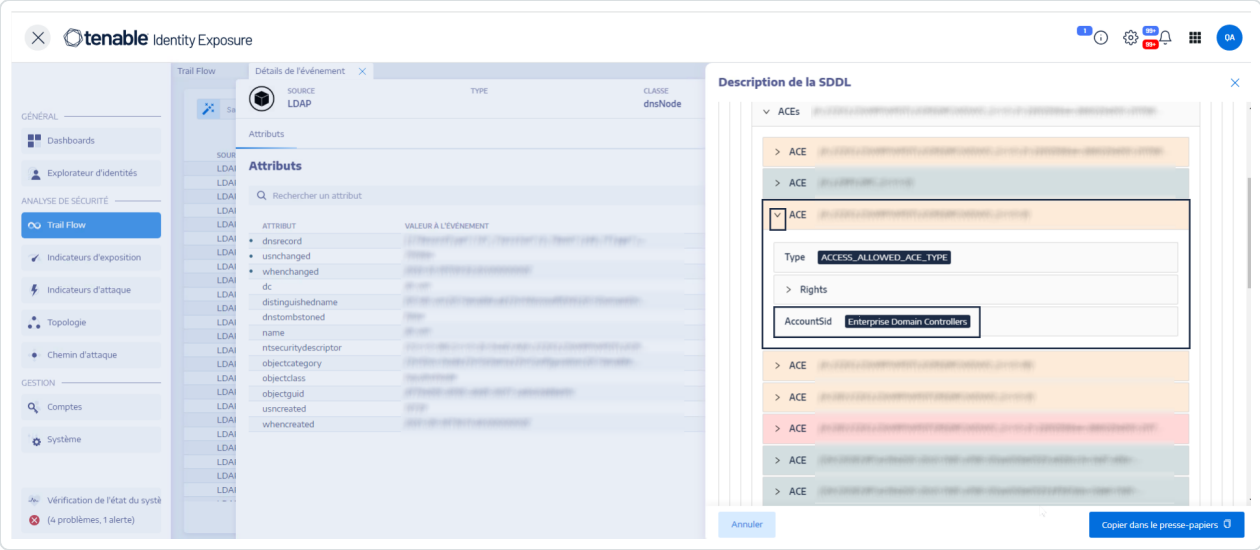
   Le volet **Description de la SDDL** apparaît.

5. Cliquez sur les flèches à gauche de SDDL (1), DACL (2) et Descripteur (3) pour développer la description :



6. Accédez à une entrée de contrôle d'accès (ACE) (4) en couleur pour afficher les droits d'accès à l'objet. Couleurs et signification :

- **Rouge** : des utilisateurs disposent de droits potentiellement dangereux et ne doivent pas disposer de droits d'accès à l'objet.
- **Orange** : des utilisateurs dotés de privilèges disposent de droits potentiellement dangereux, mais ils disposent généralement de ce type de droit (par exemple : Administrateurs de domaine).
- **Vert** : aucun droit potentiellement dangereux sur l'objet n'a été accordé.



7. Pour copier la description de la SDDL, cliquez sur **Copier dans le presse-papiers**.

Cas d'utilisation du Trail Flow

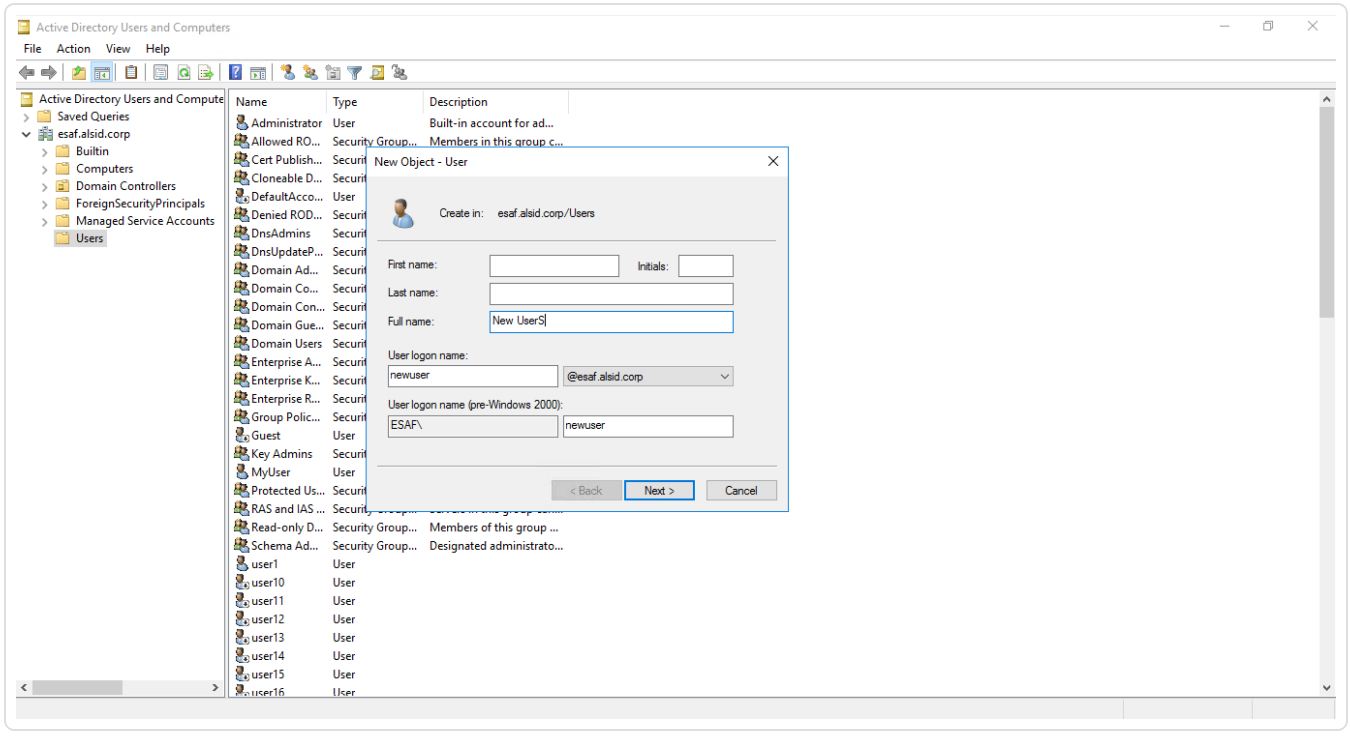
Pour comprendre le comportement du Trail Flow, deux exemples montrent comment une opération que vous effectuez dans votre interface Active Directory (AD) est répercutée dans la page Trail Flow.

Chaque exemple compare les données du point de vue de l'administrateur (dans l'interface AD) avec celles du point de vue de l'utilisateur final (dans Tenable Identity Exposure). Que vous utilisiez une application, une API ou un service pour effectuer une opération sur votre interface AD, le résultat sur le Trail Flow est le même.

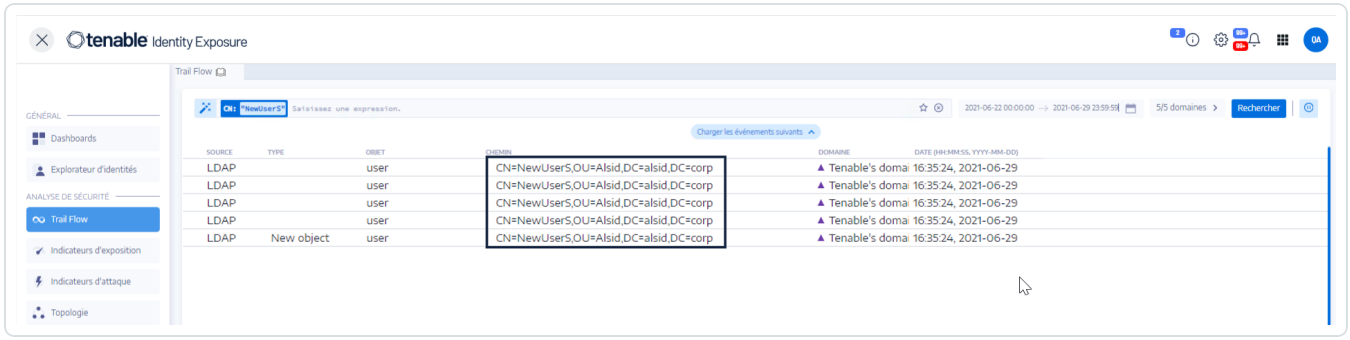
> **Remarque** : ces exemples ne sont pas exhaustifs et ne peuvent couvrir toutes les situations possibles.

Que se passe-t-il dans le Trail Flow lorsque vous créez un compte utilisateur AD ?

- Côté administrateur, vous saisissez diverses informations sur le nouveau compte utilisateur.

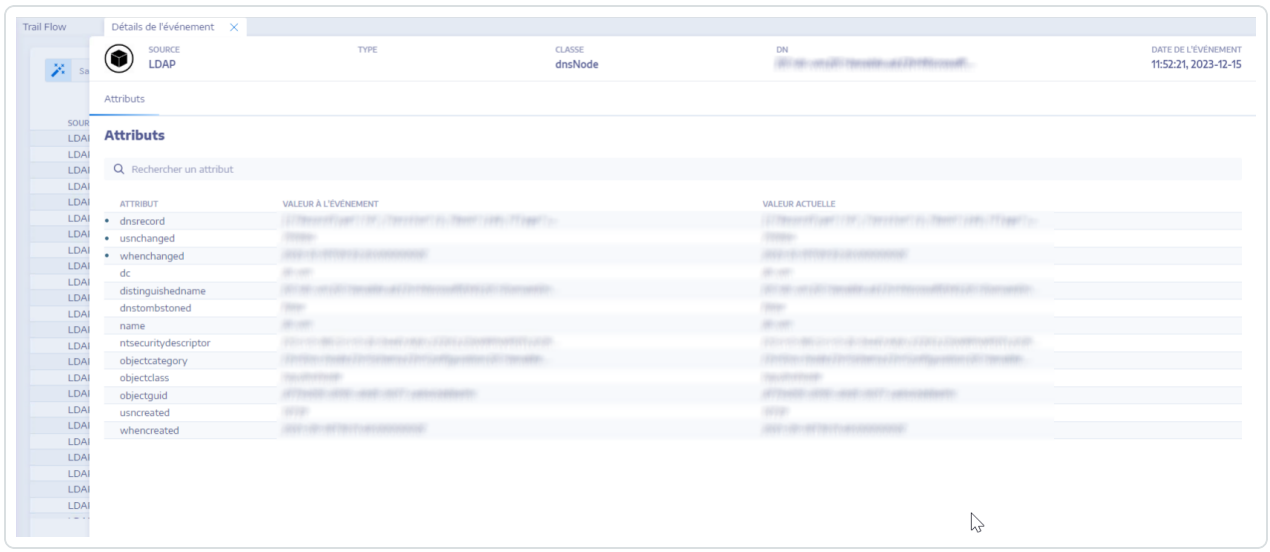


- Côté utilisateur final, Tenable Identity Exposure met à jour la page **Trail Flow**. Consultez la colonne **Type** indiquant *Nouvel objet*.



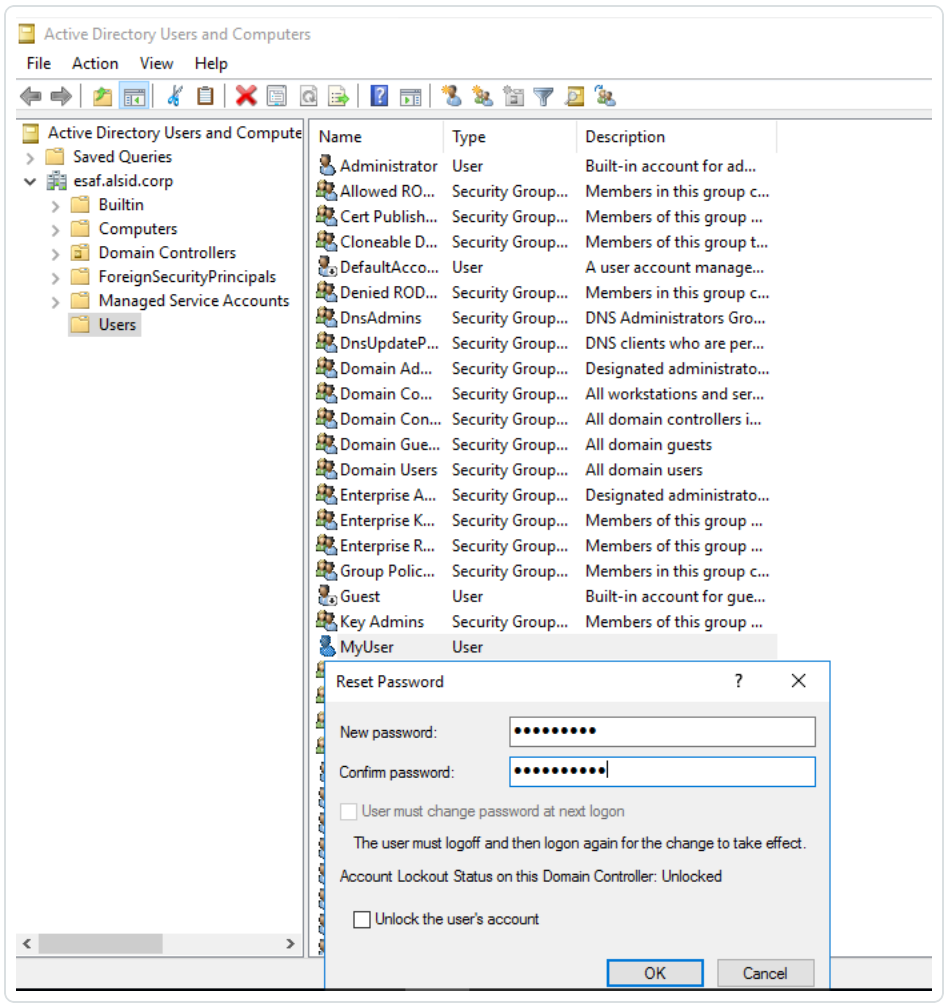
- La page **Détails de l'événement** reflète également ce changement. Le point bleu à gauche des noms d'attributs indique qu'une modification a eu lieu.

  Pour plus de détails sur les attributs, voir Détails d'un événement.

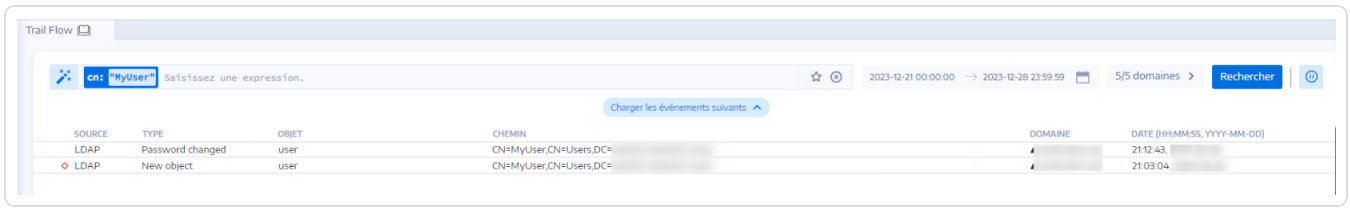


Que se passe-t-il dans le Trail Flow lorsque vous modifiez le mot de passe d'un utilisateur AD ?

- Côté administrateur, vous saisissez diverses informations pour réinitialiser le mot de passe d'un utilisateur.

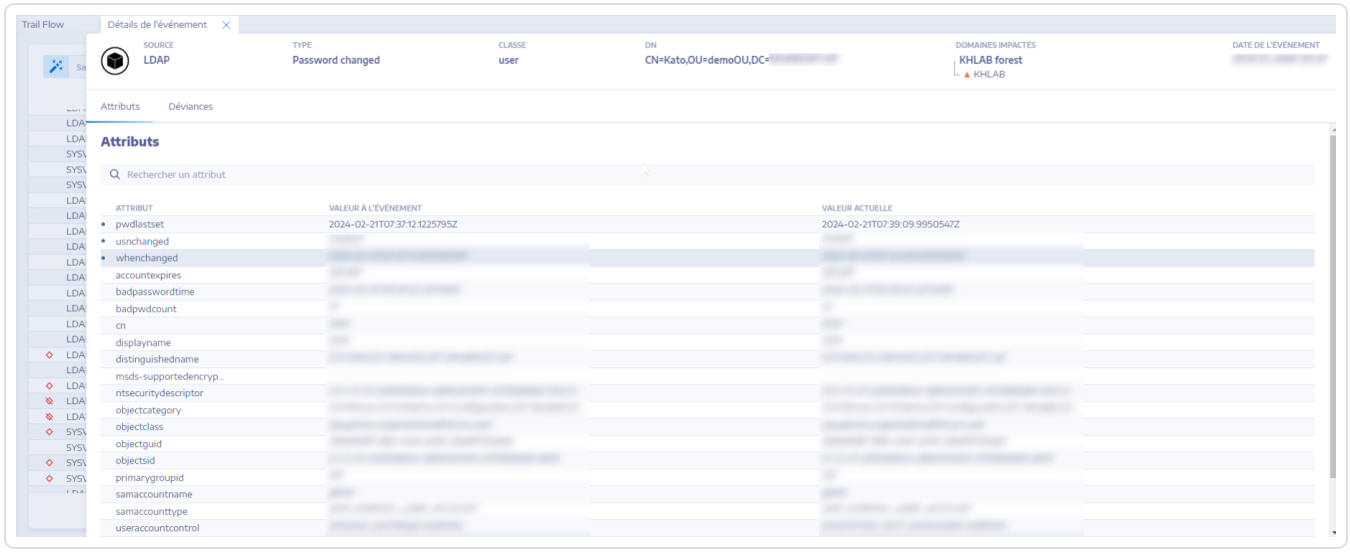


- Côté utilisateur final, Tenable Identity Exposure met à jour la page **Trail Flow**. Consultez la colonne **Type** indiquant « Mot de passe mis à jour ».



- La page **Détails de l'événement** reflète également ce changement avec un point bleu à gauche de l'attribut `whenchanged`.

Pour plus de détails sur les attributs, voir Détails d'un événement.



Voir aussi

- Recherche manuelle dans Trail Flow
- Lancer une recherche dans Trail Flow à l'aide de l'assistant
- Personnaliser les requêtes Trail Flow
- Ajouter des requêtes aux favoris
- Historique des requêtes

Indicateurs d'exposition

Tenable Identity Exposure mesure la maturité de la sécurité de vos infrastructures AD par le biais d'indicateurs d'exposition (IoE) et attribue des niveaux de sévérité au flux d'événements qu'il surveille et analyse. Tenable Identity Exposure déclenche des alertes lorsqu'il détecte des régressions de sécurité.

Pour afficher les IoE :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'exposition** dans le volet de navigation.

Le volet **Indicateurs d'exposition** apparaît. Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des déviances.

2. (Facultatif) Pour afficher tous les IoE, cliquez sur le curseur **Afficher tous les indicateurs** pour activer l'option **Oui**.

Les IoE Tenable Identity Exposure sont dotés d'une série de fonctionnalités conçues pour renforcer vos capacités d'investigation :

- Recherche et filtrage : explorez facilement l'IoE en appliquant des filtres basés sur la forêt et le domaine.
- Capacité d'exportation : l'objet déviant vous permettra d'exporter les IoE au format CSV.
- Action sur les incidents IoE : supprimez une exposition de la liste blanche pour la réactiver.

Les données des IoE incluent :

- Section Informations : cette section fournit un résumé de chaque indicateur d'exposition (IoE), en précisant les outils d'attaque connus, les domaines affectés et la documentation pertinente.
- Détails de la vulnérabilité : cette section fournit des informations plus détaillées concernant la mauvaise configuration d'Active Directory.
- Objets déviants : cette section met en évidence les mauvaises configurations d'Active Directory qui peuvent contribuer à élargir la surface d'attaque.
- Recommandation : cette section détaille des stratégies de configuration efficaces pour minimiser votre surface d'attaque.

Pour rechercher un IoE :

1. En haut de la page **Indicateurs d'exposition**, saisissez une chaîne dans la zone de recherche. Vous pouvez saisir n'importe quel terme lié à un IoE (mot de passe, utilisateur, connexion, etc.).
2. Appuyez sur Entrée.

   La page IoE est actualisée et affiche les indicateurs associés à votre terme de recherche.

Pour filtrer les IoE d'une forêt ou d'un domaine spécifique :

1. Cliquez sur **n/n domaines**.

   Le volet **Forêts et domaines** apparaît.

2. Sélectionnez la forêt ou le domaine.
3. Cliquez sur **Filtrer sur la sélection**.

Niveau de sévérité

Les niveaux de sévérité permettent d'évaluer la sévérité des vulnérabilités détectées et de prioriser les actions de remédiation.

Le volet **Indicateurs d'exposition** affiche les IoE comme suit :

- Par niveau de sévérité en utilisant des codes couleur.
- Verticalement – du plus sévère au moins sévère (rouge pour la priorité absolue et bleu pour la priorité la plus basse).
- Horizontalement – du plus complexe au moins complexe. Tenable Identity Exposure calcule dynamiquement l'indicateur de complexité afin d'indiquer le niveau de difficulté de la correction de l'IoE déviant.

Sévérité	Description
Critique – Rouge	Indique comment empêcher les attaques et la compromission de l'infrastructure Active Directory par certains utilisateurs sans privilèges.
Élevé – Orange	Traite des techniques de post-exploitation conduisant au vol d'identifiants ou à un contournement de sécurité, ou des techniques d'exploitation qui doivent être enchaînées à d'autres pour être dangereuses.
Moyen - Jaune	Indique un risque limité pour l'infrastructure Active Directory.
Faible - Bleu	Affiche les bonnes pratiques de sécurité. Certains contextes opérationnels peuvent autoriser des déviances à faible impact qui n'affectent pas nécessairement la sécurité AD. Ces déviances n'ont d'impact sur l'infrastructure AD que si un administrateur commet une erreur, en activant un compte inactif par exemple.

Date de résolution et de détection de la déviance

Tenable Identity Exposure utilise parfois une date de résolution ou de détection différente de la date réelle de l'événement. Cela se produit parce que Tenable Identity Exposure stocke la date de l'événement le plus récent qui affecte chaque objet Active Directory (AD) pendant le processus de mise en cache.

Lors de la détection et de la résolution d'une déviance affectant un objet AD, Tenable Identity Exposure attribue la date de l'événement le plus récent pour cet objet comme date de résolution.

Par exemple, lorsque l'appartenance d'un utilisateur à un groupe change, Tenable Identity Exposure enregistre la date de l'événement pour le groupe, et non pour l'utilisateur. Si la déviance qui affecte l'utilisateur est résolue par un changement d'appartenance à un groupe, Tenable Identity Exposure utilisera la date du dernier événement enregistré de l'utilisateur, et non la date du changement d'appartenance au groupe.

Voir aussi

- Détails d'un indicateur d'exposition
- Objets déviants
- Rechercher des objets déviants
- Ignorer un objet déviant ou une raison (Déviance)
- Attributs incriminants

Détails d'un indicateur d'exposition

Les détails d'un indicateur d'exposition permettent d'examiner les informations techniques sur les vulnérabilités détectées, les objets déviants associés et les recommandations de remédiation.

Pour afficher les détails d'un indicateur d'exposition :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'exposition** dans le volet de navigation.

   Le volet **Indicateurs d'exposition** apparaît. Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des déviances.

2. (Facultatif) Pour afficher tous les IoE, cliquez sur le curseur **Afficher tous les indicateurs** pour activer l'option **Oui**.
3. Cliquez sur une tuile d'**Indicateur d'exposition** sur la page.

   Le volet **Détails de l'indicateur** apparaît.

   En haut, le volet **Détails de l'indicateur** résume les informations déjà fournies dans le tableau Trail Flow :

   - Le **nom** de l'IoE.
   - Son niveau de **sévérité** (Critique, Élevé, Moyen ou Faible).
   - Son **statut** de conformité est basé sur le résultat de la dernière analyse réalisée par Tenable Identity Exposure.
   - La **dernière détection** indiquant quand Tenable Identity Exposure a exécuté la dernière analyse.

4. Cliquez sur les onglets suivants pour obtenir plus de détails sur l'IoE :

Onglet	Description
Informations	Indique les ressources internes et externes sur l'IoE, telles que : • Synthèse managériale : présentation générale du problème pour faciliter la prise de décisions appropriées. • Documents : liens vers des ressources externes sur l'IoE. • Outils d'attaque connus : nom des outils de piratage. • Arborescence des domaines impactés.
Détails de la vulnérabilité	Fournit des explications sur la faille détectée dans votre infrastructure AD et indique les risques auxquels elle est exposée si vous ne prenez pas de mesures correctives.
Objets déviants	Les objets déviants révèlent des faiblesses ou des comportements potentiellement dangereux dans votre infrastructure AD. Vous pouvez appliquer des filtres aux objets déviants pour identifier les problèmes critiques. Lorsqu'un statut IoE n'est pas conforme et inclut des objets déviants, vous pouvez prendre des mesures de remédiation pour corriger les failles de sécurité que Tenable Identity Exposure a détectées. Pour plus d'informations, voir Objets déviants.
Recommandations	Conseils pour rétablir la conformité à vos exigences de sécurité et améliorer la sécurité de votre infrastructure AD : • Une synthèse managériale présente la solution suggérée par Tenable Identity Exposure. • La sous-section Détails donne des conseils sur la mise en œuvre du plan d'action et aide les responsables à effectuer les changements nécessaires dans leurs infrastructures AD.

	• La sous-section Documents fournit des liens vers des ressources externes concernant la solution suggérée ou la menace.

Voir aussi

- Indicateurs d'exposition
- Objets déviants
- Rechercher des objets déviants
- Ignorer un objet déviant ou une raison (Déviance)
- Attributs incriminants

Objets déviants

Les indicateurs d'exposition (IoE) de Tenable Identity Exposure peuvent signaler des objets déviants qui révèlent des faiblesses ou des comportements potentiellement dangereux dans une infrastructure Active Directory (AD). L'examen de ces objets déviants peut permettre d'identifier des problèmes critiques et d'y remédier. Vous pouvez effectuer les opérations suivantes :

- Rechercher un objet déviant.
- Ignorer un objet déviant pendant une période.
- Sélectionner des forêts et des domaines pour y rechercher des objets déviants.
- Obtenir des explications sur les attributs incriminants affectant l'IoE.
- Télécharger un rapport montrant tous les objets déviants.

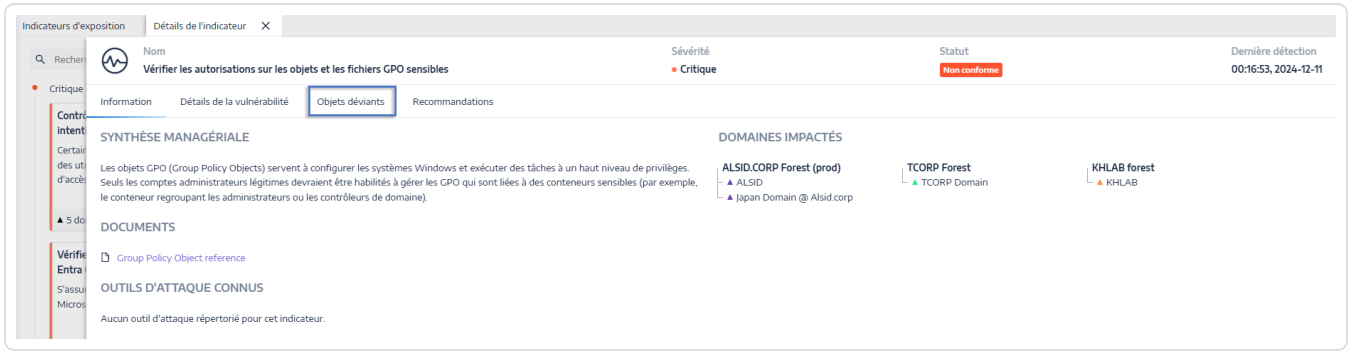
Pour afficher des objets déviants :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'exposition** dans le volet de navigation.

   La page **Indicateurs d'exposition** apparaît. Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des déviances.

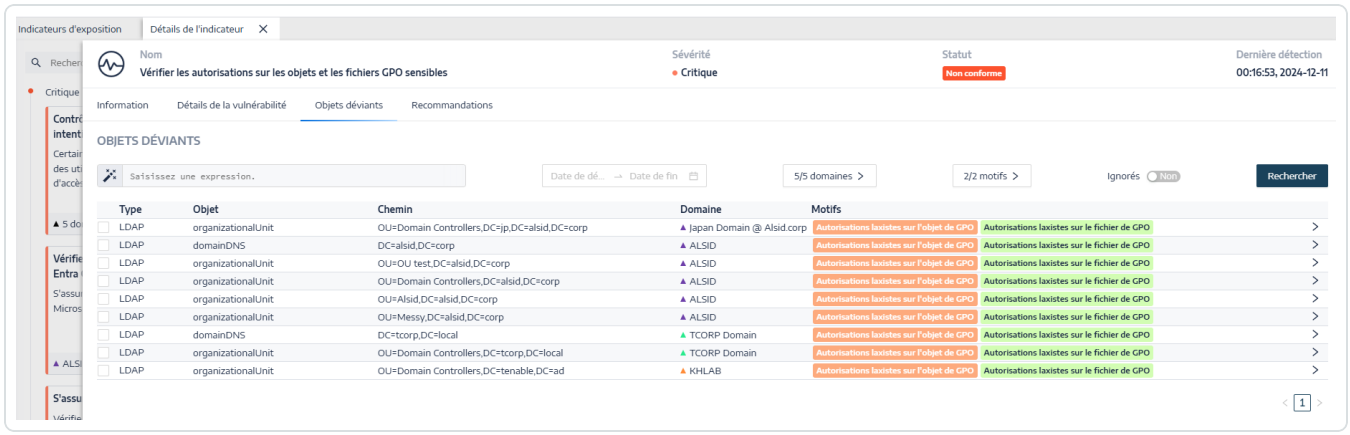
2. Cliquez sur une tuile d'**Indicateur d'exposition** sur la page.

Le volet **Détails de l'indicateur** apparaît.



3. Cliquez sur l'onglet **Objets déviants**.

   La liste des objets déviants associés aux IoE apparaît.



Le tableau des objets déviants contient les informations suivantes :

- **Type** – indique l'origine d'une modification liée à la sécurité dans AD (protocole LDAP ou SMB).
- **Objet** – indique la classe ou l'extension de fichier associée à un objet AD.
- **Chemin** – indique le chemin complet vers un objet AD pour vous permettre d'identifier son emplacement unique dans l'infrastructure AD.
- **Domaine** – indique le domaine d'origine de la modification de votre infrastructure AD.
- **Raisons** – répertorie les attributs incriminants affectant les objets déviants.

Pour exporter le rapport des objets déviants :

1. Au bas de la page **Objets déviants**, cliquez sur **Exporter tout**.

   Le volet **Exporter les objets déviants** apparaît.

2. Dans la zone **Format d'exportation**, cliquez sur la flèche déroulante pour sélectionner le format.

3. Cliquez sur **Exporter tout**.

   Tenable Identity Exposure télécharge le rapport d'objets déviants sur votre machine.

Voir aussi

- Indicateurs d'exposition
- Détails d'un indicateur d'exposition
- Rechercher des objets déviants
- Ignorer un objet déviant ou une raison (Déviance)
- Attributs incriminants

Rechercher des objets déviants

Vous pouvez rechercher les objets déviants manuellement ou à l'aide de l'assistant.

Recherche via l'assistant

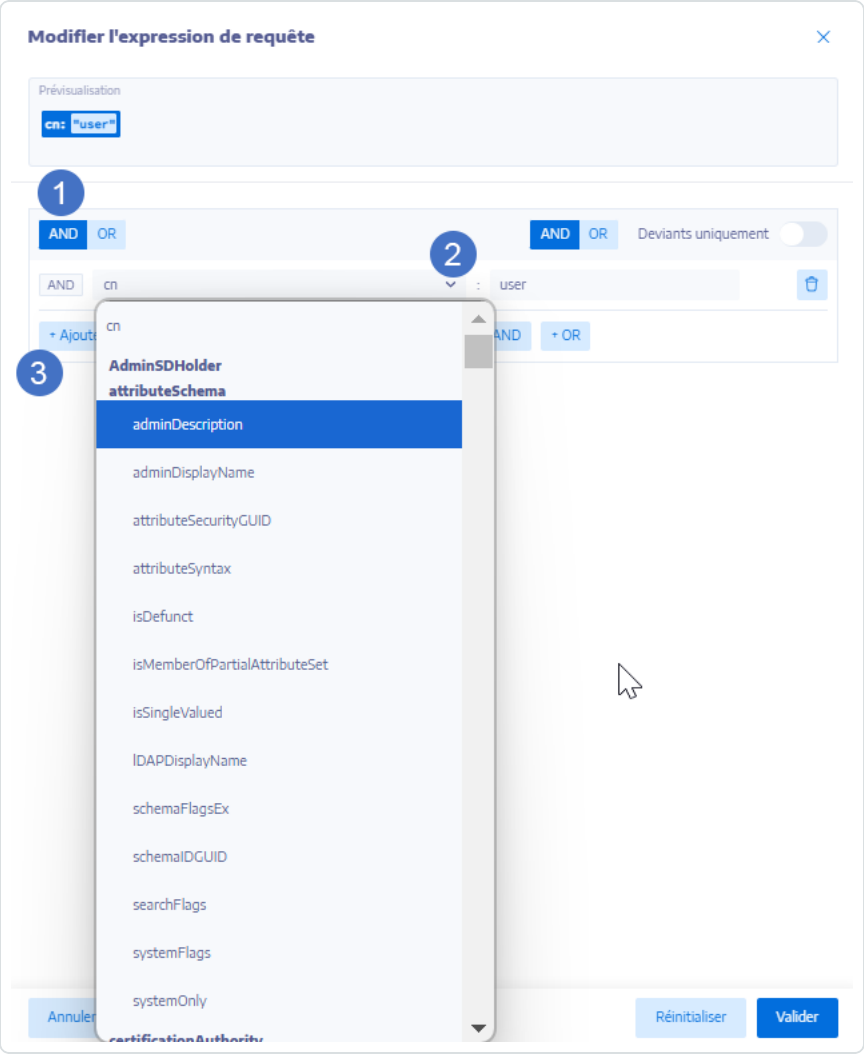
L'assistant de recherche permet de créer des expressions de requête.

- Lorsque vous utilisez des expressions fréquentes dans la zone de recherche, vous pouvez les ajouter à une liste de favoris pour les réutiliser ultérieurement.
- Lorsque vous saisissez une expression dans la zone de recherche, Tenable Identity Exposure enregistre l'expression dans son volet Historique pour que vous puissiez la réutiliser.

Pour rechercher un objet déviant à l'aide de l'assistant :

1. Affichez la liste des Objets déviants.
2. Cliquez sur l'icône .

   Le volet **Modifier l'expression de requête** apparaît.



3. Pour définir l'expression de la requête dans le panneau, cliquez sur le bouton de l'opérateur **AND** ou **OR** (1) pour l'appliquer à la première condition.
4. Sélectionnez un attribut dans le menu déroulant et saisissez sa valeur (2).
5. Effectuez l'une des opérations suivantes :

- Pour ajouter un attribut, cliquez sur **+ Ajouter une nouvelle règle** (3).
- Pour ajouter une autre condition, cliquez sur **Ajouter une nouvelle condition** et sur l'opérateur **+AND** ou **+OR**. Sélectionnez un attribut dans le menu déroulant et saisissez sa valeur.
- Pour limiter la recherche aux objets déviants, cliquez sur le bouton **Déviants uniquement**. Sélectionnez l'opérateur **+AND** ou **+OR** pour ajouter la condition à la requête.
- Pour supprimer une condition ou une règle, cliquez sur l'icône .

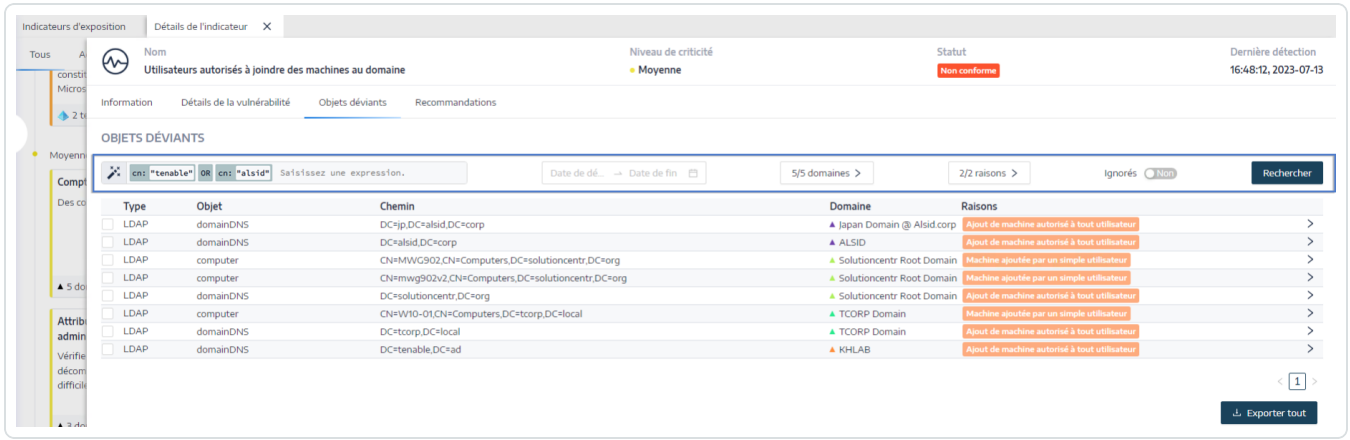
6. Cliquez sur **Valider** pour lancer la recherche ou sur **Réinitialiser** pour modifier les expressions de requête.

Recherche manuelle

Pour filtrer les objets déviants qui correspondent à des chaînes de caractères ou à des modèles spécifiques, vous pouvez saisir une expression dans le champ de recherche, afin d'affiner les résultats à l'aide des opérateurs booléens *****, **AND** et **OR**. Vous pouvez encapsuler des instructions **OR** avec des parenthèses pour modifier la priorité de recherche. La recherche identifie une valeur spécifique dans un attribut Active Directory. Pour effectuer une recherche manuelle dans Trail Flow :

Pour rechercher manuellement un objet déviant :

1. Affichez la liste des Objets déviants.



2. Dans la zone de recherche, saisissez une expression de requête.
3. Vous pouvez filtrer les résultats de la recherche comme suit :

- Cliquez dans la zone **Calendrier** pour sélectionner une date de début et une date de fin.
- Cliquez sur **n/n domaines** pour sélectionner des forêts et des domaines.

4. Cliquez sur **Rechercher**.

   Tenable Identity Exposure met à jour la liste avec les résultats correspondant à vos critères de recherche.

Grammaire et syntaxe

Une expression de requête manuelle utilise la grammaire et la syntaxe suivantes :

- Grammaire : `EXPRESSION [OPERATOR EXPRESSION]*`
- Syntaxe : `__KEY__ __SELECTOR__ __VALUE__`

  Dans ces commandes :

  - `__KEY__` désigne l'attribut d'objet AD à rechercher (par exemple, `CN`, `userAccountControl`, `membres`, etc.)
  - `__SELECTOR__` désigne l'opérateur : `:`, `>`, `<`, `>=`, `<=`.
  - `__VALUE__` désigne la valeur à rechercher.

    Vous pouvez utiliser davantage de clés pour rechercher un contenu spécifique :

  - `isDeviant` recherche les événements qui ont créé une déviance.

Vous pouvez combiner plusieurs expressions de requête Trail Flow à l'aide des opérateurs **AND** et **OR**.

Exemples :

- Rechercher tous les objets contenant la chaîne `alice` dans l'attribut de nom commun : `cn:"alice"`
- Rechercher tous les objets contenant la chaîne `alice` dans l'attribut de nom commun et ayant créé une déviance spécifique : `isDeviant:"true" and cn:"alice"`
- Rechercher la GPO nommée Politique de domaine par défaut : `objectClass:"groupPolicyContainer" and displayname:"Politique de domaine`

par défaut"

- Rechercher tous les comptes désactivés avec un SID contenant S-1-5-21 : `userAccountControl:"DISABLE" and objectSid:"S-1-5-21"`
- Rechercher tous les fichiers `script.ini` dans SYSVOL : `globalpath:"sysvol" et types:"SCRIPTSini"`

  Remarque : ici, `types` fait référence à l'attribut d'objet et non pas à l'en-tête de colonne.

Voir aussi

- Indicateurs d'exposition
- Détails d'un indicateur d'exposition
- Objets déviants
- Ignorer un objet déviant ou une raison (Déviance)
- Attributs incriminants

Ignorer un objet déviant ou une raison (Déviance)

Dans Tenable Identity Exposure, un **objet déviant** désigne tout objet de l'Active Directory (AD) qui présente des comportements anormaux ou risqués, tels que des configurations ou des autorisations inappropriées, qui pourraient potentiellement exposer des vulnérabilités de sécurité. Ces objets sont identifiés par le biais des indicateurs d'exposition (IoE) de Tenable qui identifient les déviations par rapport aux bonnes pratiques et aux normes de sécurité.

Une **raison**, également appelée « **déviance** », est l'attribut ou le facteur spécifique qui rend un objet déviant. Plusieurs raisons peuvent expliquer pourquoi l'IoE a marqué un objet comme déviant. Par exemple, un objet peut être marqué comme déviant en raison d'autorisations de fichier incorrectes, de mauvaises configurations ou d'une délégation risquée, chacun représentant une « raison » distincte.

En résumé :

- **Objet déviant** : objet AD signalé en raison d'un comportement risqué ou anormal.
- **Raison/Déviance** : attribut ou facteur spécifique qui amène l'IoE à signaler l'objet.

Ces raisons sont essentielles pour comprendre les faiblesses de sécurité sous-jacentes associées à chaque objet déviant.

Ignorer un objet déviant

Lorsque vous choisissez d'ignorer un objet déviant, vous ignorez également toutes les raisons ou déviances associées.

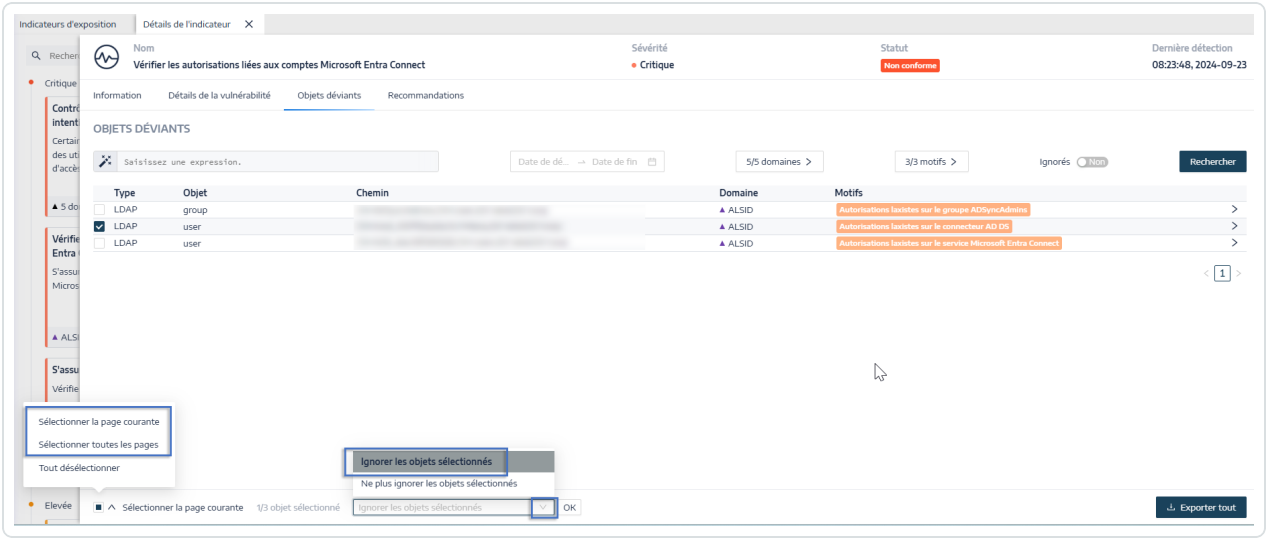
Cela peut être utile pour réduire l'encombrement de l'interface lorsque certains objets signalés ne sont pas préoccupants dans l'immédiat.

Cependant, ignorer ces objets ne résout pas les problèmes sous-jacents ; cela les empêche simplement d'apparaître dans les rapports ou sur les écrans d'investigation pendant la période spécifiée.

Pour ignorer des objets déviants :

1. Dans Tenable Identity Exposure, affichez la liste des Objets déviants.
2. Cochez les cases correspondant aux objets déviants à ignorer.
3. Le cas échéant, vous pouvez aussi filtrer les objets déviants à ignorer :
    - Cliquez sur la zone **Calendrier** pour sélectionner une date de début et une date de fin.
    - Cliquez sur **n/n domaines** pour sélectionner des forêts et des domaines.

> **Astuce** : pour accélérer la sélection, vous pouvez cocher la case **Sélectionner toutes les pages** ou **Sélectionner la page courante** en bas de la page.



4. Dans la liste déroulante en bas de la page, sélectionnez **Ignorer les objets sélectionnés**.
5. Cliquez sur **OK**.

   Le volet **Ignorer les objets sélectionnés** apparaît.
6. Cliquez sur la zone **Ignorer jusqu'à** pour afficher le calendrier et sélectionnez la date jusqu'à laquelle Tenable Identity Exposure doit ignorer l'objet déviant.
7. Cliquez sur **OK**.

   Tenable Identity Exposure affiche un message de confirmation et met à jour la liste des objets déviants restants.

Pour afficher les objets déviants ignorés :

1. Cliquez sur le curseur **Ignoré** pour activer l'option **Oui**.
2. Au bas de la page, cliquez sur **Sélectionner toutes les pages**.
3. Sélectionnez **Ne plus ignorer les objets sélectionnés** dans la liste déroulante.
4. Cliquez sur **OK**.

   Un volet de confirmation apparaît.
5. Cliquez sur **OK** pour valider vos modifications.

   Tenable Identity Exposure affiche les objets déviants ignorés.

Ignorer une raison ou une « déviance »

Lorsque vous choisissez d'ignorer une raison (ou « déviance ») spécifique dans Tenable Identity Exposure, l'IoE cesse de vous alerter sur ce problème particulier, mais ne résout pas le problème lui-même.

La déviance ignorée n'apparaît plus dans le dashboard de surveillance active, désactivant ainsi l'alerte associée à cette raison spécifique.

Cependant, d'autres déviances liées au même objet continuent de déclencher des alertes à moins que vous n'ayez également ignoré chacune d'elles.

Pour ignorer une raison (« déviance ») :

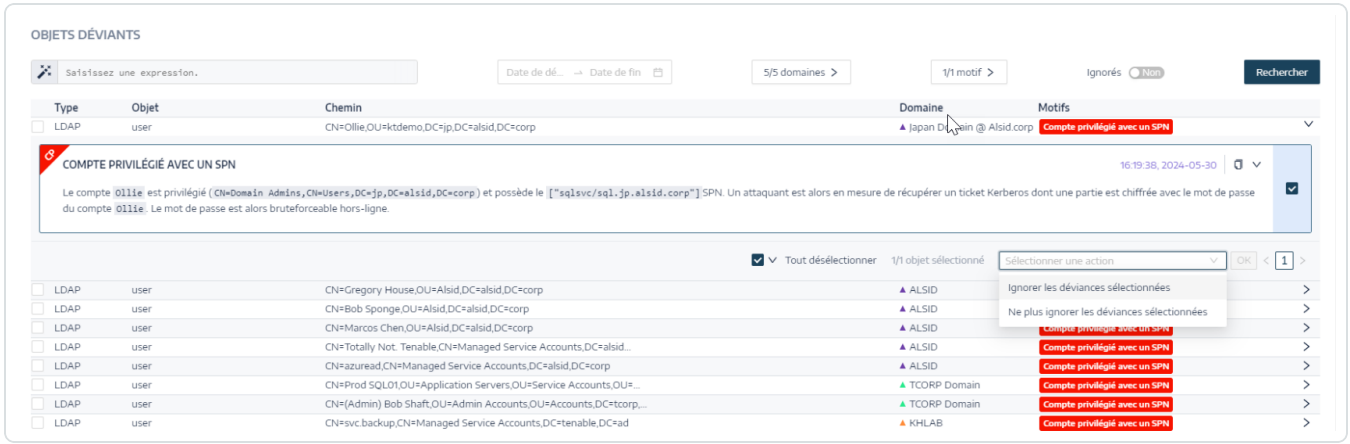
1. Dans Tenable Identity Exposure, affichez la liste des Objets déviants.

   Une liste d'objets déviants apparaît.

2. Identifiez un objet déviant et cliquez sur la flèche (>) à la fin de la ligne.

   La vue s'agrandit pour afficher les détails de la raison.

3. Cochez la case à la fin de la ligne. S'il y a plusieurs raisons, sélectionnez celles qu'il faut ignorer ou cliquez sur **Tout sélectionner** pour ignorer toutes les raisons associées.



4. Cliquez sur **OK**.

   Le volet **Ignorer les déviances sélectionnées** apparaît.

5. Cliquez sur la zone **Ignorer jusqu'à** pour afficher le calendrier et sélectionnez la date jusqu'à laquelle Tenable Identity Exposure doit ignorer l'objet déviant.
6. Cliquez sur **OK**.

   Tenable Identity Exposure affiche un message de confirmation et met à jour la liste des déviances restantes.

Pour afficher les déviances ignorées :

1. Cliquez sur le curseur **Ignoré** pour activer l'option **Oui**.

   La liste des objets déviants est mise à jour avec une vue développée pour toutes les raisons.

   Les raisons ignorées affichent l'icône .
2. Sélectionnez la raison ignorée et cliquez sur Ne plus ignorer les déviances sélectionnées dans la liste déroulante.
3. Cliquez sur **OK**.

   Le volet « Ne plus ignorer les déviances sélectionnées » apparaît.
4. Cliquez sur **OK**.

   Tenable Identity Exposure affiche un message de confirmation et met à jour la liste des déviances restantes.

Voir aussi

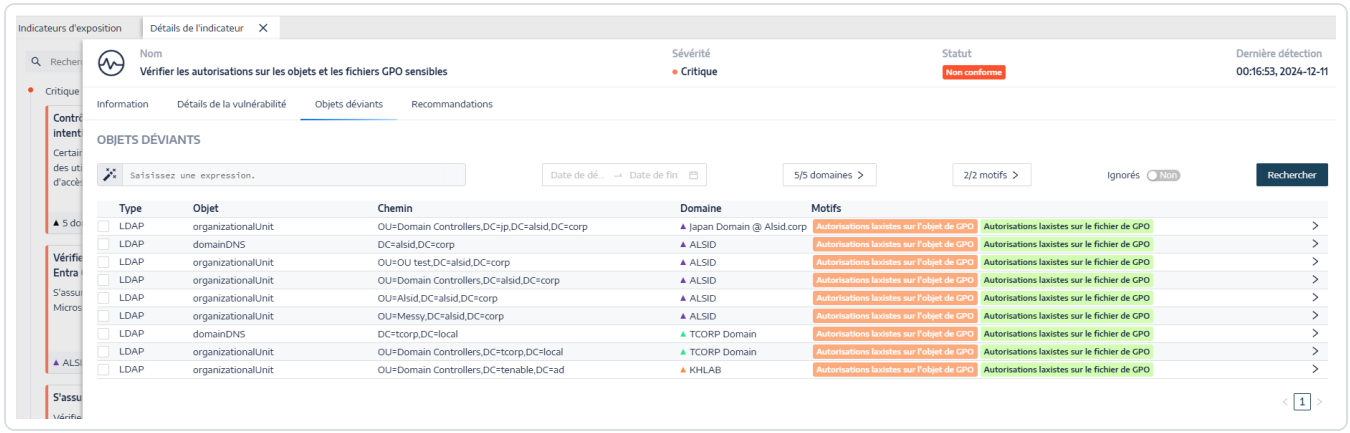
- Indicateurs d'exposition
- Détails d'un indicateur d'exposition
- Objets déviants
- Rechercher des objets déviants
- Attributs incriminants

Attributs incriminants

Tenable Identity Exposure affiche les attributs incriminants qui déclenchent des objets déviants dans un indicateur d'exposition (IoE) et en donne les raisons pour vous aider à comprendre la déviance et à y remédier.

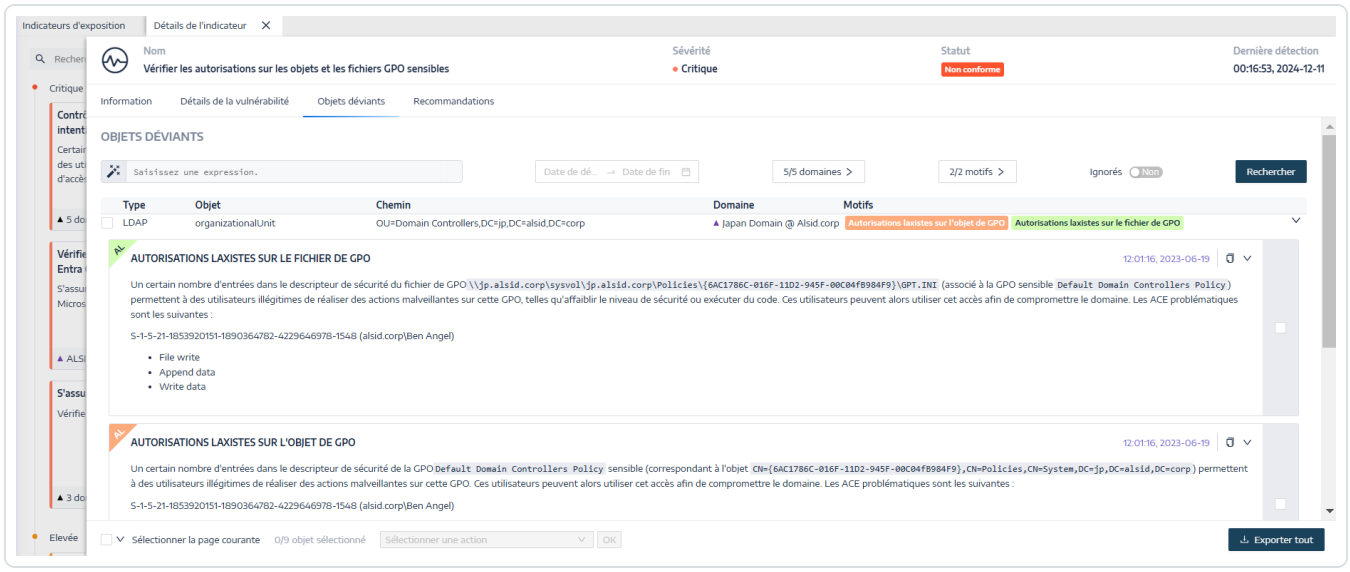
Pour afficher les attributs incriminants :

1. Affichez la liste des Objets déviants.



2. Cliquez sur une entrée dans la liste des objets déviants.

   Tenable Identity Exposure affiche une liste d'attributs incriminants pour cet objet déviant :



La liste contient les informations suivantes :

- Des **tags colorés** pour distinguer les différentes raisons lorsqu'il en existe plusieurs.
- Valeurs :

- `?` – Valeur d'attribut manquante (vide) indiquant un comportement anormal.
- `Aucune description n'est disponible pour cette déviance` : la détection date de la version 2.6 et Tenable Identity Exposure ne gère plus cet attribut.

Pour copier un attribut incriminant :

- Sélectionnez l'attribut et cliquez sur l'icône .

Voir aussi

- Indicateurs d'exposition
- Détails d'un indicateur d'exposition
- Objets déviants
- Rechercher des objets déviants
- Ignorer un objet déviant ou une raison (Déviance)

Indicateurs d'exposition basé sur un RSoP

Tenable Identity Exposure utilise un ensemble d'indicateurs d'exposition (IoE) basés sur un RSoP (jeu de stratégies résultant) pour évaluer et assurer la sécurité et la conformité de divers aspects. Cette section fournit des informations sur le comportement actuel de certains IoE basés sur un RSoP et sur la manière dont Tenable Identity Exposure traite les problèmes de performances associés à leurs calculs.

Les IoE suivants, qui dépendent d'un RSoP, jouent un rôle dans l'infrastructure de sécurité de Tenable Identity Exposure :

- Restrictions d'authentification des utilisateurs avec privilèges
- Privilèges sensibles dangereux
- Stratégies de mots de passe faibles appliquées aux utilisateurs
- Durcissement insuffisant contre les ransomwares
- Configuration non sécurisée du protocole Netlogon

Ces IoE dépendent du cache des résultats de calcul d'un RSoP qui est initialisé en cas de besoin, ce qui permet de calculer les valeurs ajoutées à la demande au lieu de s'appuyer sur des valeurs pré-existantes. Auparavant, les modifications apportées aux `AdObjects` provoquaient l'invalidation du cache, entraînant fréquemment un recalcul pendant les exécutions du RSoP de l'IoE.

Tenable Identity Exposure traite l'impact exercé sur les performances par les calculs d'un RSoP de la manière suivante :

1. **Analyse d'IoE en direct avec des données potentiellement obsolètes** – Le calcul (événement d'entrée/sortie) d'IoE qui dépendent de RSoP a lieu en temps réel à mesure qu'ils se produisent, même si les données utilisées pour le traitement ne sont pas les plus récentes. Les événements mis en mémoire tampon qui sont susceptibles d'invalider le cache du RSoP restent stockés jusqu'à ce qu'ils remplissent une condition spécifique, ce qui déclenche alors le calcul prévu.
2. **Invalidation de RSoP planifiée** – Après avoir rempli la condition d'un nouveau calcul, le système invalide le cache du RSoP, en tenant compte des événements mis en mémoire tampon pendant le processus d'invalidation.
3. **Réexécution des IoE avec un cache à jour** – Après l'invalidation du cache, les IoE sont réexécutés avec la dernière version de l'`AdObject` du cache, en intégrant les événements mis en mémoire tampon. Tenable Identity Exposure calcule chaque IoE individuellement pour chaque événement mis en mémoire tampon.

Pour ces raisons, la durée de calcul optimisée pour les IoE dépendant d'un RSoP entraîne un calcul plus lent des déviances liées au RSoP.

Améliorations

Tenable Identity Exposure a mis en œuvre des modifications des indicateurs d'exposition traitant des tâches RSoP afin d'améliorer leurs performances globales et leur réactivité.

- **Vérifications de sécurité plus intelligentes** – L'exécution de certaines vérifications de sécurité (appelées vérifications RSoP) a été repensée pour réduire les ralentissements du système.
- **Planification adaptative** – Le système choisira automatiquement les meilleurs moments pour exécuter ces vérifications en fonction de la charge de travail actuelle.

- **Protection contre les surcharges** – Nous avons mis en place de nouvelles mesures pour empêcher la surcharge du système pendant les périodes de pointe.
- **Analyse de sécurité des fichiers de GPO** – Les indicateurs d'exposition qui analysent la sécurité des fichiers de GPO seront désormais traités toutes les 30 minutes, et non en temps réel comme les autres IoE.

Avantages

- **Temps de réponse plus rapides** – Grâce à l'optimisation de notre processus de vérification de sécurité, vous devriez observer des réponses système plus rapides, en particulier pendant les heures d'utilisation de pointe.
- **Amélioration de la fiabilité** – La nouvelle planification adaptative permet de garantir que les vérifications de sécurité importantes n'interfèrent pas avec votre travail.
- **Expérience plus fluide** – Grâce à une meilleure protection contre les surcharges, le système devrait maintenir des performances constantes même en cas d'utilisation intensive.
- **Amélioration de la stabilité de la plateforme** – Ces changements profiteront particulièrement aux clients ayant une activité AD élevée, en améliorant la constance des performances.

Aspects techniques

- Les vérifications RSoP et les analyses de sécurité des fichiers de GPO sont exécutées périodiquement et non en temps réel.
- Toutes les 30 minutes, la plateforme évalue sa charge de travail. Si elle détermine qu'elle est en mesure de gérer une analyse, elle poursuit ; sinon, elle attend que la charge diminue.
- Mise en œuvre d'un algorithme pour détecter la surcharge du système, en tenant compte de facteurs tels que la longueur de la file d'attente des messages et les tendances de traitement.
- Pendant les périodes de surcharge, les vérifications non critiques sont reportées pour maintenir la réactivité du système.

Remédier à des déviances liées à des indicateurs d'exposition

Tenable Identity Exposure déclenche des alertes lorsqu'un indicateur d'exposition (IoE) rencontre des objets déviants qui nécessitent une remédiation.

Voici des exemples montrant comment effectuer une procédure de remédiation pour trois IoE spécifiques.

- Attribut adminCount appliqué à des utilisateurs non administrateurs
- Délégation Kerberos dangereuse
- S'assurer de la cohérence de SDProp

Pour des informations complètes sur les IoE, voir la documentation fournie dans l'interface utilisateur Tenable Identity Exposure.

Attribut adminCount appliqué à des utilisateurs non administrateurs

Lorsque l'attribut `adminCount` est appliqué à un compte utilisateur, cela signifie que ce compte a appartenu à un groupe d'administration. L'attribut n'est jamais réinitialisé lorsque le compte quitte le groupe. De ce fait, les anciens comptes administrateurs conservent indéfiniment cette propriété. Ce comportement avait pour but de protéger les administrateurs, mais il peut créer des problèmes d'autorisations difficiles à gérer.

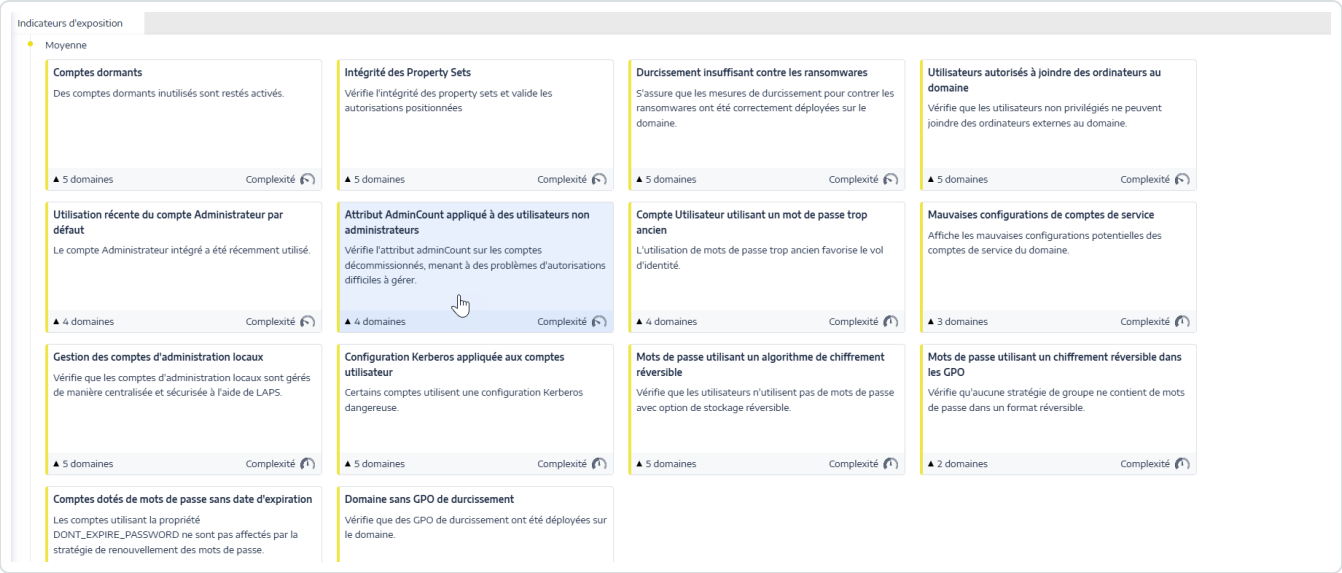
Cet IoE de niveau moyen ne signale que les comptes utilisateur et les groupes actifs avec cet attribut et exclut les groupes privilégiés avec des membres légitimes dont l'attribut `adminCount` est défini sur `1`.

Pour remédier à un objet déviant de l'IoE **Attribut adminCount appliqué à des utilisateurs non administrateurs** :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'exposition** dans le volet de navigation pour l'ouvrir.

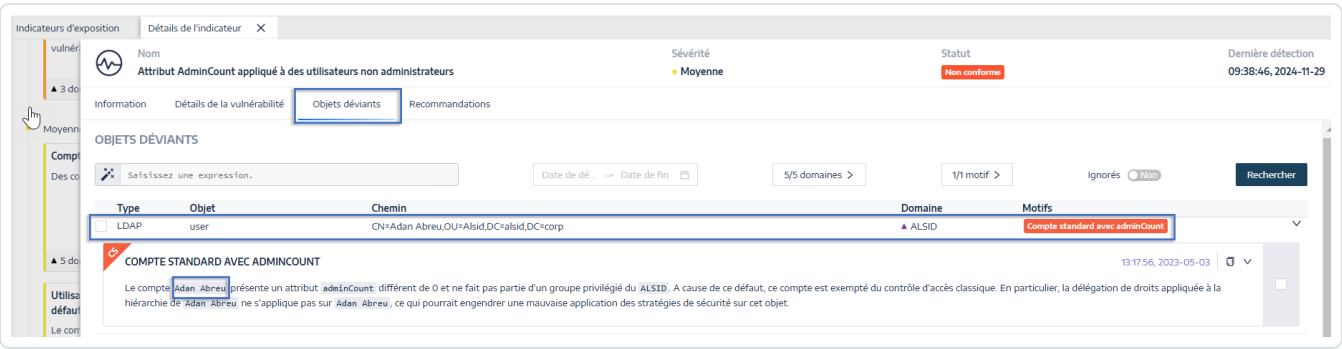
   Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des objets déviants.

2. Cliquez sur la tuile de l'IoE **Attribut adminCount appliqué à des utilisateurs non administrateurs**.



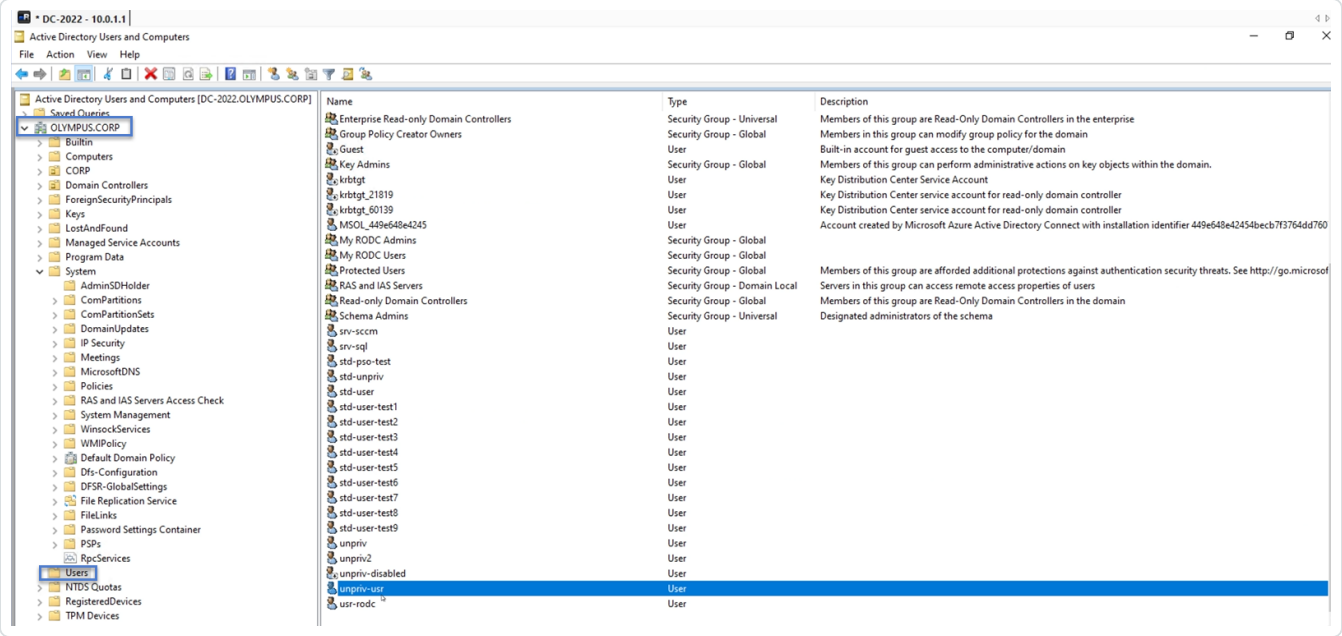
Le volet **Détails de l'indicateur** apparaît.

3. Survolez l'objet déviant et cliquez dessus pour afficher ses détails, puis notez le nom de domaine et le compte. (Dans cet exemple : le domaine = `OLYMPUS.CORP` et le compte standard est `unpriv-usr`)



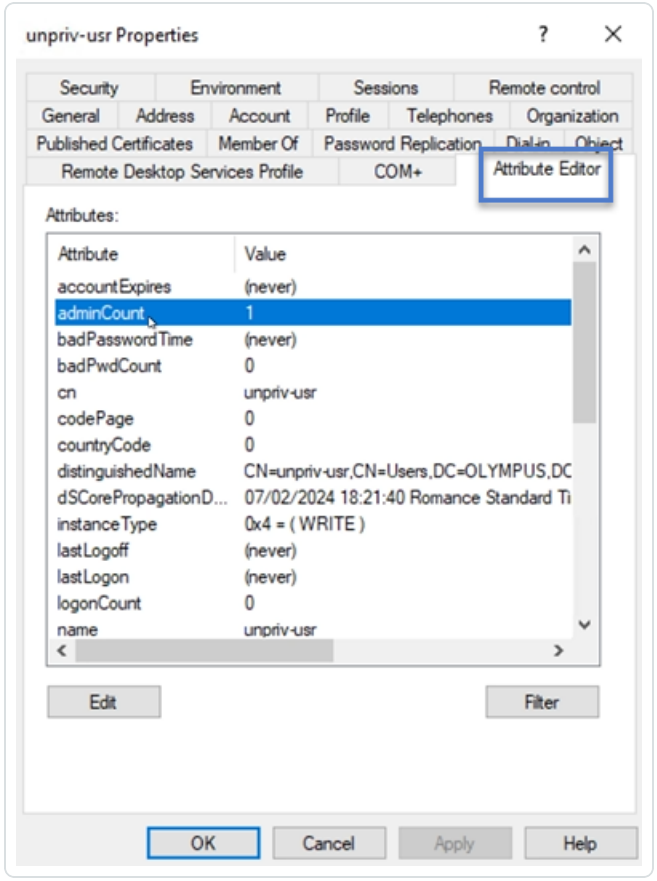
4. Dans le gestionnaire de bureau à distance (ou un outil similaire), localisez le nom de domaine et accédez aux **utilisateurs** ainsi qu'au compte signalé par Tenable Identity Exposure.

> **Autorisation requise** : vous devez disposer d'un compte administrateur sur le domaine pour effectuer la procédure.

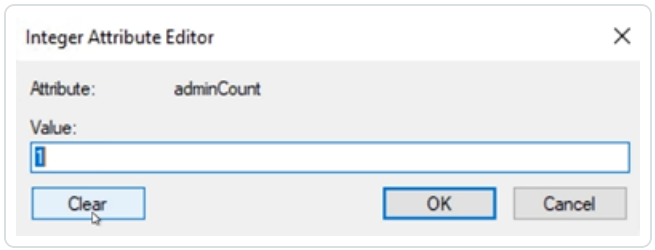


5. Cliquez sur le nom du compte pour ouvrir la boîte de dialogue **Propriétés** et sélectionnez l'onglet **Éditeur d'attributs**.

6. Dans la liste des attributs, cliquez sur `adminCount` pour ouvrir la boîte de dialogue **Integer Attribute Editor** (Éditeur d'attributs de type Entier).



7. Dans la boîte de dialogue, cliquez sur **Effacer**, puis sur **OK**.



8. Dans Tenable Identity Exposure, revenez au volet Détails de l'indicateur et actualisez la page.

   L'objet déviant n'apparaît plus dans la liste.

Délégation Kerberos dangereuse

Le protocole Kerberos sur lequel repose la sécurité de l'Active Directory, autorise certains serveurs à réutiliser les informations d'authentification des utilisateurs. Si l'un de ces serveurs est compromis, un attaquant peut s'authentifier sur d'autres ressources après avoir dérobé les informations d'authentification.

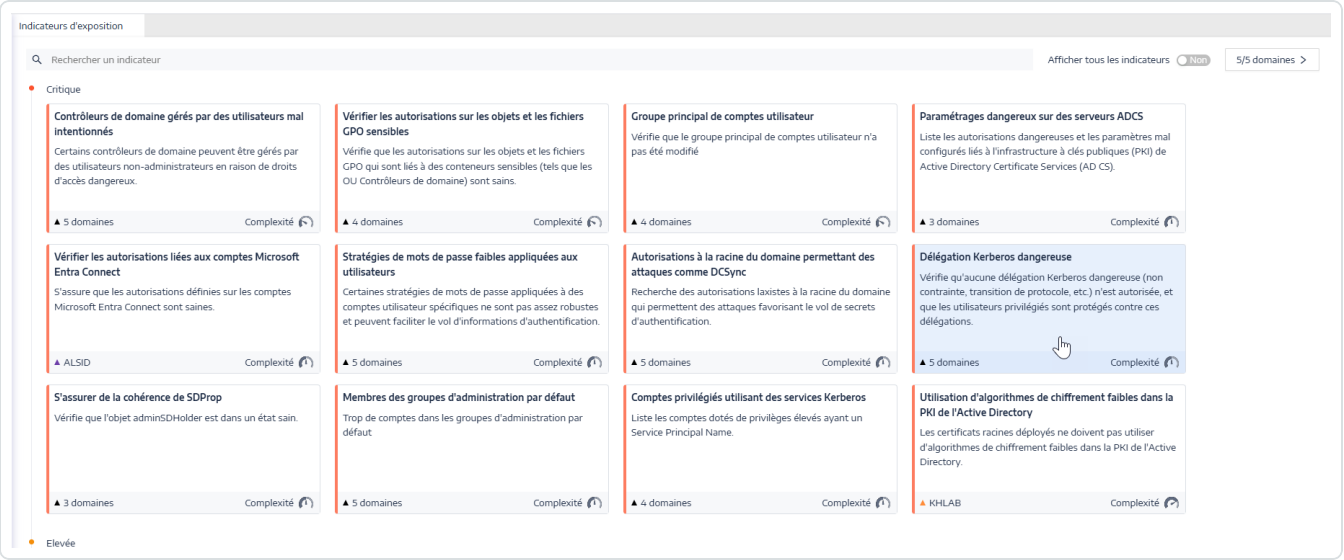
Cet IoE de niveau critique signale tous les comptes avec des attributs de délégation et exclut les comptes désactivés. Les utilisateurs privilégiés ne devraient pas avoir d'attributs de délégation. Pour protéger ces comptes utilisateur, ajoutez-les au groupe « Protected Users » ou marquez-les comme « Le compte est sensible et ne peut pas être délégué ».

Pour ajouter le compte au groupe « Protected Users » :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'exposition** dans le volet de navigation pour l'ouvrir.

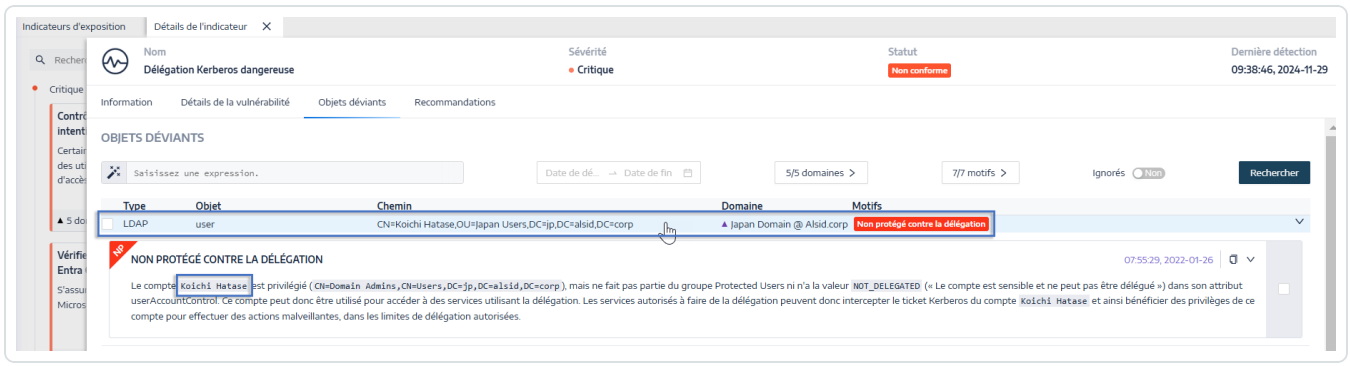
   Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des objets déviants.

2. Cliquez sur la tuile de l'IoE **Délégation Kerberos dangereuse**.



   Le volet **Détails de l'indicateur** apparaît.

3. Survolez l'objet déviant et cliquez dessus pour afficher ses détails, puis notez le nom de domaine et le compte. (Dans cet exemple : le domaine = OLYMPUS.CORP et le compte = `adm-t0`)

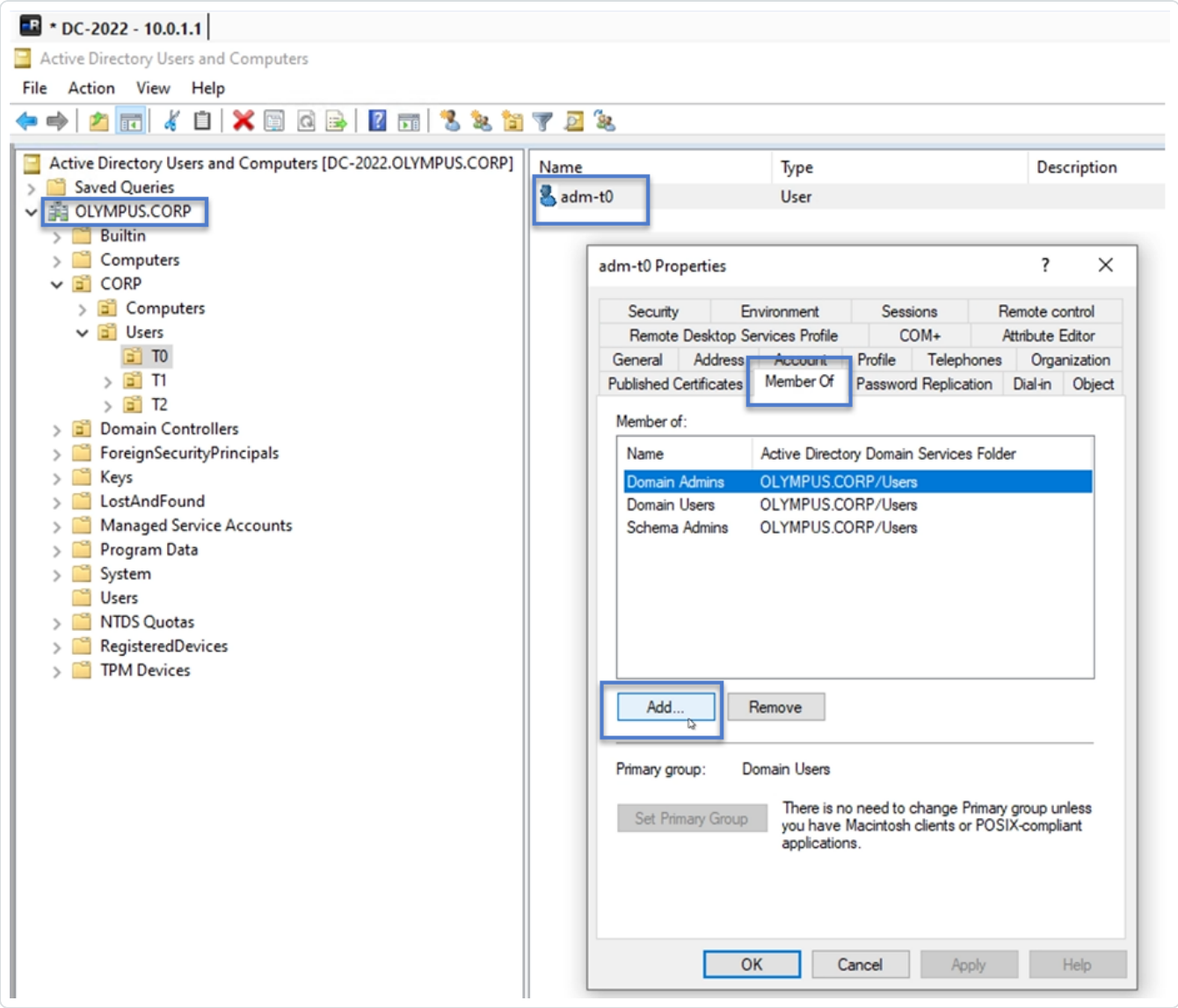


4. Dans le gestionnaire de bureau à distance (ou un outil similaire), localisez le nom de domaine et accédez au domaine et au compte signalés par Tenable Identity Exposure.

   Autorisation requise : vous devez disposer d'un compte administrateur sur le domaine pour effectuer la procédure.

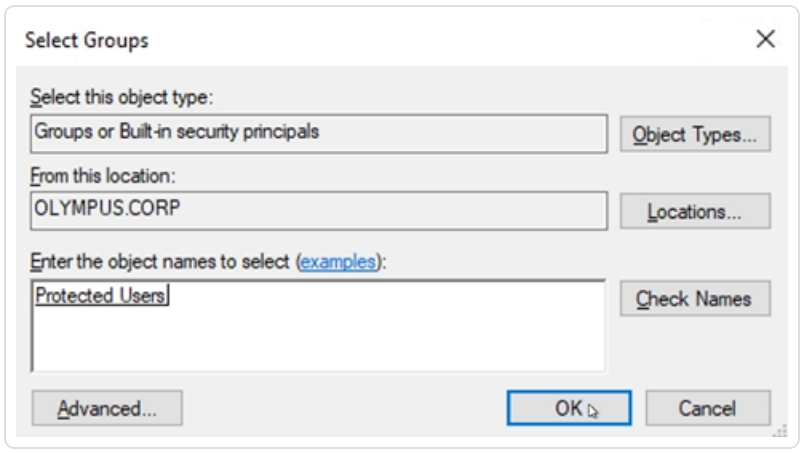
5. Cliquez sur le nom du compte pour ouvrir la boîte de dialogue **Propriétés** et sélectionnez l'onglet **Membre de**.

6. Dans la liste des membres, cliquez sur **Ajouter**.



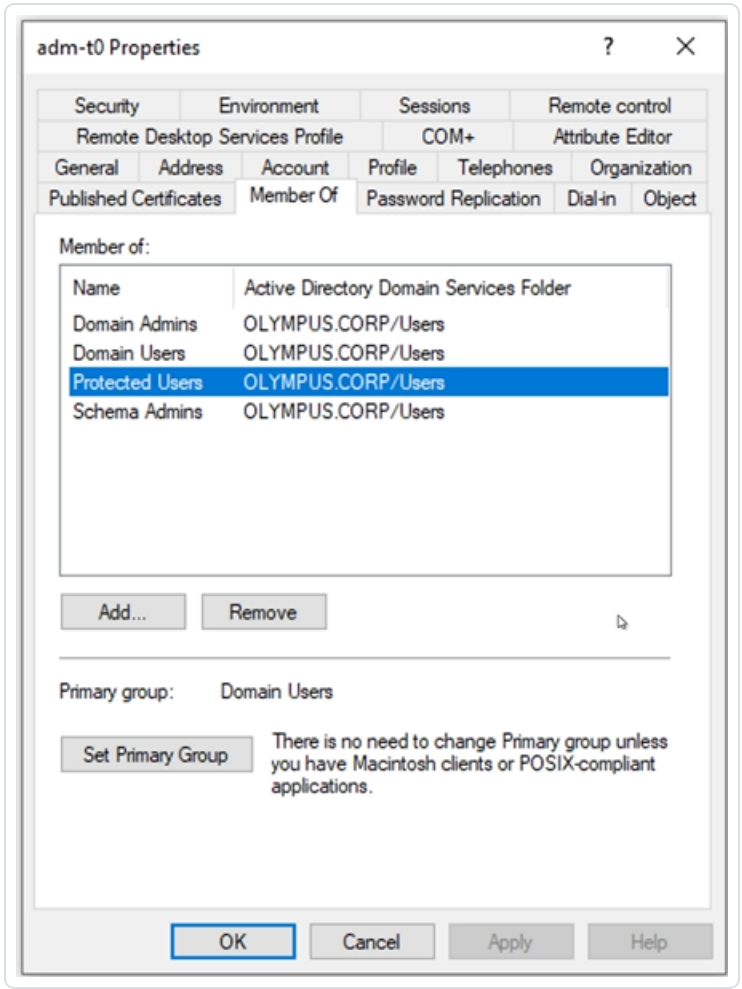
La boîte de dialogue **Sélectionner des groupes** apparaît.

7. Saisissez le nom d'objet « Protected Users » et cliquez sur **Vérifier les noms**.



8. Cliquez sur **OK** pour refermer la boîte de dialogue.
9. Dans la boîte de dialogue **Propriétés**, cliquez sur **Appliquer**.

   Le nouveau groupe apparaît dans la liste des membres.



10. Cliquez sur **OK** pour refermer la boîte de dialogue.
11. Dans Tenable Identity Exposure, revenez au volet Détails de l'indicateur et actualisez la page.

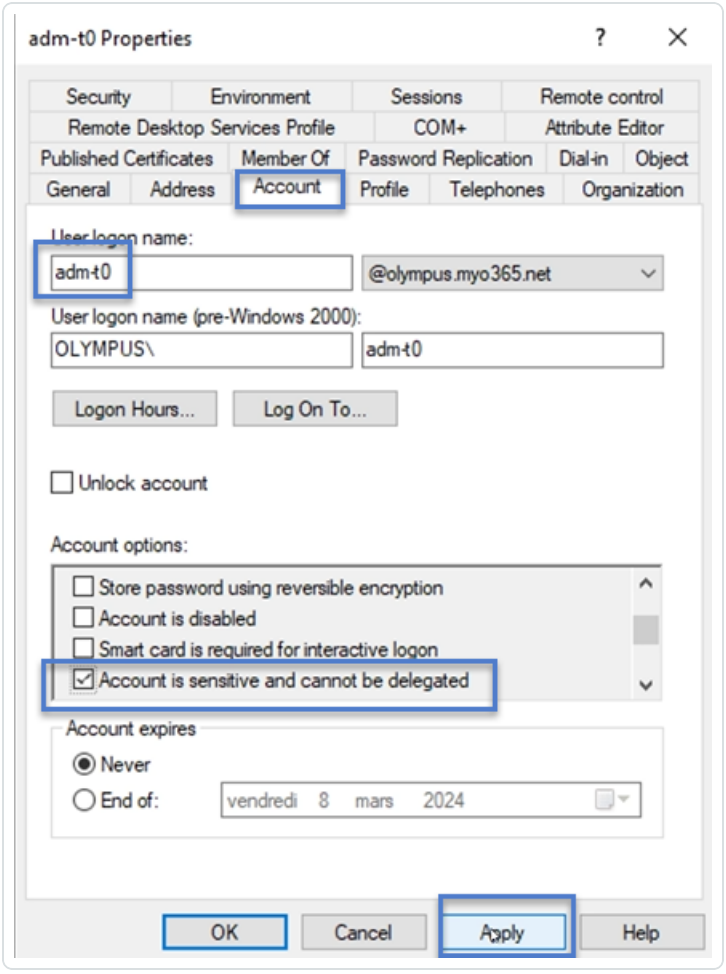
    L'objet déviant n'apparaît plus dans la liste.

Pour définir le compte comme « ne peut pas être délégué » :

1. Dans le gestionnaire de bureau à distance, localisez le nom de domaine et accédez au domaine et au compte signalés par Tenable Identity Exposure.

   > **Autorisation requise** : vous devez disposer d'un compte administrateur sur le domaine pour effectuer la procédure.

2. Cliquez sur le nom du compte pour ouvrir la boîte de dialogue **Propriétés** et sélectionnez l'onglet **Compte**.
3. Dans la liste des options de compte, sélectionnez « Le compte est sensible et ne peut pas être délégué » et cliquez sur **Appliquer**.



4. Cliquez sur **OK** pour refermer la boîte de dialogue.
5. Dans Tenable Identity Exposure, revenez au volet Détails de l'indicateur et actualisez la page.

   L'objet déviant n'apparaît plus dans la liste.

S'assurer de la cohérence de SDProp

Les attaquants qui compromettent un domaine Active Directory modifient généralement l'ACL de l'objet `adminSDHolder`. Ensuite, toute autorisation qu'ils ajoutent à l'ACL est copiée vers les utilisateurs privilégiés, ce qui facilite la configuration de portes dérobées.

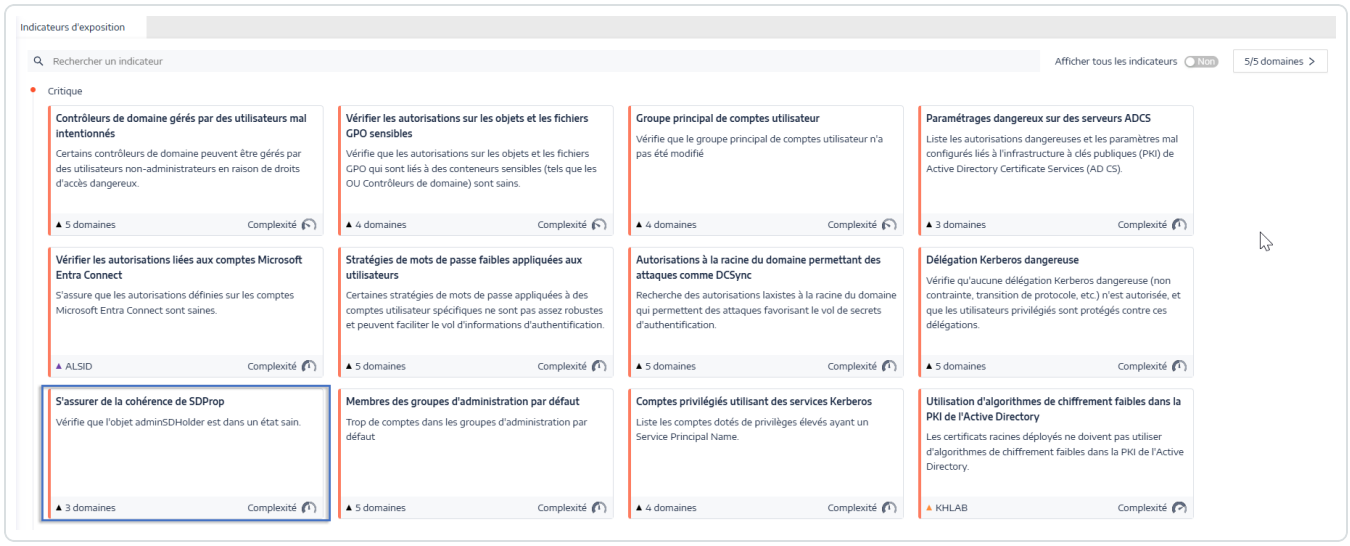
Cet IoE de niveau critique vérifie que les autorisations définies sur l'objet `adminSDHolder` autorisent uniquement un accès privilégié aux comptes administratifs.

Pour remédier à un objet déviant de l'IoE **S'assurer de la cohérence de SDProp** :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'exposition** dans le volet de navigation pour l'ouvrir.

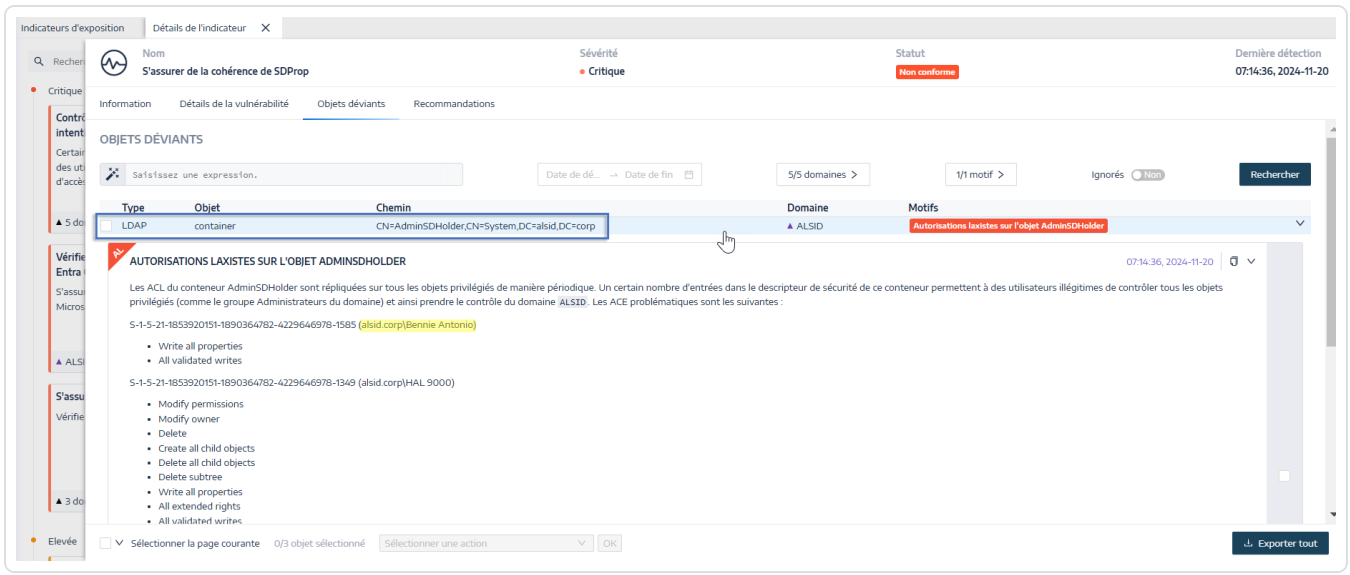
   Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des objets déviants.

2. Cliquez sur la tuile de l'IoE **S'assurer de la cohérence de SDProp**.



   Le volet **Détails de l'indicateur** apparaît.

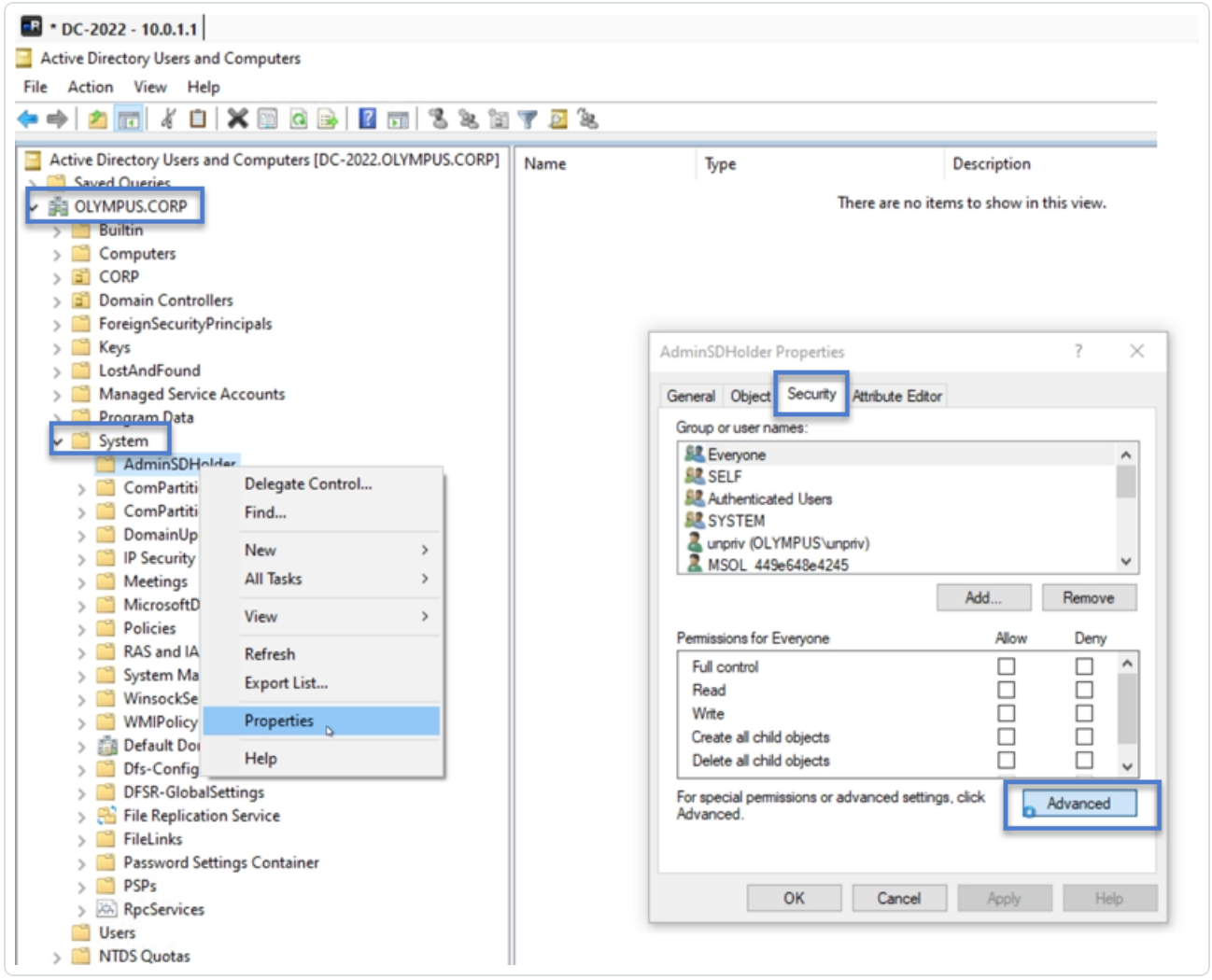
3. Survolez l'objet déviant et cliquez dessus pour afficher ses détails. Notez le nom de domaine et l'autorisation associée signalés par Tenable Identity Exposure (dans cet exemple : `OLYMPUS.CORP .\unpriv`).



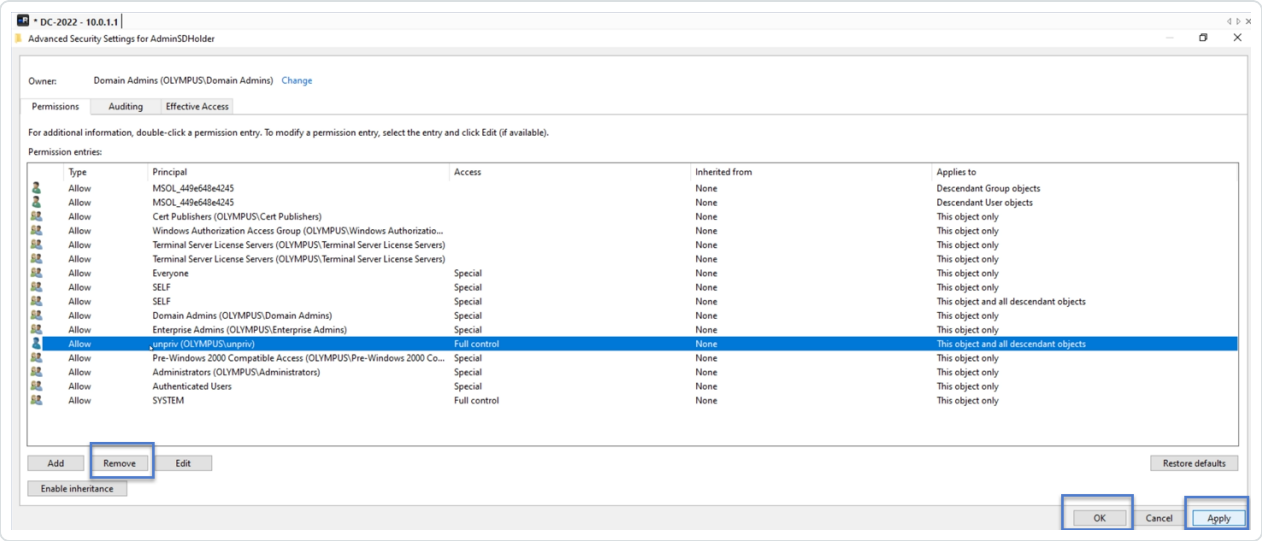
4. Dans le gestionnaire de bureau à distance (ou un outil similaire), localisez le nom de domaine et accédez à **Système** > **AdminSDHolder**.

   Autorisation requise : vous devez disposer d'un compte administrateur sur le domaine pour effectuer la procédure.

5. Effectuez un clic droit sur **AdminSDHolder** et sélectionnez **Propriétés** dans le menu contextuel.



6. Dans la boîte de dialogue **Propriétés**, sélectionnez l'onglet **Sécurité** et cliquez sur **Avancé**.
7. Dans la fenêtre **Paramètres de sécurité avancés** et dans l'onglet **Autorisations**, sélectionnez l'autorisation qui a déclenché l'alerte dans la liste des entrées d'autorisations.
8. Cliquez sur **Supprimer**.
9. Cliquez sur **Appliquer** et sur **OK** pour refermer la fenêtre des paramètres.
10. Cliquez sur **OK** pour refermer la fenêtre **Propriétés**.



11. Dans Tenable Identity Exposure, revenez au volet Détails de l'indicateur et actualisez la page.

    L'objet déviant n'apparaît plus dans la liste.

Indicateurs d'attaque

> **Licence requise** : Indicators of Attack

Les **indicateurs d'attaque** (IoA) de Tenable Identity Exposure permettent de détecter les attaques contre votre infrastructure Active Directory (AD).

Une vue consolidée des indicateurs d'attaque affiche, dans un même volet, une chronologie, les 3 principaux incidents qui ont impacté votre infrastructure AD en temps réel et la distribution des attaques. Vous pouvez effectuer les opérations suivantes :

- Visualiser chaque menace à partir d'une chronologie d'attaque précise.
- Analyser en profondeur les détails d'une attaque AD.
- Explorer les descriptions MITRE ATT&CK directement à partir des incidents détectés.

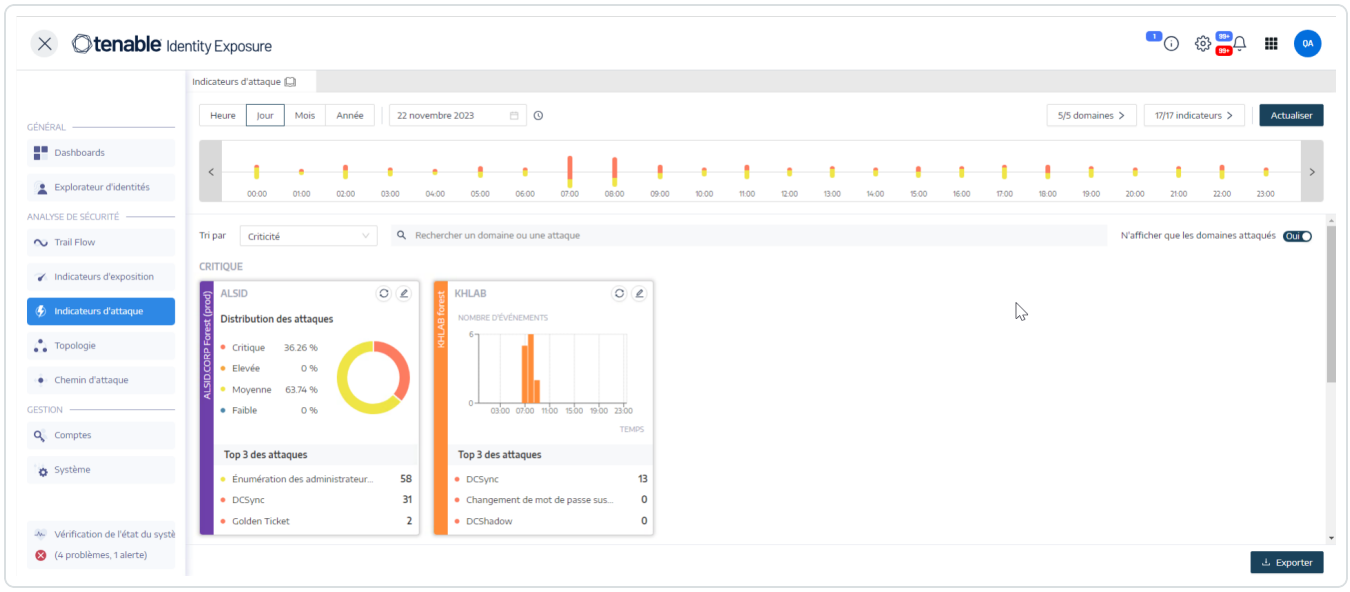
Pour plus d'informations sur des IoA spécifiques, voir Indicators of Attack Reference Guide (Guide de référence des IoA), qui nécessite une connexion au site de téléchargements de Tenable.

> **Remarque :** si vous observez un nombre élevé d'attaques détectées, vérifiez que votre administrateur a correctement calibré les indicateurs d'attaque en appliquant les valeurs recommandées pour les différentes options d'IoA. Pour plus d'informations, voir Pour calibrer les IoA.

Pour afficher les indicateurs d'attaque :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'attaque** dans le volet de navigation.

   Le volet **Indicateurs d'attaque** apparaît.



2. Par défaut, Tenable Identity Exposure affiche toutes vos forêts et tous vos domaines AD. Pour ajuster cette vue, vous pouvez procéder de différentes manières :

   - Sélectionner la période à afficher : cliquez sur **Heure**, **Jour** (par défaut), **Mois** ou **Année**.
   - Parcourir la chronologie : cliquez sur la flèche gauche ou droite pour avancer ou reculer dans la chronologie.
   - Sélectionner une heure spécifique : cliquez sur le sélecteur de date pour choisir une heure, un jour, un mois ou une année.
   - Revenir à la date et à l'heure actuelles : cliquez sur l'icône à côté du sélecteur de date.
   - Sélectionner les domaines : cliquez sur **n/n domaines**.

     a. Dans le volet **Forêt et domaines**, sélectionnez les domaines.

     b. Cliquez sur **Filtrer sur la sélection**.

Tenable Identity Exposure met à jour la vue.

- Sélectionner les IoA : cliquez sur **n/n indicateurs**.

  a. Dans le volet Indicateurs d'attaque, sélectionnez les IoA.

  b. Cliquez sur **Filtrer sur la sélection**.

  Tenable Identity Exposure met à jour la vue.

- Trier les tuiles IoA : dans la zone **Tri par**, cliquez sur la flèche pour afficher une liste déroulante d'options : **Domaine**, **Criticité** ou **Forêt**.
- Rechercher un domaine ou une attaque : dans la zone de **recherche**, saisissez le nom du domaine ou l'attaque.
- Afficher uniquement les domaines attaqués : cliquez sur le curseur **N'afficher que les domaines attaqués** pour activer l'option **Oui**.
- Exporter un rapport d'attaque : cliquez sur **Exporter**.

  Le volet **Exporter les cartes** apparaît.

  a. Dans la zone **Format d'exportation**, cliquez sur la flèche de liste déroulante pour sélectionner un format : **PDF**, **CSV** ou **PPTX**.

  b. Cliquez sur **Exporter**.

  Tenable Identity Exposure télécharge le rapport sur la machine locale.

Niveau de sévérité

Tenable Identity Exposure détecte et attribue des niveaux de sévérité aux attaques :

Niveau	Description
Critique - Rouge	Détection d'une attaque post-exploitation prouvée dont la domination de domaine est une condition préalable.
Élevé - Orange	Détection d'une attaque majeure qui permet à un attaquant d'atteindre la domination de domaine.
Moyen - Jaune	L'IoA est liée à une attaque qui pourrait conduire à une élévation dangereuse des privilèges ou permettre l'accès à des ressources sensibles.

Faible - Bleu	Alertes sur les comportements suspects liés aux actions de reconnaissance ou aux incidents à faible impact.

Voir aussi

- Détails d'un indicateur d'attaque
- Incidents liés aux indicateurs d'attaque

Détails d'un indicateur d'attaque

Le volet Indicateur d'attaque de Tenable Identity Exposure affiche des informations sur les attaques qui se sont produites dans votre infrastructure Active Directory.

Pour afficher les indicateurs d'attaque :

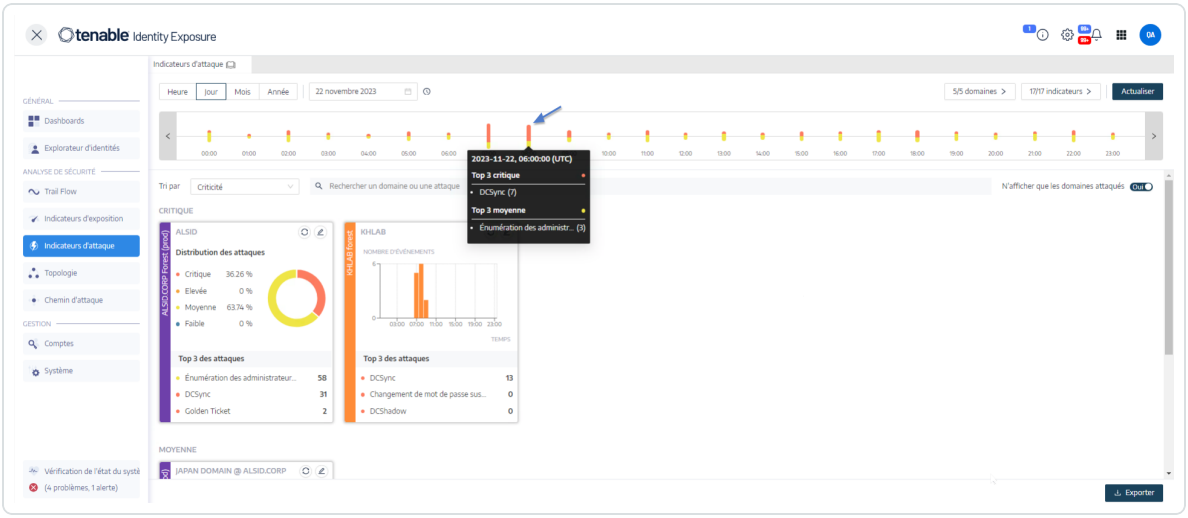
- Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'attaque** dans le volet de navigation.

  Le volet **Indicateurs d'attaque** apparaît.

Pour afficher les informations d'attaque dans la chronologie :

- Cliquez sur un événement dans la chronologie pour afficher :
  - La date et l'heure de détection de l'incident.
  - Le niveau de sévérité des 3 principales attaques.

- Le nombre total d'attaques détectées à la date et à l'heure indiquées.



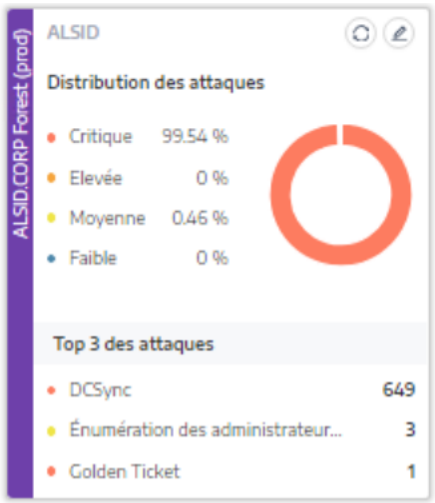
Pour modifier le type de graphique :

1. Cliquez sur l'icône pour modifier la tuile de domaine.

   Le volet **Modifier les informations de la carte** apparaît.

2. Sélectionnez un type de graphique :

   - **Distribution des attaques** : affiche la sévérité des attaques.



- **Nombre d'événements** : affiche les 3 principales attaques et leur nombre d'occurrences.



3. Cliquez sur **Enregistrer**.

   Tenable Identity Exposure met à jour le graphique.

Voir aussi

- Indicateurs d'attaque
- Incidents liés aux indicateurs d'attaque

Incidents liés aux indicateurs d'attaque

La liste d'incidents Indicateurs d'attaques (IoA) fournit des informations détaillées sur des attaques spécifiques sur votre infrastructure Active Directory (AD). Cela vous permet de prendre les mesures nécessaires en fonction du niveau de sévérité des IoA.

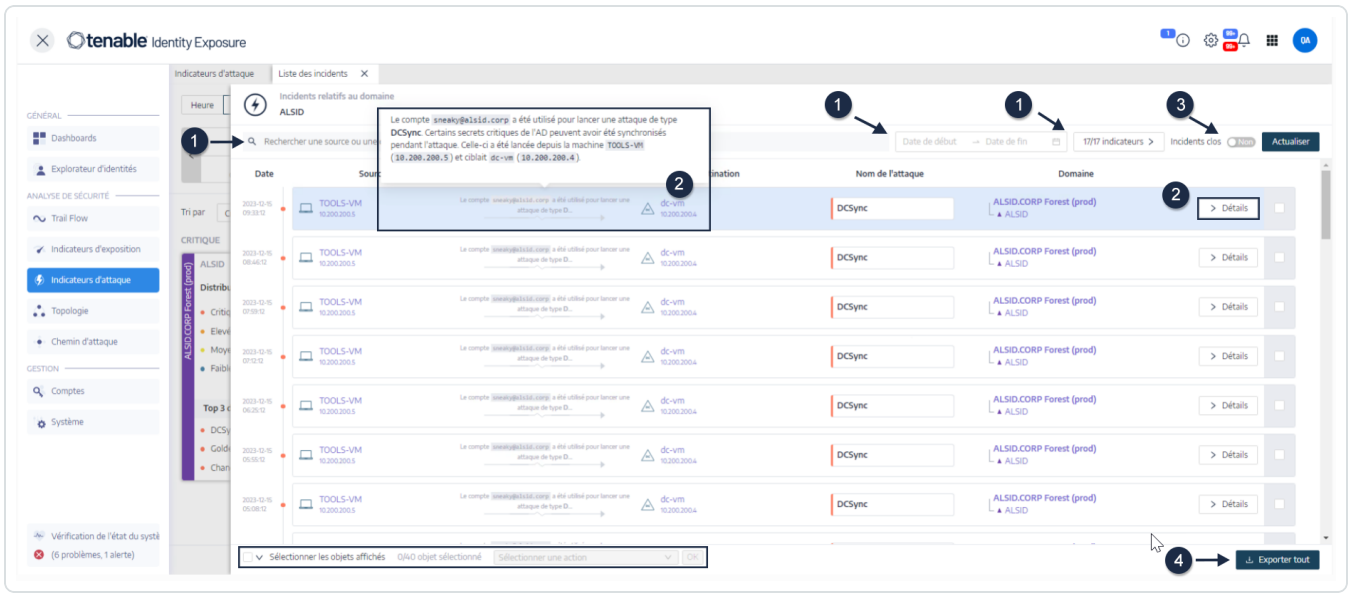
Pour afficher les incidents d'attaque :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'attaque** dans le volet de navigation.

   Le volet **Indicateurs d'attaque** apparaît.

2. Cliquez sur une tuile de domaine.

   Le volet **Liste des incidents** affiche la liste des incidents survenus sur le domaine.

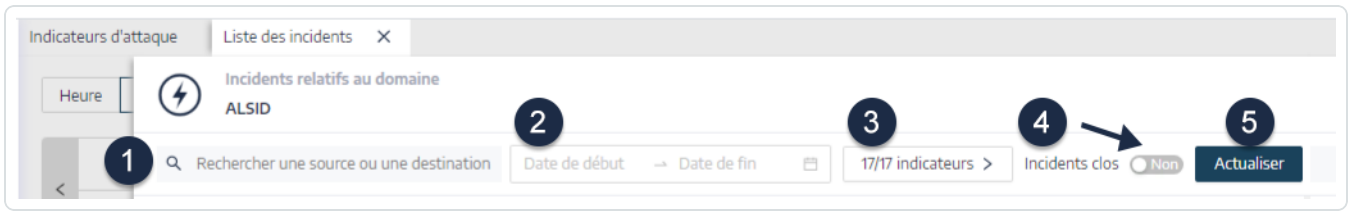


3. Dans cette liste, vous pouvez effectuer les actions suivantes :
    - Définir des critères de recherche pour rechercher des incidents spécifiques (**1**).
    - Accéder à des explications détaillées sur les attaques affectant l'infrastructure (**2**).
    - Fermer ou rouvrir un incident (**3**).
    - Télécharger un rapport montrant tous les incidents (**4**).

Pour rechercher un incident :

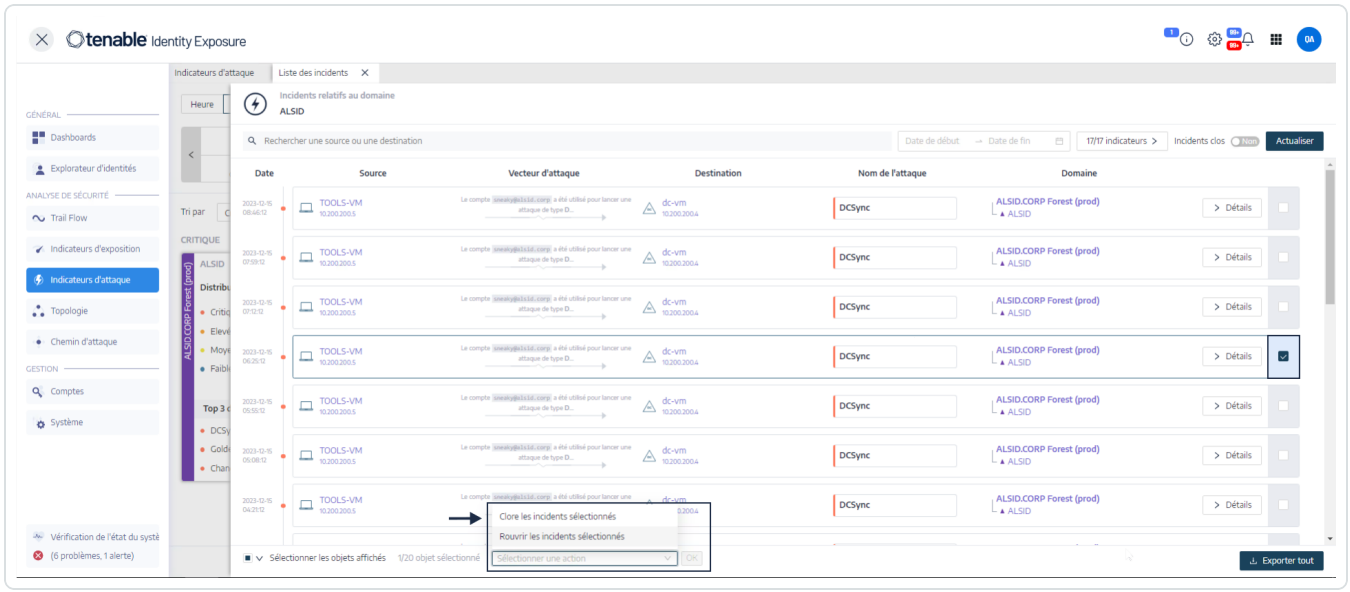
1. Dans la zone de **recherche**, saisissez le nom d'une source ou d'une destination.
2. Cliquez sur le sélecteur de date pour sélectionner les dates de début et de fin de l'incident.
3. Cliquez sur **n/n Indicateurs** pour sélectionner les indicateurs associés.
4. Cliquez sur le curseur **Incidents clos** pour activer l'option **Oui**, afin de limiter la recherche aux incidents clos.
5. Cliquez sur **Actualiser**.

   Tenable Identity Exposure met à jour la liste avec les incidents correspondants.



Pour clore un incident :

1. Dans la liste des incidents, sélectionnez un incident à clore ou à rouvrir.



2. Au bas du volet, cliquez sur le menu déroulant et sélectionnez **Clore les incidents sélectionnés**.
3. Cliquez sur **OK**.

   Un message demande de confirmer la clôture.
4. Cliquez sur **Confirmer**.

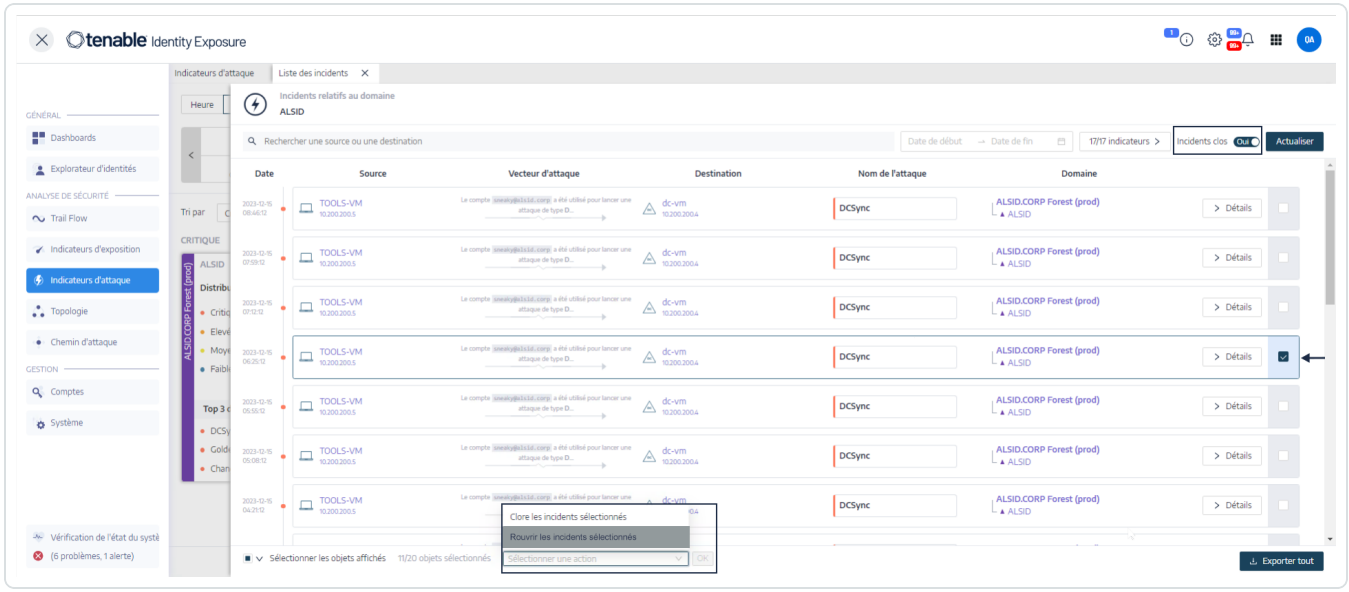
   Un message confirme que Tenable Identity Exposure a clos l'incident et ne l'affiche plus.

Pour rouvrir un incident :

1. Dans le volet **Liste des incidents**, cliquez sur le curseur **Incidents clos** pour activer l'option **Oui**.

Tenable Identity Exposure met à jour la liste des incidents clos.

2. Sélectionnez l'incident à rouvrir.



3. Au bas du volet, cliquez sur le menu déroulant et sélectionnez **Rouvrir l'incident sélectionné**.
4. Cliquez sur **OK**.

   Un message confirme que Tenable Identity Exposure a rouvert l'incident.

Astuce : vous pouvez fermer ou rouvrir plusieurs incidents simultanément. Au bas du volet, cliquez sur **Sélectionner les objets affichés**.

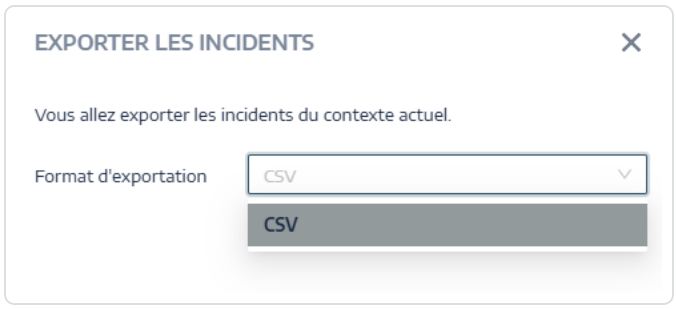
Pour exporter des incidents

1. Dans le volet **Liste des incidents**, cliquez sur le bouton **Exporter tout** en bas.

   Le panneau latéral **Exporter les incidents** s'ouvre.

2. Dans la zone de liste déroulante **Séparateur**, sélectionnez un séparateur pour les données exportées : **virgule** ou **point-virgule**.

   Tenable Identity Exposure exporte les données au format CSV pour permettre leur téléchargement.



Détails de l'incident

Chaque entrée de la liste des incidents affiche les informations suivantes :

- **Date** : date à laquelle l'incident déclenchant l'IoA s'est produit. Tenable Identity Exposure affiche le plus récent en haut de la chronologie.
- **Source** : la source à l'origine de l'attaque et son adresse IP.
- **Vecteur d'attaque** : explication de ce qui s'est passé pendant l'attaque.

  Astuce : survolez le vecteur d'attaque pour afficher plus d'informations sur l'IoA.
- **Destination** : cible de l'attaque et son adresse IP.
- **Nom de l'attaque** : nom technique de l'attaque.
- **Domaine** : domaines touchés par l'attaque.

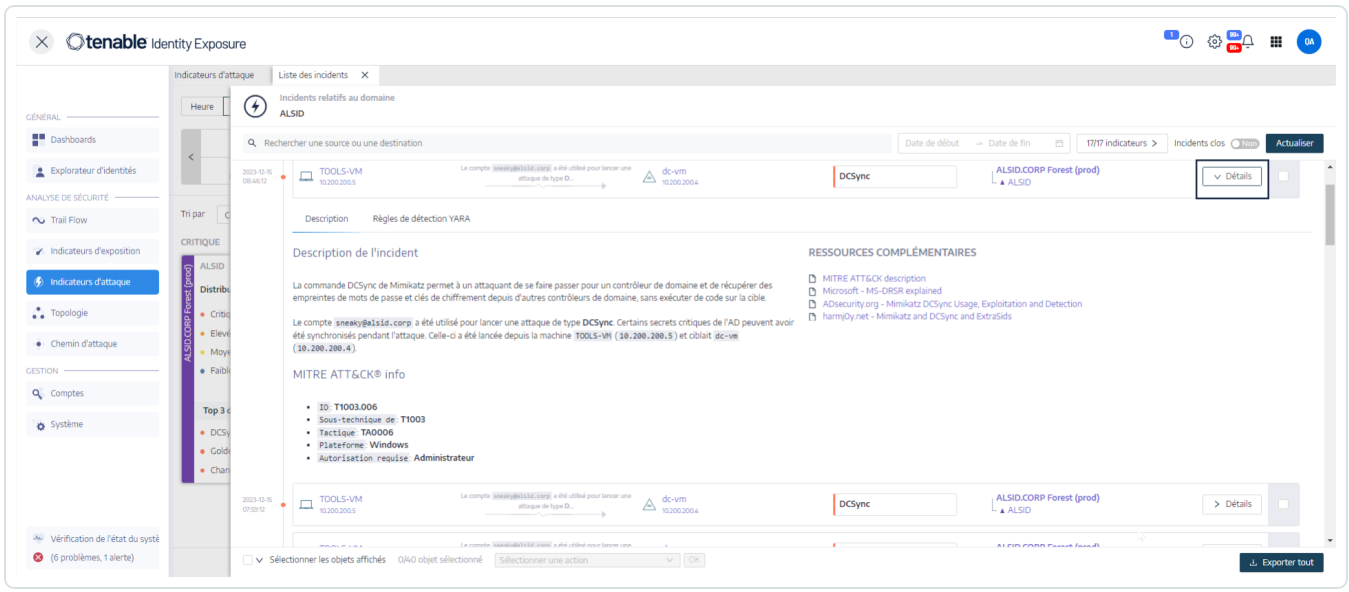
  Astuce : Tenable Identity Exposure peut afficher un maximum de cinq volets lorsque vous cliquez sur plusieurs éléments interactifs (liens, boutons d'action, etc.) dans la **liste des incidents**. Pour fermer tous les volets simultanément, cliquez n'importe où sur la page.

Détails de l'attaque

Dans la liste des incidents, vous pouvez explorer une attaque et prendre les mesures nécessaires pour y remédier.

Pour afficher les détails d'une attaque :

1. Dans la liste des incidents, sélectionnez un incident pour afficher ses détails.
2. Cliquez sur **Détails**.



Tenable Identity Exposure affiche les détails associés à l'attaque :

Description

L'onglet **Description** contient les sections suivantes :

- **Description de l'incident** : décrit brièvement l'attaque.
- **Informations MITRE ATT&CK** : fournit des informations techniques extraites de la base de connaissances Mitre Att&ck (tactiques et techniques adverses et connaissances générales). Mitre Att&ck est un cadre qui classe les attaques adverses et décrit les actions entreprises par les attaquants après la compromission d'un réseau. Il fournit également des identifiants standard pour les vulnérabilités de sécurité, dotant ainsi la communauté de cyber-sécurité d'un langage commun.
- **Ressources complémentaires** : fournit des liens vers des sites web, des articles et des livres blancs qui proposent des informations plus détaillées sur l'attaque.

Règles de détection YARA

L'onglet **Règles de détection YARA** décrit les règles YARA que Tenable Identity Exposure utilise pour détecter les attaques AD au niveau du réseau, afin de renforcer la chaîne de détection de Tenable Identity Exposure.

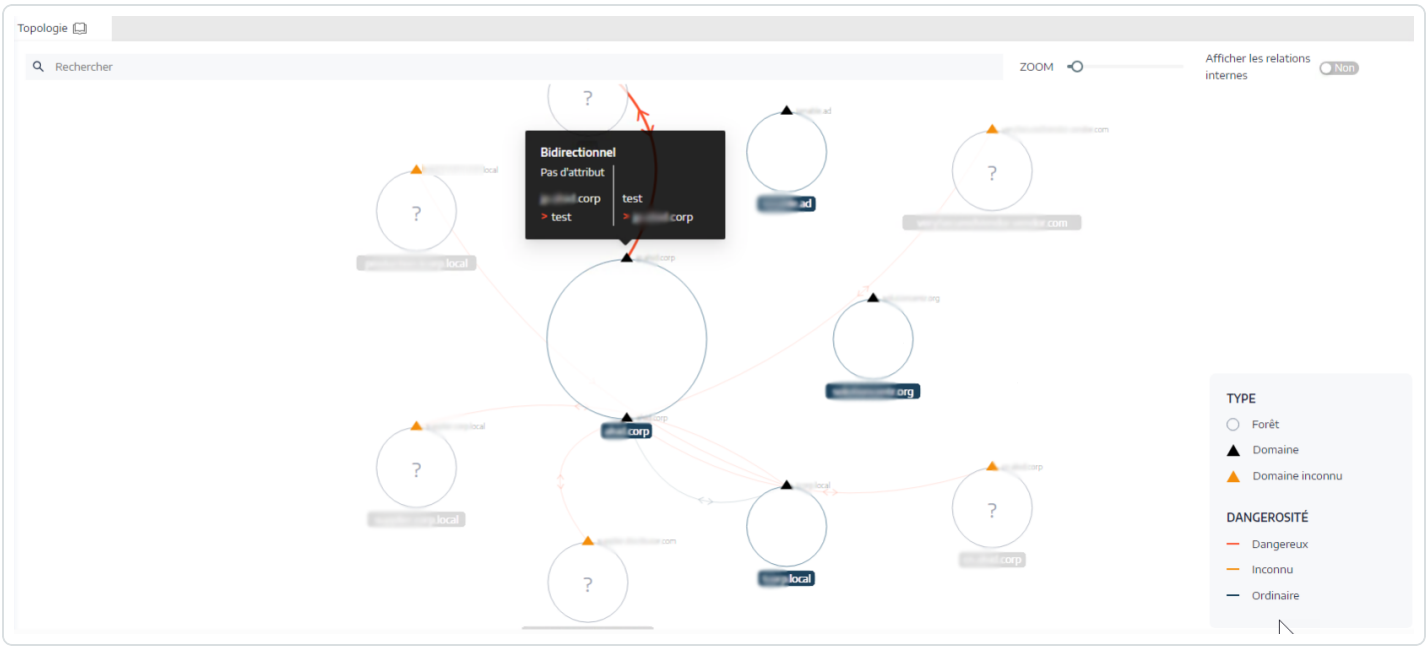
Remarque : YARA est le nom d'un outil principalement utilisé dans la recherche et la détection des logiciels malveillants. Il s'appuie sur des règles pour créer des descriptions de familles de logiciels malveillants sur la base de modèles textuels ou binaires. Une description est essentiellement un nom de règle YARA, et ces règles se composent de chaînes combinées par une expression booléenne (source : wikipedia.org).

Voir aussi

- Indicateurs d'attaque
- Détails d'un indicateur d'attaque

Topologie

La page Topologie fournit une visualisation graphique interactive de votre infrastructure Active Directory. Le **graphique de topologie** affiche les forêts, les domaines et les relations d'approbation qui existent entre eux.



Pour ouvrir la page Topologie :

- Dans Tenable Identity Exposure, cliquez sur **Topologie** dans le menu de navigation de gauche.

  Le volet Topologie apparaît avec la représentation graphique de votre architecture AD.

Pour rechercher un domaine :

- Dans le volet **Topologie**, saisissez un nom de domaine dans la zone de **recherche**.

  Tenable Identity Exposure met le domaine en évidence.

Pour zoomer sur le graphique :

- Dans le volet **Topologie**, cliquez sur le curseur **Zoom** pour ajuster la taille du graphique.

Pour afficher le lien entre deux domaines :

- Dans le volet **Topologie**, cliquez sur le curseur **Afficher les relations internes** pour activer l'option **Oui**.

Pour afficher les détails d'un domaine :

- Dans le volet **Topologie**, cliquez sur ▲ devant le nom de domaine.

  Le volet **Détails du domaine** apparaît avec les indicateurs d'exposition (IoE) détectés et le score de conformité du domaine. Vous pouvez cliquer sur la tuile de l'IoE pour accéder à plus d'informations.

Voir aussi

- Relations d'approbation
- Relations d'approbation dangereuses

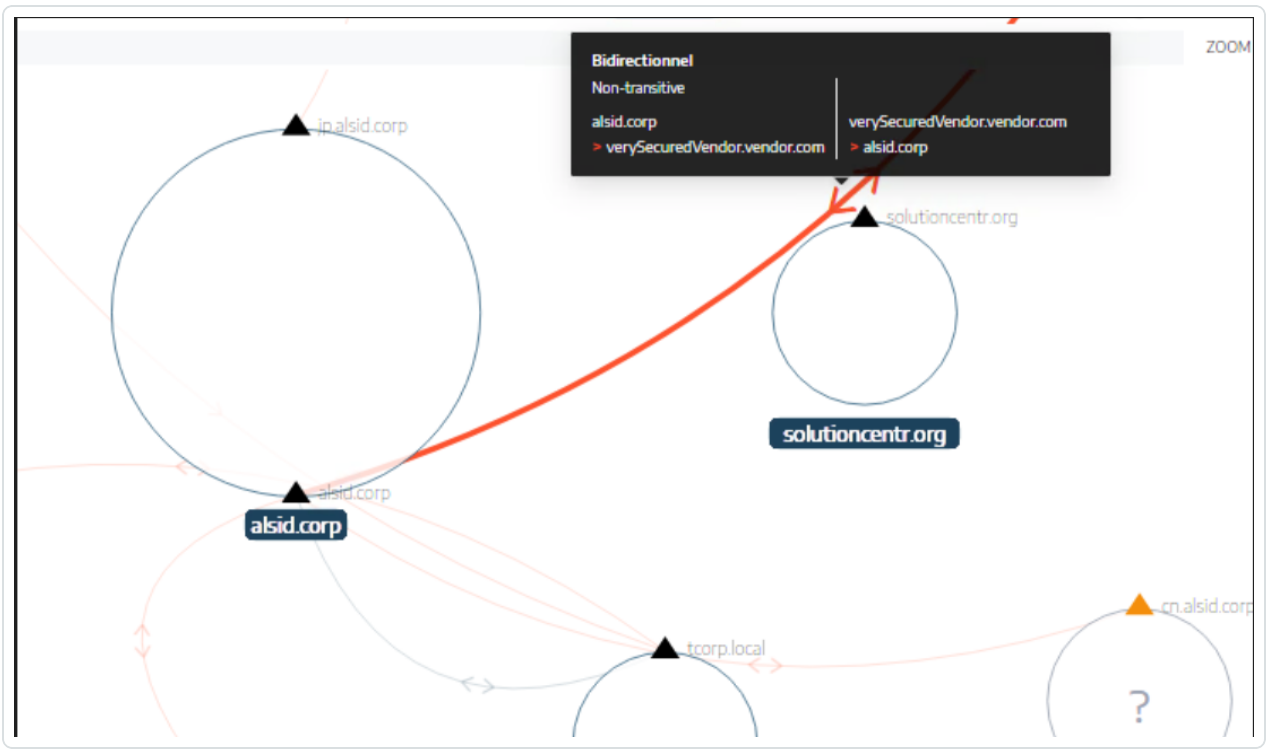
Relations d'approbation

Les flèches courbes entre les domaines sur le graphique de topologie représentent les relations d'approbation.

Pour afficher les relations d'approbation :

- Sur le graphique de topologie, survolez les flèches courbes.

  Tenable Identity Exposure affiche les relations d'approbation entre deux entités ainsi que des attributs spécifiques.



La couleur d'une relation d'approbation dépend de son niveau de menace :

- **Rouge** pour les relations d'approbation dangereuses
- **Orange** pour les relations d'approbation normales
- **Bleu** pour les relations d'approbation inconnues

Pour plus d'informations, voir Relations d'approbation dangereuses.

Les informations des attributs d'approbation indiquent la direction d'approbation – **unidirectionnelle** ou **bidirectionnelle** (entrante/sortante) – et affichent l'une des valeurs suivantes :

Valeur	Description
Non-transitive	Par défaut, les approbations dans les forêts sont transitives. Tenable Identity Exposure utilise cet indicateur pour les convertir en approbations non transitives. D'autre part, les approbations entre les forêts ne sont pas transitives par défaut, d'où la présence de l'indicateur de transitivité de forêt. Tenable Identity Exposure affiche cette valeur s'il existe une approbation entre les domaines au sein d'une même forêt. L'approbation n'accorde aucun accès et ne délègue aucune autorité aux domaines interconnectés au-delà de la forêt.

Forest transitive	Indique qu'une relation d'approbation transitive existe entre deux forêts. La relation d'approbation accordée à un autre domaine peut être transmise à la forêt approuvée.
Within forest	Indique qu'une relation d'approbation entre domaines existe dans la même forêt. Si `WITHIN_FOREST` et `QUARANTINED_DOMAIN` sont tous les deux présents, l'approbation est appelée **QuarantinedWithinForest**.
Uplevel only	Indique que seuls les clients exécutant les systèmes d'exploitation Windows 2000 ou des versions ultérieures peuvent utiliser cette relation d'approbation.
Treat as external	(Uniquement lorsque `FOREST_TRANSITIVE` s'applique) Indique un type de relation d'approbation externe. Tenable Identity Exposure modifie le filtrage des identifiants de sécurité (SID) sur la relation d'approbation et autorise les SID dont l'identifiant relatif (RID) est supérieur ou égal à 1 000 dans la forêt.
Quarantined	Indique que Tenable Identity Exposure a activé le filtrage des SID dont le RID est supérieur ou égal à 1 000 pour la relation d'approbation. Par défaut, Tenable Identity Exposure ne l'active que pour une relation d'approbation externe, mais il peut également l'appliquer à une relation d'approbation parent/enfant ou de forêt.
Cross-organization authentication	Indique que Tenable Identity Exposure a activé l'authentification sélective et peut l'utiliser dans les relations d'approbation entre domaines ou forêts.
Selective authentication	Voir « Cross-organization authentication ».
Cross organization without TGT delegation	Apparaît si la délégation dans un domaine approuvé est entièrement désactivée (ne définit jamais l'option ok-as-delegate dans les tickets de service émis).
RC4 encryption	Indique que la relation d'approbation prend en charge les clés de chiffrement RC4 pour les échanges Kerberos. Cet indicateur est présent

	uniquement si `trustType` s'applique à `TRUST_TYPE_MIT`.
AES keys	Indique que la relation d'approbation prend en charge les clés de chiffrement AES pour les échanges Kerberos.
PIM trust	Si les indicateurs `FOREST_TRANSITIVE` et `TREAT_AS_EXTERNAL` s'appliquent et que l'indicateur `QUARANTINED_DOMAIN` n'est pas activé, l'indicateur Pim Trust signale que la forêt approuvée gère les identités avec privilèges (Privileged Identity Management) concernant le filtrage SID (les SID locaux peuvent contourner cette approbation). La relation d'approbation PIM (Pim Trust) permet d'implémenter des forêts bastions.
Pas d'attribut	Indique que la relation d'approbation externe n'a pas d'attribut spécifique.

Relations d'approbation dangereuses

La couleur d'une relation d'approbation dépend de son niveau de menace :

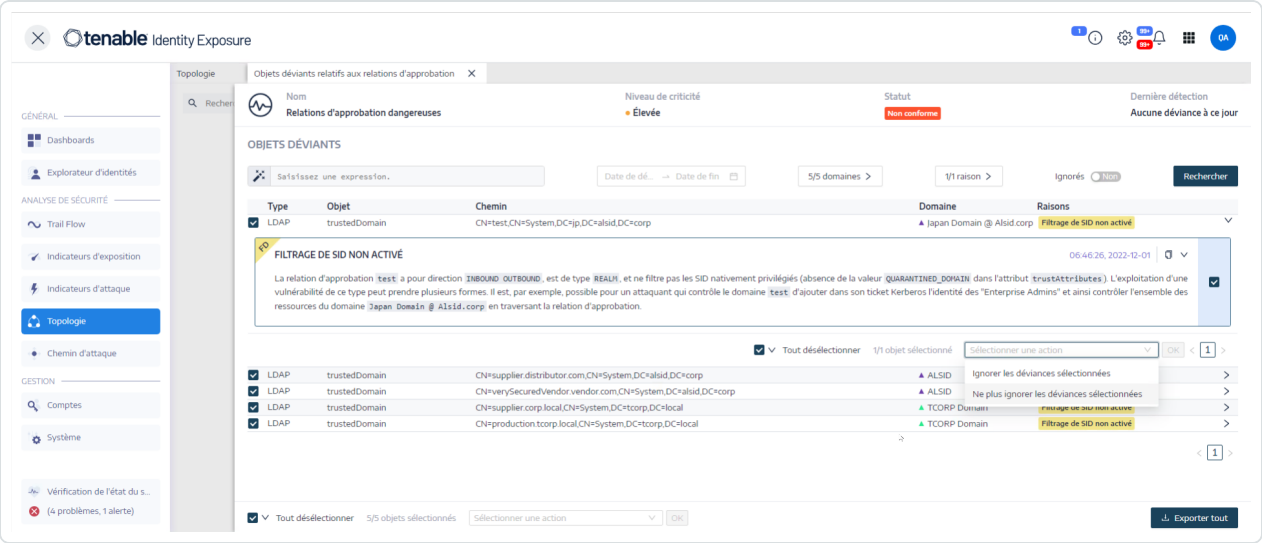
- **Rouge** pour les relations d'approbation dangereuses
- **Orange** pour les relations d'approbation normales
- **Bleu** pour les relations d'approbation inconnues

Pour investiguer une relation d'approbation dangereuse :

1. Sur le graphique de topologie, cliquez sur les flèches courbes.

   Le volet **Objets déviants liés aux relations d'approbation** apparaît.

   > **Conseils** : les détails des événements affichés sur ce volet des relations d'approbation dangereuses sont tous liés à l'indicateur d'exposition **Relations d'approbation dangereuses** auquel vous pouvez également accéder à partir du menu de navigation **Indicateurs d'exposition**.



2. Survolez un objet déviant de la liste et cliquez dessus pour afficher les détails.

Pour exporter des objets déviants :

1. Sur le graphique de topologie, cliquez sur les flèches courbes.

   Le volet **Objets déviants liés aux relations d'approbation** apparaît.

2. Cliquez sur **Exporter tout**.

   Le volet **Exporter les objets déviants** apparaît.

3. Dans la zone **Format d'exportation**, cliquez sur la flèche déroulante pour sélectionner un format.

4. Cliquez sur **Exporter tout**.

   Tenable Identity Exposure télécharge sur votre ordinateur un fichier ayant le format sélectionné.

5. Cliquez sur la croix (**X**) pour refermer le volet.

Chemin d'attaque

Tenable Identity Exposure offre plusieurs façons de visualiser la vulnérabilité potentielle d'un asset opérationnel à l'aide de représentations graphiques.

- **Chemin d'attaque** : affiche les chemins qu'un attaquant peut emprunter pour compromettre un asset à partir d'un point d'entrée.
- **Blast Radius** : affiche les mouvements latéraux possibles dans l'infrastructure Active Directory à partir de n'importe quel asset.
- **Exposition d'un asset** : affiche tous les chemins pouvant potentiellement prendre le contrôle d'un asset.

Comprendre le chemin d'attaque vous permet d'identifier les mesures d'atténuation nécessaires pour empêcher les attaquants d'exploiter les vulnérabilités. Cela peut impliquer de corriger les systèmes, de durcir les configurations, de mettre en œuvre des contrôles d'accès plus stricts ou de sensibiliser les utilisateurs.

Le chemin d'attaque dans Tenable Identity Exposure offre plusieurs avantages :

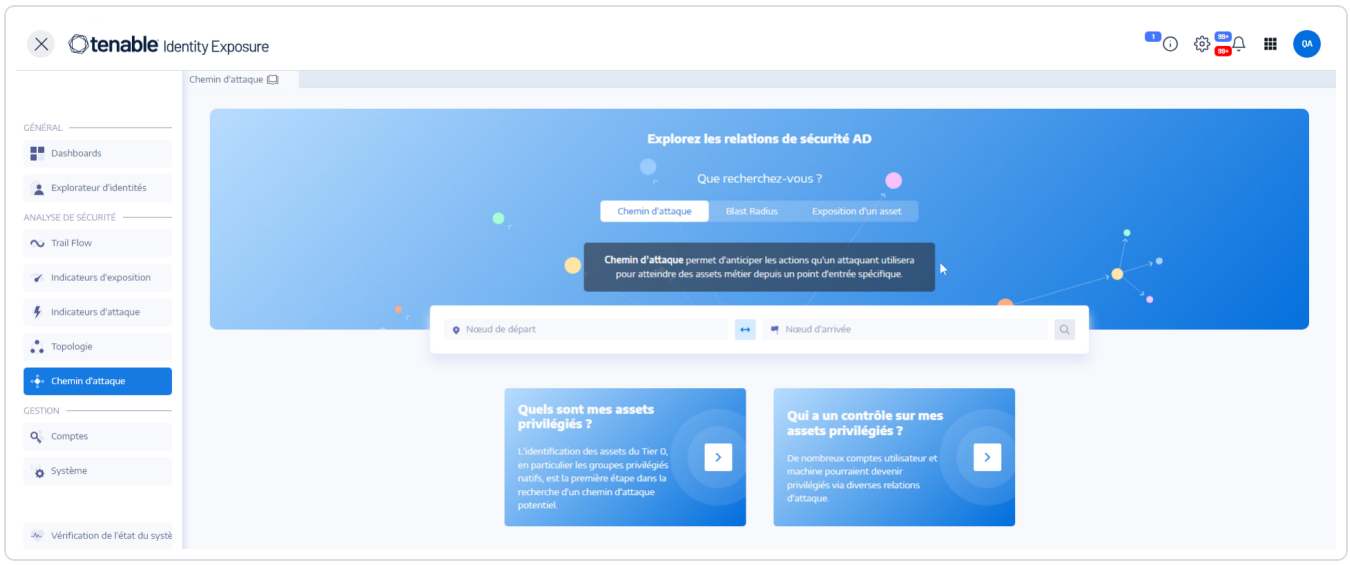
- **Sécurité proactive** : il permet d'anticiper et de traiter les vecteurs d'attaque potentiels avant qu'ils ne soient exploités.
- **Priorisation** : il oriente les efforts de sécurité vers les vulnérabilités et les chemins d'attaque les plus critiques.
- **Visualisation** : il fournit une représentation claire et facile à comprendre des relations de sécurité complexes au sein de votre infrastructure AD.
- **Communication** : il facilite la communication des risques de sécurité aux parties prenantes en fournissant des preuves visuelles des scénarios d'attaque potentiels.

Pour afficher le chemin d'attaque :

Vous spécifiez le point de départ, qui peut être n'importe quel asset de votre infrastructure AD (par exemple, un compte utilisateur, un ordinateur ou un groupe). Vous définissez le point d'arrivée, qui représente l'asset que l'attaquant vise à compromettre (par exemple, un contrôleur de domaine ou un serveur de données sensible).

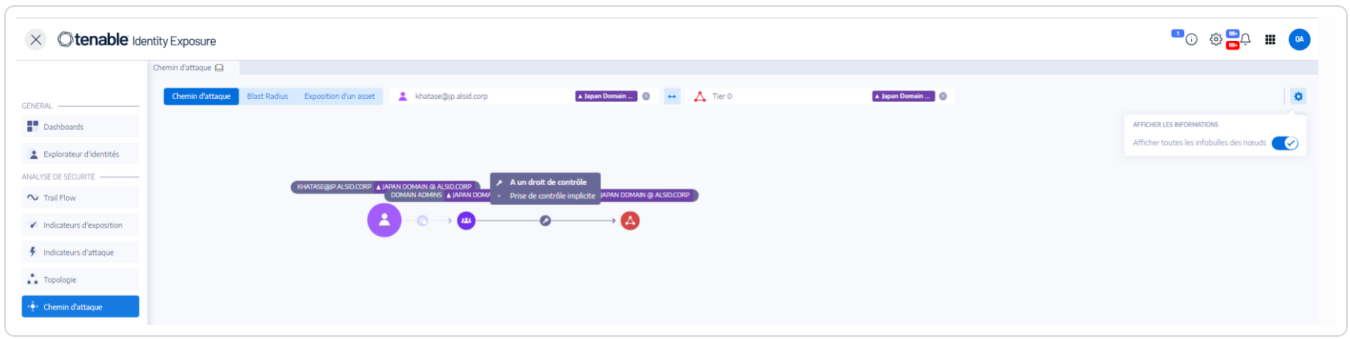
1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

   Le volet **Chemin d'attaque** apparaît.



2. Dans la bannière, cliquez sur **Chemin d'attaque**.
3. Dans la zone **Point de départ**, saisissez l'asset au point d'entrée.
4. Dans la zone **Point d'arrivée**, saisissez l'asset à la fin du chemin.
5. Cliquez sur l'icône .

   Tenable Identity Exposure affiche le chemin d'attaque entre les deux assets.



6. Éventuellement, vous pouvez cliquer sur l'icône pour effectuer les actions suivantes :
   - Cliquer sur le curseur **Zoom** pour ajuster le niveau de grossissement des graphiques.
   - Cliquer sur le curseur **Afficher toutes les infobulles des nœuds** pour afficher des informations sur les assets.

Pour afficher le Blast Radius (rayon d'impact) :

Tenable Identity Exposure affiche une représentation graphique du chemin d'attaque potentiel, mettant ainsi en évidence les connexions entre les assets. Chaque connexion représente une vulnérabilité ou une mauvaise configuration potentielle que l'attaquant pourrait exploiter pour se déplacer latéralement au sein de votre infrastructure AD. Vous pouvez zoomer et dézoomer pour mieux comprendre les détails du chemin.

1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

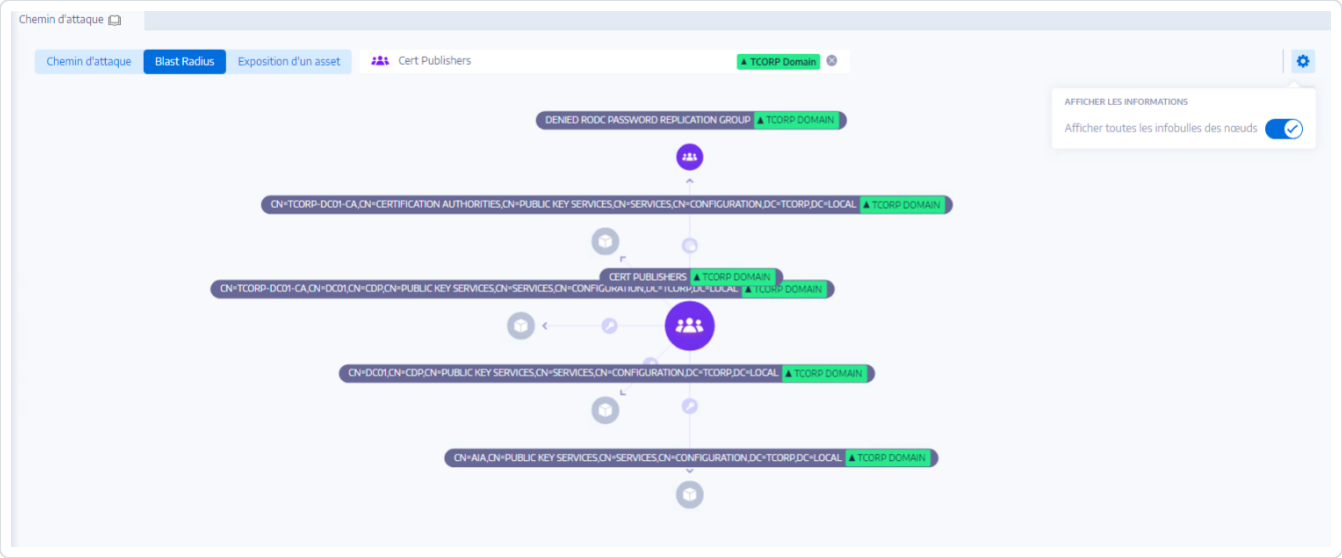
   Le volet **Chemin d'attaque** apparaît.

2. Dans la bannière, cliquez sur **Blast Radius**.

3. Dans la zone **Rechercher un objet**, saisissez le nom d'un asset.

4. Cliquez sur l'icône .

   Tenable Identity Exposure affiche les connexions latérales qui partent de l'asset :



5. Cliquez sur les icônes des flèches qui relient les assets pour afficher leurs relations.



Pour afficher l'exposition d'un asset :

Chaque étape du chemin d'attaque est associée à un score de risque indiquant la sévérité de la vulnérabilité. Cela vous aide à traiter en priorité les chemins qui constituent la menace la plus importante et requièrent une attention immédiate. Vous pouvez également cliquer sur des points de connexion individuels pour obtenir plus de détails sur la vulnérabilité ou la mauvaise configuration impliquée.

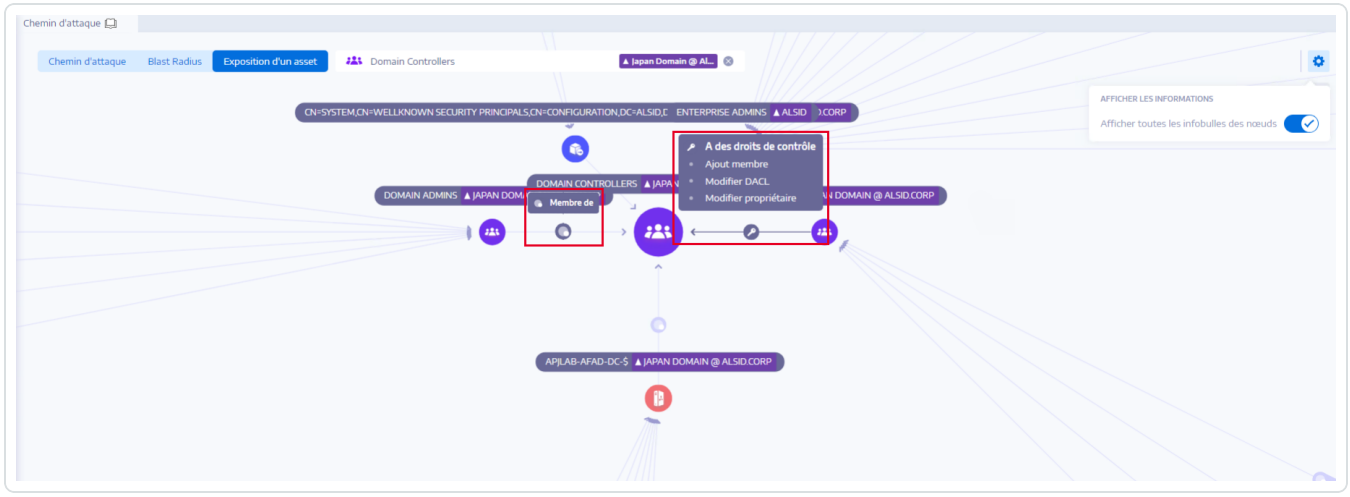
1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

   Le volet **Chemin d'attaque** apparaît.

2. Dans la bannière, cliquez sur **Exposition de l'asset**.
3. Dans la zone **Rechercher un objet**, saisissez le nom d'un asset.
4. Cliquez sur l'icône .

   Tenable Identity Exposure affiche les chemins vers l'asset et les relations entre les assets.

5. Cliquez sur les icônes des flèches qui relient les assets pour afficher leurs relations.



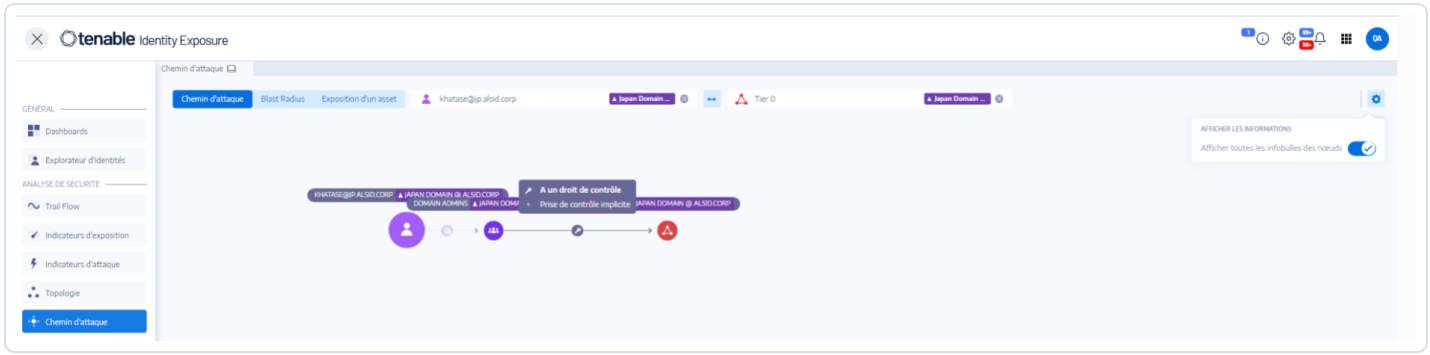
Pour épingler un chemin d'attaque :

Voir aussi

- Relations d'attaque
- Identification des assets Tier 0
- Comptes avec des chemins d'attaque
- Types de nœuds du chemin d'attaque

Relations d'attaque

Les relations d'attaque sont unidirectionnelles et vont d'un nœud source vers un nœud cible. Comme les relations sont transitives, les attaquants peuvent les enchaîner pour créer un « chemin d'attaque » :



Tenable Identity Exposure présente les relations d'attaque suivantes :

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Ajouter des identifiants de clé

Description

Le principal de sécurité source peut emprunter l'identité de la cible en exploitant les mappages de comptes de confiance clés, également appelés identifiants clés ou « identifiants fantômes ».

Cela est possible, car la source est autorisée à modifier l'attribut `msDS-KeyCredentialLink` de la cible.

C'est normalement Windows Hello for Business (WHfB) qui utilise cette fonctionnalité, mais elle peut être exploitée par les attaquants, même si elle n'est pas utilisée.

Exploitation

Les attaquants qui compromettent le principal de sécurité source doivent modifier l'attribut `msDS-KeyCredentialLink` de l'ordinateur cible à l'aide d'outils de piratage spécialisés tels que Whisker ou DSInternals.

Le but des attaquants est d'ajouter un nouveau certificat à l'attribut de cette cible, dont ils possèdent la clé privée. Ils peuvent ensuite s'authentifier en tant que cible avec la clé privée connue à l'aide du protocole Kerberos PKINIT pour obtenir un TGT. Ce protocole permet également aux attaquants de récupérer l'empreinte NTLM de la cible.

Remédiation

Plusieurs principaux de sécurité natifs avec privilèges disposent de cette autorisation par défaut, à savoir les opérateurs de compte, les administrateurs, les administrateurs de domaine, les administrateurs d'entreprise, les administrateurs de clés d'entreprise, les administrateurs de clés et SYSTEM. Ces principaux de sécurité légitimes ne nécessitent pas de remédiation.

Pour les principaux de sécurité source sans besoin légitime de modifier cet attribut, vous devez supprimer cette autorisation. Recherchez des autorisations telles que « Write all properties », « Write msDS-AllowedToActOnBehalfOfOtherIdentity », « Full control », etc.

Voir aussi

- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID

- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Ajouter un membre

Description

Le principal de sécurité source peut s'ajouter lui-même (droit d'écriture validé), ou une autre personne (droit de propriété en écriture), aux membres du groupe Cible et bénéficier des droits d'accès accordés au groupe.

Un principal de sécurité malveillant qui effectue cette opération crée une relation d'attaque « Membre de ».

Exploitation

Les attaquants qui compromettent le principal de sécurité source n'ont qu'à modifier l'attribut « membres » du groupe cible à l'aide de commandes Windows natives telles que « net group/domain », de commandes PowerShell comme « Add-ADGroupMember », d'outils d'administration tels que « Utilisateurs et ordinateurs Active Directory » ou d'outils de piratage dédiés tels que PowerSploit.

Remédiation

Si le principal de sécurité source n'a pas besoin du droit d'ajouter un membre au groupe cible, vous devez supprimer cette autorisation.

Pour modifier le descripteur de sécurité du groupe cible :

1. Dans « Utilisateurs et ordinateurs Active Directory », cliquez avec le bouton droit sur **Propriétés** > **Sécurité**.
2. Supprimez les autorisations telles que « Write Members » (Écrire les membres), « Write all properties » (Écrire toutes les propriétés), « Full control » (Contrôle total), « All validated writes » (Toutes les écritures validées), « Add/remove self as member » (Ajouter/supprimer soi-même en tant que membre), etc.

Remarque : un groupe peut hériter de l'autorisation d'un objet situé plus haut dans l'arborescence Active Directory.

Voir aussi

- Ajouter des identifiants de clé
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC

- Modifier DACL
- Modifier propriétaire

Autorisé à agir

Description

Le principal de sécurité source est autorisé à effectuer une délégation contrainte basée sur les ressources Kerberos sur l'ordinateur cible. Cela signifie qu'il peut emprunter l'identité de n'importe quel utilisateur lorsqu'il s'authentifie avec Kerberos dans un service exécuté sur l'ordinateur cible.

Cela conduit souvent à la compromission totale de l'ordinateur cible.

Cette attaque s'appelle également Délégation contrainte basée sur les ressources (RBCD), Délégation contrainte basée sur les ressources Kerberos (KRBCD), Délégation contrainte Kerberos basée sur les ressources (RBKCD) et « autorisé à agir au nom d'une autre identité ».

Exploitation

Les attaquants qui compromettent le principal de sécurité source peuvent utiliser des outils de piratage dédiés tels que Rubeus pour exploiter les extensions de protocole Kerberos légitimes (S4U2self et S4U2proxy), afin de falsifier des tickets de service Kerberos et d'emprunter l'identité de l'utilisateur ciblé. Les attaquants choisiront probablement d'usurper l'identité d'un utilisateur avec privilèges pour obtenir un accès avec privilèges.

Une fois que les attaquants ont falsifié le ticket de service, ils peuvent utiliser n'importe quel outil d'administration natif ou de piratage spécialisé compatible avec Kerberos pour exécuter des commandes arbitraires à distance.

Une tentative d'exploitation réussie doit respecter les contraintes suivantes :

- Les principaux de sécurité source et cible doivent avoir un nom de principal de service (ServicePrincipalName). Tenable Identity Exposure ne crée pas cette relation d'attaque sans cette condition.
- Le compte ciblé pour l'usurpation d'identité ne doit pas avoir l'indicateur « est sensible et ne peut pas être délégué » (`ADS_UF_NOT_DELEGATED` dans UserAccountControl) ni être membre

du groupe « Protected Users » (Utilisateurs protégés), car Active Directory protège ces comptes des attaques par délégation.

Remédiation

Si le principal de sécurité source n'a pas besoin de l'autorisation d'effectuer une délégation restreinte basée sur les ressources Kerberos (RBCD) sur l'ordinateur cible, vous devez la supprimer. Vous devez effectuer la modification sur la cible, contrairement à la relation d'attaque par délégation « Autorisé à déléguer ».

Vous ne pouvez pas gérer RBCD avec les outils d'administration graphiques existants tels que « Utilisateurs et ordinateurs Active Directory ». Vous devez utiliser PowerShell pour modifier le contenu de l'attribut `msDS-AllowedToActOnBehalfOfOtherIdentity`.

Utilisez les commandes suivantes pour répertorier les principaux de sécurité source autorisés à agir sur la cible (dans la section « Accès ») :

```
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -
ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

Si aucun des principaux de sécurité répertoriés n'est souhaité, vous pouvez tous les supprimer avec cette commande :

```
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

Si vous devez supprimer un seul principal de sécurité de la liste, Microsoft ne fournit malheureusement pas de commande directe. Pour supprimer l'attribut, utilisez la même liste en retirant l'attribut souhaité. Par exemple, si « sourceA », « sourceB » et « sourceC » sont tous autorisés et que vous souhaitez supprimer uniquement « sourceB », exécutez :

```
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

Enfin, en tant que recommandation générale, afin de limiter l'exposition des comptes avec privilèges sensibles à ces attaques par délégation, Tenable Identity Exposure recommande de leur donner l'indicateur « est sensible et ne peut pas être délégué » (`ADS_UF_NOT_DELEGATED`) ou de les ajouter au groupe « Protected Users » (Utilisateurs protégés), après avoir vérifié minutieusement les impacts opérationnels.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Autorisé à déléguer

Description

Le principal de sécurité de la source est autorisé à effectuer une délégation contrainte Kerberos (KCD) avec transition de protocole sur l'ordinateur cible. Cela signifie qu'il peut emprunter l'identité de n'importe quel utilisateur lorsqu'il s'authentifie avec Kerberos dans un service exécuté sur l'ordinateur cible.

Cela conduit souvent à la compromission totale de l'ordinateur cible.

Exploitation

Les attaquants qui compromettent le principal de sécurité source peuvent utiliser des outils de piratage dédiés tels que Rubeus pour exploiter les extensions de protocole Kerberos légitimes (S4U2self et S4U2proxy), afin de falsifier des tickets de service Kerberos et d'emprunter l'identité de l'utilisateur ciblé. Les attaquants choisiront probablement d'usurper l'identité d'un utilisateur avec privilèges pour obtenir un accès avec privilèges.

Une fois que les attaquants ont falsifié le ticket de service, ils peuvent utiliser n'importe quel outil d'administration natif ou de piratage spécialisé compatible avec Kerberos pour exécuter des commandes arbitraires à distance.

Une tentative d'exploitation réussie doit respecter les contraintes suivantes :

- Le principal de sécurité source doit être activé pour la transition de protocole (`ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION` dans UserAccountControl/ « Utiliser tout protocole d'authentification » dans l'interface graphique de délégation). Plus précisément, l'attaque peut fonctionner sans transition de protocole (« Utiliser Kerberos uniquement » dans l'interface graphique de délégation), mais les attaquants doivent d'abord contraindre une authentification Kerberos de l'utilisateur ciblé vers le principal de sécurité source, ce qui complique l'attaque. Par conséquent, Tenable Identity Exposure ne crée pas de relation d'attaque dans ce cas.
- Les principaux de sécurité source et cible doivent avoir un nom de principal de service (ServicePrincipalName). Tenable Identity Exposure ne crée pas cette relation d'attaque sans cette condition.
- Le compte ciblé par l'usurpation ne doit pas porter l'indicateur « est sensible et ne peut pas être délégué » (`ADS_UF_NOT_DELEGATED` dans UserAccountControl) ni être membre du groupe « Protected Users » (Utilisateurs protégés), car Active Directory protège ces comptes contre les attaques par délégation.

En revanche, l'ordinateur cible, sur lequel la délégation est autorisée, est désigné par un nom principal de service (SPN) et contient donc un service spécifique tel que SMB avec « cifs/host.exemple.net », HTTP avec « http/host.exemple.net », etc. Cependant, les attaquants peuvent cibler tout autre SPN et service exécuté sous le même compte cible dans le cadre d'une « attaque par substitution de nom ». Il ne s'agit donc pas d'une limitation.

Remédiation

Si le principal de sécurité source n'a pas besoin de l'autorisation d'effectuer une délégation contrainte Kerberos (KCD) sur l'ordinateur cible, vous devez le supprimer. Vous devez effectuer la modification dans la source, contrairement à une relation d'attaque par délégation « Autorisé à agir ».

Pour supprimer le principal de sécurité source :

1. Dans l'interface graphique d'administration « Utilisateurs et ordinateurs Active Directory », accédez à l'onglet **Propriétés** > **Délégation** de l'objet source.
2. Supprimez le nom principal du service correspondant à la cible.
3. Si vous ne souhaitez aucune délégation à partir de cette source, supprimez tous les SPN et sélectionnez « Ne pas approuver cet ordinateur pour la délégation ».

Vous pouvez également utiliser PowerShell pour modifier le contenu de l'attribut « msDS-AllowedToDelegateTo » de la source.

- Par exemple, dans Powershell, exécutez cette commande pour remplacer toutes les valeurs :

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @{ "msDS-
AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }
```

- Si vous ne souhaitez aucune délégation à partir de cette source, exécutez la commande suivante pour effacer l'attribut :

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-
AllowedToDelegateTo"
```

Il est également possible de réduire le risque sans fermer complètement ce chemin d'attaque en désactivant la transition de protocole. Il faut pour cela que tous les principaux de sécurité se connectent à la source en utilisant uniquement Kerberos au lieu de NTLM.

Pour désactiver la transition de protocole :

1. Dans l'interface graphique d'administration « Utilisateurs et ordinateurs Active Directory », accédez à l'onglet **Propriétés** > **Délégation** de l'objet source.
2. Sélectionnez « Utiliser uniquement Kerberos » à la place de « Utiliser tout protocole d'authentification ».

Vous pouvez également exécuter la commande suivante dans PowerShell pour désactiver la transition de protocole :

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation
$false
```

Enfin, d'une manière générale, afin de limiter l'exposition des comptes avec privilèges sensibles à ces attaques par délégation, Tenable Identity Exposure il est recommandé de leur donner l'indicateur « est sensible et ne peut pas être délégué » (`ADS_UF_NOT_DELEGATED`) ou de les ajouter au groupe « Protected Users » (Utilisateurs protégés), après avoir vérifié minutieusement les impacts opérationnels.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC

- Modifier DACL
- Modifier propriétaire

Appartient à la GPO

Description

Le fichier ou le dossier GPO source dans le partage SYSVOL appartient au GPC cible (GPO), ce qui signifie qu'il définit les paramètres ou les programmes/scripts que la GPO applique.

Exploitation

Ce n'est pas une relation d'attaque qu'un attaquant utiliserait isolément. Cependant, à titre d'exemple, elle peut mettre en évidence des chemins d'attaque complets, dans lesquels les attaquants ayant le contrôle sur un fichier/dossier GPO appartenant à une GPO peuvent forcer l'application de paramètres arbitraires ou lancer des scripts sur les utilisateurs/ordinateurs à la fin du chemin d'attaque.

Remédiation

Cette relation montre comment les fichiers et dossiers GPO trouvés dans SYSVOL sont liés à l'objet GPC (GPO) correspondant. Cette situation est normale et conforme à la conception.

Aucune remédiation n'est nécessaire.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- DCSync
- Attribuer autorisé à agir
- A un historique SID

- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

DCSync

Description

DCSync est une fonctionnalité Active Directory légitime que les contrôleurs de domaine n'utilisent que pour répliquer des modifications, mais que les principaux de sécurité illégitimes peuvent également utiliser.

Le principal de sécurité source peut demander des secrets sensibles (hachages de mot de passe, clés Kerberos, etc.) à un domaine cible en utilisant la fonctionnalité DCSync, ce qui a pour effet de compromettre entièrement le domaine.

Pour récupérer des secrets, deux autorisations de sécurité sont requises : « Réplication des modifications d'annuaire » (`DS-Replication-Get-Changes`) et « Réplication de toutes les modifications de l'annuaire » (`DS-Replication-Get-Changes-All`). La relation se produit uniquement si vous accordez ces deux autorisations à la source, soit directement, soit par l'appartenance à un groupe imbriqué.

Exploitation

Les attaquants qui compromettent le principal de sécurité source peuvent récupérer des secrets à l'aide d'outils de piratage dédiés tels que *mimikatz* ou *impacket*.

- **Golden Ticket** : résulte de l'obtention de l'empreinte du mot de passe du compte « krbtgt », qui permet de falsifier un TGT Kerberos et d'emprunter l'identité de n'importe qui sur n'importe quel ordinateur ou service. Cela confère notamment des privilèges administratifs sur n'importe quel ordinateur du domaine.
- **Silver Ticket** : il résulte de l'obtention de l'empreinte du mot de passe d'un compte d'ordinateur/service, ce qui permet de falsifier un ticket de service Kerberos et d'emprunter l'identité de n'importe qui sur l'ordinateur ou service en question.

Remédiation

Les principaux de sécurité légitimes autorisés par défaut à utiliser DCSync sont les suivants :

- Administrateurs
- Administrateurs de domaine
- Administrateurs d'entreprise
- SYSTEM

De plus, la configuration Microsoft Entra ID Connect permet à son compte de service de synchronisation de l'empreinte du mot de passe (MSOL_...) d'exploiter DCSync.

Enfin, il est possible de découvrir des comptes de service pour certains outils de sécurité, notamment des solutions d'audit de mots de passe. Vérifiez leur légitimité auprès des responsables.

Vous devez supprimer cette autorisation pour les principaux de sécurité source qui n'ont pas un besoin légitime d'exécuter DCSync.

Pour modifier le descripteur de sécurité du domaine cible :

1. Dans « Utilisateurs et ordinateurs Active Directory », cliquez avec le bouton droit de la souris sur le nom du domaine et sélectionnez Propriétés > Sécurité.
2. Supprimez les autorisations « Réplication des modifications d'annuaire » et « Réplication de toutes les modifications de l'annuaire » pour les principaux de sécurité illégitimes.

> **Remarque** : les relations DCSync peuvent être le résultat d'autorisations héritées d'un groupe imbriqué. Par conséquent, selon la situation, vous devrez supprimer les groupes eux-mêmes ou seulement certains de leurs membres.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Attribuer autorisé à agir

Description

Le principal de sécurité source est autorisé à s'accorder ou à accorder à quelqu'un d'autre une relation Autorisé à agir avec l'ordinateur cible. Cette situation conduit souvent à la compromission totale de l'ordinateur cible par le biais d'une attaque par délégation Kerberos RBCD.

Cela s'explique par le fait que la source a le droit de modifier l'attribut « msDS-AllowedToActOnBehalfOtherIdentity » de la cible.

Un principal de sécurité malveillant qui effectue cette opération peut créer une relation d'attaque « Autorisé à agir ».

Exploitation

Les attaquants qui compromettent le principal de sécurité source doivent modifier l'attribut `msDS-AllowedToActOnBehalfOfOtherIdentity` de l'ordinateur cible à l'aide de PowerShell (par exemple « Set-ADComputer<target> -PrincipalsAllowedToDelegateToAccount ... »).

Remédiation

Plusieurs principes de sécurité par défaut avec privilèges disposent de cette autorisation, à savoir les opérateurs de compte, les administrateurs, les administrateurs de domaine, les administrateurs d'entreprise et SYSTEM. Ces principaux de sécurité légitimes ne nécessitent pas de remédiation.

Kerberos RBCD est conçu pour que les administrateurs d'un ordinateur puissent accorder les droits de délégation sur l'ordinateur à toute personne qui en a besoin. Cette méthode diffère des autres modes de délégation Kerberos qui requièrent une autorisation au niveau des administrateurs de domaine. Ainsi, les administrateurs de niveau inférieur peuvent gérer eux-mêmes ces paramètres de sécurité, un principe également appelé délégation. Dans ce cas, la relation est légitime.

Toutefois, si le principal de sécurité source n'est pas un administrateur légitime de l'ordinateur cible, la relation n'est pas légitime et vous devez supprimer cette autorisation.

Pour modifier le descripteur de sécurité de l'ordinateur cible :

1. Dans « Utilisateurs et ordinateurs Active Directory », cliquez avec le bouton droit sur **Propriétés** > **Sécurité**.
2. Supprimez l'autorisation accordée au principal de sécurité source. Recherchez des autorisations telles que « Write msDS-AllowedToActOnBehalfOfOtherIdentity », « Toutes les propriétés en écriture », « Restrictions de compte en écriture », « Contrôle total », etc.

> **Remarque** : le principal de sécurité source peut hériter de l'autorisation d'un objet situé plus haut dans l'arborescence Active Directory.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

A un historique SID

Description

Le principal de sécurité source détient le SID du principal de sécurité cible dans son attribut SIDHistory, ce qui signifie que la source a les mêmes droits que la cible.

L'historique des SID est un mécanisme légitime utilisé lors de la migration des principaux de sécurité entre des domaines pour conserver toutes les autorisations faisant référence à leur précédent SID fonctionnel.

Cependant, il s'agit également d'un mécanisme de persistance utilisé par les attaquants, car il permet à un compte de porte dérobée discret d'avoir les mêmes droits que la cible souhaitée, un compte administrateur par exemple.

Exploitation

Les attaquants qui compromettent le principal de sécurité source peuvent s'authentifier directement en tant que principal de sécurité cible puisque le SID de la cible est ajouté de manière transparente dans le jeton généré par les mécanismes d'authentification Active Directory (NTLM et Kerberos).

Remédiation

Si les principaux de sécurité source et cible sont liés à une migration de domaine approuvée, vous pouvez considérer que la relation est légitime et ne pas agir. Cette relation reste visible en tant que rappel de chemin d'attaque potentiel.

Si le domaine d'origine a été supprimé après la migration ou n'est pas configuré dans Tenable Identity Exposure, le principal de sécurité cible est marqué comme non résolu. Étant donné que le risque réside dans la cible et que cette cible n'existe pas, il n'existe pas de risque et donc aucune correction n'est requise.

En revanche, les relations d'historique de SID avec des utilisateurs ou des groupes avec des privilèges natifs sont très probablement malveillantes, car Active Directory empêche leur création. Ils ont donc probablement été créés à l'aide de techniques de piratage telles qu'une attaque « DCShadow ». Vous pouvez également trouver ces cas dans l'IoE lié à l'« historique des SID ».

Dans ce cas, Tenable Identity Exposure recommande d'effectuer une analyse contextuelle de l'ensemble de la forêt Active Directory, car les attaquants doivent avoir obtenu des privilèges élevés (administrateur de domaine ou équivalent) pour pouvoir modifier à des fins malveillantes l'historique des SID de la source. Cette analyse contextuelle permet d'analyser l'attaque avec les conseils de remédiation correspondants et d'identifier les portes dérobées potentielles à supprimer.

Enfin, Microsoft recommande de modifier tous les droits d'accès dans tous les services (partages SMB, Exchange, etc.) pour utiliser les nouveaux SID, et de supprimer les valeurs SIDHistory inutiles après la migration. Il s'agit d'une bonne pratique d'administration, bien qu'il soit très difficile d'identifier de manière exhaustive toutes les listes ACL et de les corriger.

Un utilisateur qui a le droit de modifier l'attribut SIDHistory sur l'objet source lui-même peut supprimer les valeurs SIDHistory. Contrairement à la création, cette opération ne nécessite pas de droits d'administrateur de domaine.

Pour ce faire, vous ne pouvez utiliser que PowerShell, car les outils graphiques tels que Utilisateurs et ordinateurs Active Directory échoueront. Exemple :

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

Attention : il est très facile de supprimer une valeur SIDHistory, mais très compliqué d'annuler cette opération. En effet, vous devez recréer la valeur SIDHistory, ce qui nécessite la présence de l'autre domaine susceptible d'être mis hors service. Pour cette raison, Microsoft recommande également de préparer des instantanés ou des sauvegardes.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC

- Modifier DACL
- Modifier propriétaire

Prise de contrôle implicite

Description

La source est un principal de sécurité Tier 0. Tier 0 (niveau 0) est l'ensemble des objets Active Directory qui disposent des privilèges les plus élevés dans le domaine, tels que les membres du groupe Administrateurs de domaine ou Contrôleurs de domaine. Tous les assets Tier 0 peuvent implicitement compromettre tout autre objet du domaine, même s'il n'existe aucune autre relation explicite.

Cette relation permet de modéliser des droits implicites intégrés à Active Directory. Ces droits étant propres à la conception et documentés, les attaquants les connaissent. Cependant, Tenable Identity Exposure ne peut pas collecter ces droits par des moyens standards. De plus, cette relation simplifie les graphes de chemin d'attaque, car dès que les attaquants compromettent un nœud Tier 0, ils peuvent attaquer directement n'importe quel autre objet sans passer par d'autres relations explicites.

En résumé, les assets Tier 0 source sont considérés comme ayant tous des relations de « prise de contrôle implicite » avec n'importe quel nœud cible du graphe.

Exploitation

La méthode d'exploitation exacte dépend du type d'asset Tier 0 source ciblé, mais ce sont des techniques bien documentées que les attaquants maîtrisent efficacement.

Remédiation

Cette relation est propre à la conception, et vous ne pouvez pas y remédier. Il est presque impossible d'empêcher un attaquant qui atteint un asset Tier 0 de poursuivre ses attaques.

Les efforts de remédiation doivent se concentrer sur les relations en amont dans les chemins d'attaque.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Hérite de GPO

Description

Un conteneur source pouvant être lié, comme une unité d'organisation (UO) ou un domaine (mais pas un site), contient l'unité d'organisation cible, l'utilisateur, le périphérique, le contrôleur de domaine ou le contrôleur de domaine en lecture seule (RODC) dans l'arborescence LDAP. En effet, les objets enfants du conteneur pouvant être lié héritent de la GPO à laquelle il est lié (voir Relations « GPO liée »).

Tenable Identity Exposure tient compte du blocage de l'héritage par une UO.

Exploitation

Les attaquants n'ont rien à faire pour exploiter cette relation tant qu'ils parviennent à compromettre la GPO en amont dans le chemin d'attaque. Conformément à la conception, la relation s'applique aux conteneurs pouvant être liés et aux objets situés en dessous, comme indiqué par les relations d'héritage de GPO.

Remédiation

Dans la plupart des cas, il est normal et légitime que les GPO s'appliquent aux conteneurs enfants pouvant être liés à partir de leurs conteneurs parents. Cependant, ce lien expose des chemins d'attaque supplémentaires.

Par conséquent, afin de réduire les risques, vous devez lier les GPO au niveau le plus bas de la hiérarchie des unités d'organisation, dans la mesure du possible.

De plus, les GPO doivent être protégées contre les modifications par des attaquants, afin de ne pas les exposer à d'autres relations d'attaque.

Enfin, les unités d'organisation peuvent désactiver l'héritage de GPO à partir des niveaux supérieurs grâce à leur option de blocage d'héritage. Cependant, n'utilisez cette option qu'en dernier recours, car elle bloque toutes les GPO, y compris, potentiellement, des GPO de durcissement de la sécurité définies au niveau du domaine le plus élevé. En outre, elle complique la logique liée aux GPO appliquées.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID

- Prise de contrôle implicite
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

GPO liée

Description

La GPO source est liée au conteneur cible, tel qu'un domaine ou une unité d'organisation (UO). Cela signifie que la GPO source peut attribuer des paramètres et exécuter des programmes sur les appareils et les utilisateurs contenus dans la cible. La GPO source s'applique également aux objets dans les conteneurs situés en dessous via les relations « Hérite de GPO ».

En fin de compte, la GPO peut compromettre les appareils et les utilisateurs sur lesquels elle s'applique.

Exploitation

Les attaquants doivent d'abord compromettre la GPO source via une autre relation d'attaque.

Ensuite, ils emploient plusieurs techniques pour effectuer des actions malveillantes sur les appareils et les utilisateurs contenus dans la cible et ceux en dessous. Exemples :

- Abus de « tâches planifiées immédiates » légitimes pour exécuter des scripts arbitraires sur les appareils.
- Ajout d'un nouvel utilisateur local avec des droits d'administration sur tous les appareils
- Installation d'un programme MSI
- Désactivation du pare-feu ou de l'antivirus

- Octroi de droits supplémentaires
- etc.

Les attaquants peuvent modifier une GPO en éditant manuellement son contenu à l'aide d'outils d'administration tels que « Gestion des stratégies de groupe » ou d'outils de piratage dédiés tels que PowerSploit.

Remédiation

Dans la plupart des cas, lier une GPO à un conteneur pouvant être lié est normal et légitime. Cependant, cette liaison augmente la surface d'attaque là où elle se produit, ainsi que dans les conteneurs en dessous.

Par conséquent, afin de réduire les risques, vous devez lier les GPO au niveau le plus bas de la hiérarchie des unités d'organisation, dans la mesure du possible.

De plus, les GPO doivent être protégées contre les modifications par des attaquants, afin de ne pas les exposer à d'autres relations d'attaque.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- Membre de

- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Membre de

Description

Le principal de sécurité source est membre du groupe cible. Par conséquent, il bénéficie de tous les droits d'accès que détient le groupe, tels que l'accès aux partages de fichiers, l'exécution de rôles dans les applications métier, etc.

Exploitation

Les attaquants n'ont rien à faire pour exploiter cette relation d'attaque. Il leur suffit de s'authentifier en tant que principal de sécurité source pour obtenir le groupe cible dans leur jeton de sécurité local ou distant, ou dans leur ticket Kerberos.

Remédiation

Si le principal de sécurité source est un membre illégitime du groupe cible, vous devez le supprimer.

Vous pouvez utiliser n'importe quel outil d'administration Active Directory standard tel que « Utilisateurs et ordinateurs Active Directory » ou une commande PowerShell telle que Remove-ADGroupMember.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer

- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Détient

Description

Le principal de sécurité source est le propriétaire déclaré de l'objet cible, car il l'a probablement créé. Les propriétaires ont des droits implicites (« Contrôle en lecture » et « Modifier DACL ») qui leur permettent d'obtenir des droits supplémentaires, pour eux-mêmes ou pour quelqu'un d'autre, et donc de compromettre l'objet cible.

Exploitation

Il suffit aux attaquants qui compromettent le principal de sécurité source de modifier le descripteur de sécurité de l'objet cible à l'aide de commandes Windows natives telles que « dsacls », de commandes PowerShell telles que « Set-ACL », d'outils d'administration tels que « Utilisateurs et ordinateurs Active Directory » ou d'outils de piratage spécialisés tels que PowerSploit.

La création d'un objet entraîne un risque d'élévation des privilèges. C'est le cas si un utilisateur à faibles privilèges (par exemple, un technicien du service d'assistance standard) crée un objet et que cet objet reçoit ensuite des privilèges plus élevés – de niveau administrateur, par exemple. Le

propriétaire d'origine demeure et peut désormais compromettre l'objet possédant ces nouveaux privilèges pour en profiter.

Remédiation

Si le principal de sécurité source n'est pas un propriétaire légitime de l'objet cible, vous devez le modifier.

Pour changer le propriétaire de l'objet cible :

1. Dans « Utilisateurs et ordinateurs Active Directory », cliquez avec le bouton droit sur **Propriétés** > **Sécurité** > **Avancé**.
2. Sur la ligne **Propriétaire** en haut, cliquez sur **Modifier**.

Les propriétaires d'objets cible sûrs, utilisés par défaut pour les objets Active Directory les plus sensibles, sont :

- Objets dans la partition Domaine : « Administrateurs » ou « Administrateurs de domaine »
- Objets dans la partition Configuration : « Administrateurs d'entreprise »
- Objets dans la partition Schéma : « Administrateurs de schéma »

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite

- Hérite de GPO
- GPO liée
- Membre de
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Réinitialiser mot de passe

Description

Le principal de sécurité source peut réinitialiser le mot de passe de la cible, ce qui lui permet de s'authentifier en tant que cible à l'aide du nouveau mot de passe attribué et de bénéficier des privilèges de la cible.

La réinitialisation d'un mot de passe n'est pas la même opération qu'un changement de mot de passe, ce que toute personne connaissant le mot de passe actuel peut réaliser. Un changement de mot de passe se produit généralement lorsqu'un mot de passe expire.

Exploitation

Les attaquants qui compromettent le principal de sécurité de la source peuvent réinitialiser le mot de passe de la cible à l'aide de commandes Windows natives telles que « net user /domain », de commandes PowerShell telles que « Set-ADAccountPassword -Reset », d'outils d'administration tels que « Utilisateurs et ordinateurs Active Directory » ou d'outils de piratage dédiés tels que PowerSploit.

Il suffit alors aux attaquants de s'authentifier dans Active Directory ou la ressource ciblée en utilisant des méthodes d'authentification légitimes avec leur nouveau mot de passe pour usurper entièrement l'identité de la cible.

Mais la plupart du temps, les attaquants ne connaissent pas le mot de passe précédent et ne peuvent pas le rétablir après l'attaque. Par conséquent, l'attaque est souvent visible pour la

personne légitime qui se trouve derrière la cible et peut même provoquer un déni de service, en particulier dans le cas des comptes de service.

Remédiation

Les administrateurs informatiques et le personnel du service d'assistance sont légitimement autorisés à réinitialiser les mots de passe. Mais vous devez mettre en place les délégations appropriées pour leur permettre d'effectuer cette action uniquement dans leur périmètre autorisé.

De plus, selon le modèle de hiérarchisation, vous devez vous assurer qu'un opérateur de niveau inférieur, comme un technicien du service d'assistance des utilisateurs standard, ne peut pas réinitialiser le mot de passe d'un compte de niveau supérieur, tel que celui d'un administrateur de domaine, car il y existe un risque d'élévation des privilèges.

Pour modifier le descripteur de sécurité de la cible et supprimer les autorisations illégitimes :

1. Dans « Utilisateurs et ordinateurs Active Directory », cliquez avec le bouton droit sur Propriétés > Sécurité.
2. Supprimez l'autorisation « Réinitialiser le mot de passe » du principal de sécurité source.

   > **Remarque** : ne confondez pas cette autorisation avec « Modifier le mot de passe ».

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID

- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Gestion RODC
- Modifier DACL
- Modifier propriétaire

Gestion RODC

Description

Le principal de sécurité source se trouve dans l'attribut « ManagedBy » du contrôleur de domaine cible en lecture seule (RODC), ce qui signifie que la source dispose de droits d'administration sur le contrôleur RODC cible.

> **Remarque** : d'autres types d'objets Active Directory utilisent le même attribut « ManagedBy » à titre d'information uniquement, et ne donnent aucun droit administratif au gestionnaire déclaré. Par conséquent, cette relation n'existe que pour les nœuds cibles de type RODC.

Les contrôleurs RODC sont moins sensibles que les contrôleurs de domaine inscriptibles plus courants, mais ils restent une cible important pour les attaquants, car ils peuvent voler les identifiants des contrôleurs RODC pour leur permettre d'accéder à d'autres systèmes. Cela dépend du niveau de durcissement de la configuration du contrôleur RODC ; par exemple, du nombre d'objets avec des secrets qu'il peut synchroniser.

Exploitation

La méthode d'exploitation est identique à celle de la relation « AdminTo ».

Les attaquants qui compromettent le principal de sécurité source peuvent utiliser son identité pour se connecter à distance et exécuter des commandes sur le contrôleur RODC cible avec des droits d'administration. Ils peuvent exploiter les protocoles natifs disponibles tels que Server

Message Block (SMB) avec partages administratifs, Remote Desktop Protocol (RDP), Windows Management Instrumentation (WMI), Remote Procedure Call (RPC), Windows Remote Management (WinRM), etc.

Les attaquants peuvent utiliser des outils natifs d'administration à distance tels que PsExec, des services, des tâches planifiées, Invoke-Command, etc., ou des outils de piratage spécialisés tels que wmiexec, smbexec, Invoke-DCOM, SharpRDP, etc.

L'objectif final de l'attaque peut être soit de compromettre le RODC cible, soit d'utiliser des outils de récupération des informations d'identification tels que mimikatz pour obtenir davantage d'identifiants et de secrets et ainsi accéder à d'autres machines.

Remédiation

Si le principal de sécurité source n'est pas un administrateur légitime du contrôleur RODC cible, vous devez le remplacer par un administrateur approprié.

Notez que les administrateurs de domaine n'administrent généralement pas les contrôleurs RODC, d'où le paramètre dédié « géré par ». En effet, les contrôleurs RODC ont un niveau d'approbation inférieur, et les administrateurs de domaine à privilèges élevés ne doivent pas exposer leurs identifiants en s'authentifiant dessus.

Par conséquent, vous devez sélectionner un administrateur de « niveau intermédiaire » approprié pour les RODC, conformément à vos règles RODC Active Directory ; par exemple, l'administrateur informatique de la succursale locale où ils se trouvent.

Pour modifier l'attribut « ManagedBy » :

1. Dans « Utilisateurs et ordinateurs Active Directory », sélectionnez l'onglet RODC > **Propriétés** > « **ManagedBy** ».
2. Cliquez sur **Modifier**.

Vous pouvez également exécuter la commande suivante dans PowerShell :

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Modifier DACL
- Modifier propriétaire

Modifier DACL

Description

Le principal de sécurité source est autorisé à modifier les autorisations de l'objet cible dans la liste des contrôles d'accès (DACL). Ainsi, la source peut obtenir des droits supplémentaires pour elle-même ou quelqu'un d'autre, et compromettre l'objet cible.

Exploitation

Il suffit aux attaquants qui compromettent le principal de sécurité source de modifier le descripteur de sécurité de l'objet cible à l'aide de commandes Windows natives telles que « dsacls », de

commandes PowerShell telles que « Set-ACL », d'outils d'administration tels que « Utilisateurs et ordinateurs Active Directory » ou d'outils de piratage spécialisés tels que PowerSploit.

Remédiation

Si le principal de sécurité source n'a pas l'autorisation légitime de modifier les autorisations de l'objet cible, vous devez supprimer cette autorisation.

Pour modifier le descripteur de sécurité de l'objet cible :

1. Dans « Utilisateurs et ordinateurs Active Directory », cliquez avec le bouton droit sur l'objet, puis sélectionnez **Propriétés** > **Sécurité** > **Avancé**.
2. Supprimez l'autorisation « Modifier les autorisations » du principal de sécurité source.

Remarque : un objet peut hériter de cette autorisation d'un objet situé plus haut dans l'arborescence Active Directory.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de

- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier propriétaire

Modifier propriétaire

Description

Le principal de sécurité source est autorisé à modifier le propriétaire de l'objet cible, et peut se désigner lui-même comme propriétaire. Les propriétaires ont des droits implicites (« Contrôle en lecture » et « Modifier DACL ») qui leur permettent d'obtenir des droits supplémentaires, pour eux-mêmes ou pour quelqu'un d'autre, et donc de compromettre l'objet cible.

Pour plus d'informations, voir la relation Détient.

Exploitation

Les attaquants qui compromettent le principal de sécurité source peuvent se désigner comme propriétaire de la cible en utilisant des commandes Windows natives telles que « dsacls/takeownership », des commandes PowerShell telles que « Set-ACL », des outils d'administration tels que « Utilisateurs et ordinateurs Active Directory » ou des outils de piratage spécialisés tels que PowerSploit.

Ils peuvent ensuite modifier le descripteur de sécurité de l'objet cible en utilisant des méthodes similaires.

Remédiation

Si le principal de sécurité source n'a pas l'autorisation légitime de modifier le propriétaire de l'objet cible, vous devez supprimer cette autorisation.

Pour modifier le descripteur de sécurité de l'objet cible :

1. Dans « Utilisateurs et ordinateurs Active Directory », cliquez avec le bouton droit sur l'objet, puis sélectionnez **Propriétés** > **Sécurité** > **Avancé**.
2. Supprimez l'autorisation « Modifier le propriétaire » du principal de sécurité source.

Remarque : un objet peut hériter de cette autorisation d'un objet situé plus haut dans l'arborescence Active Directory.

Voir aussi

- Ajouter des identifiants de clé
- Ajouter un membre
- Autorisé à agir
- Autorisé à déléguer
- Appartient à la GPO
- DCSync
- Attribuer autorisé à agir
- A un historique SID
- Prise de contrôle implicite
- Hérite de GPO
- GPO liée
- Membre de
- Détient
- Réinitialiser mot de passe
- Gestion RODC
- Modifier DACL

Identification des assets Tier 0

Les assets Tier 0 incluent des comptes, des groupes et d'autres assets qui ont un contrôle administratif direct ou indirect sur les forêts et les domaines Active Directory.

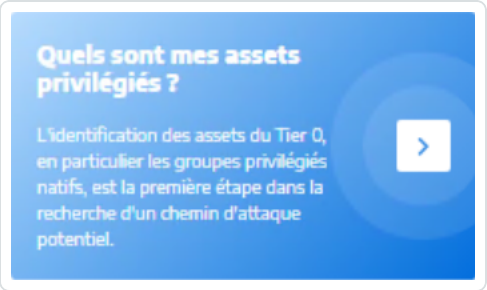
Tenable Identity Exposure répertorie vos assets et vos comptes Tier 0 avec les chemins d'attaque potentiels menant à l'asset.

Pour afficher la liste des assets Tier 0 :

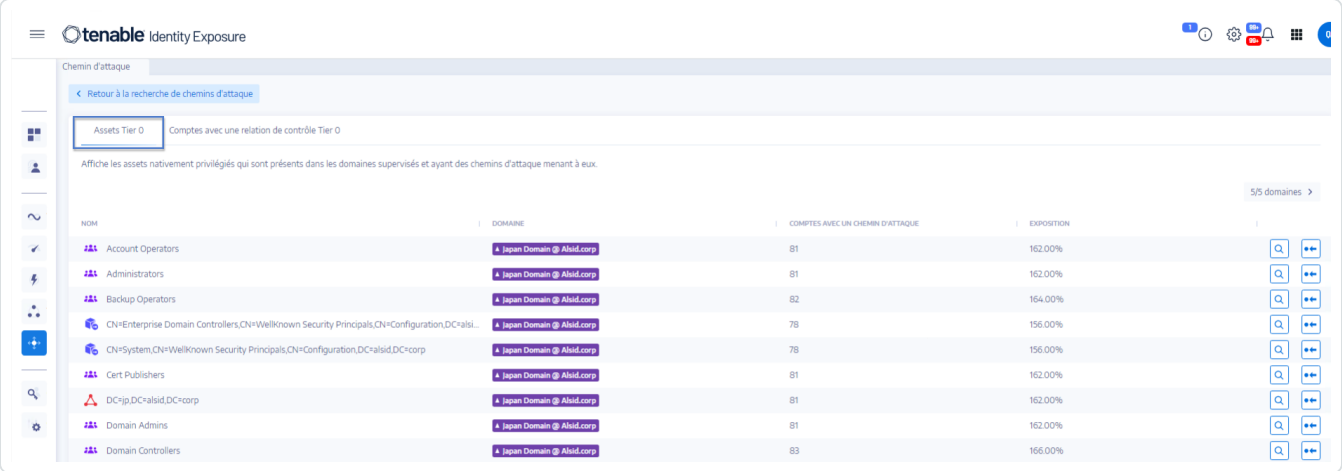
1. Dans Tenable Identity Exposure, cliquez sur l'icône de chemin d'attaque dans la barre de navigation de gauche.

   Le volet **Chemin d'attaque** apparaît.

2. Cliquez sur le titre « **Quels sont mes assets privilégiés ?** ».

   Tenable Identity Exposure affiche la liste des assets Tier 0 dans votre infrastructure AD.

   Chaque ligne indique le **nom de l'asset**, son **domaine** et les informations suivantes :

   - **Comptes avec chemin d'attaque** : nombre d'assets dont un chemin d'attaque mène à l'asset Tier 0.
   - **Exposition** : comptes dont un chemin d'attaque mène à l'asset Tier 0, en pourcentage du nombre total de comptes du domaine.

Pour filtrer les assets d'un domaine :

1. Cliquez sur le bouton **n/n**.

   Le volet **Forêts et domaines** apparaît. Vous pouvez procéder de deux manières :

   - Dans la zone de **recherche**, saisissez le nom d'une forêt ou d'un domaine.
   - Cochez la case **Tout développer** et sélectionnez la forêt ou le domaine souhaités.

2. Cliquez sur **Filtrer sur la sélection**.

   Tenable Identity Exposure met à jour la liste des assets.

Pour établir la liste des comptes dont les chemins d'attaque mènent à l'asset Tier 0 :

- À la fin de la ligne du nom de l'asset Tier 0, cliquez sur l'icône .

  Tenable Identity Exposure affiche la liste des comptes dont les chemins d'attaque mènent à l'asset Tier 0 :

Pour voir l'exposition de l'asset Tier 0 :

- À la fin de la ligne du nom de l'asset Tier 0, cliquez sur l'icône .

  Tenable Identity Exposure ouvre la page Exposition d'un asset pour l'asset Tier 0. Pour plus d'informations, voir Relations d'attaque.

Comptes avec des chemins d'attaque

Tenable Identity Exposure affiche les comptes ayant des chemins d'attaque menant aux assets Tier 0 pour vous donner une vue complète d'une menace de sécurité potentielle, car les comptes utilisateur et machine peuvent recevoir des privilèges supplémentaires par le biais de diverses relations d'attaque.

Pour plus d'informations, voir Identification des assets Tier 0.

Pour afficher les assets ayant des chemins d'attaque :

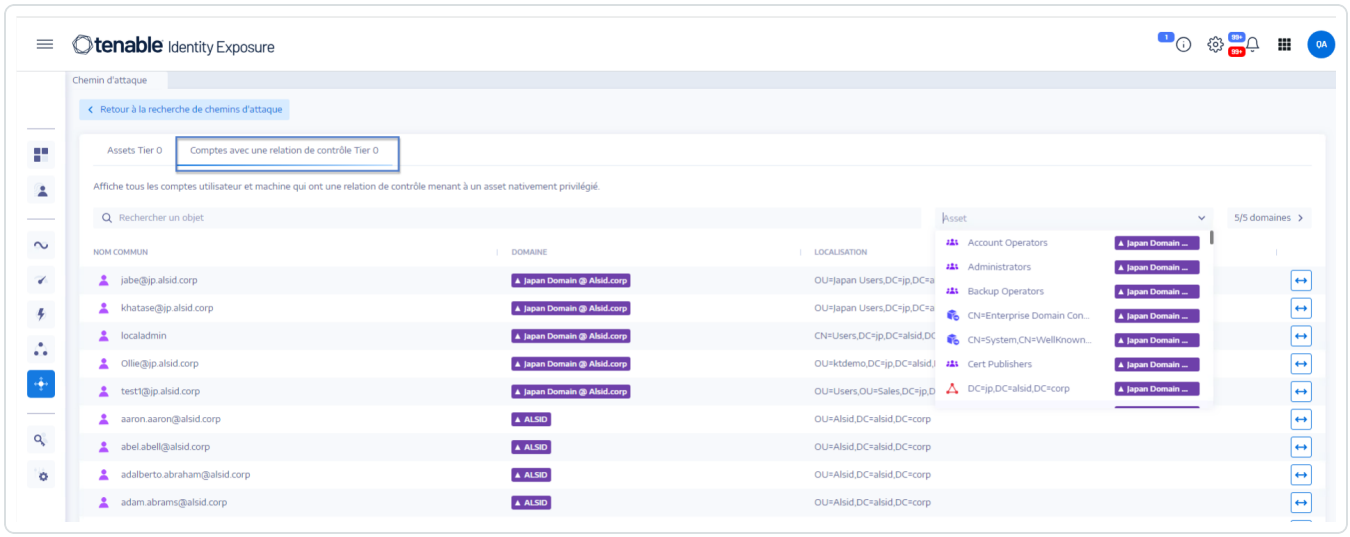
1. Dans Tenable Identity Exposure, cliquez sur l'icône de chemin d'attaque  dans la barre de navigation de gauche.

   Le volet **Chemin d'attaque** apparaît.

2. Cliquez sur la tuile « **Qui a un contrôle sur mes assets privilégiés ?** ».



Tenable Identity Exposure affiche tous les comptes utilisateur et machine ayant un chemin d'attaque menant à un asset Tier 0.



Pour rechercher un asset :

1. Dans la zone de **recherche**, saisissez le nom de l'asset.
2. Dans la zone **Asset**, cliquez sur la flèche **>** pour afficher la liste déroulante des assets Tier 0 et sélectionnez-en un.

   Tenable Identity Exposure met à jour la liste avec les résultats correspondants.

Pour filtrer les assets d'un domaine :

1. Cliquez sur le bouton **n/n**.

   Le volet **Forêts et domaines** apparaît. Vous pouvez procéder de deux manières :

- Dans la zone de **recherche**, saisissez le nom d'une forêt ou d'un domaine.
- Cochez la case **Tout développer** et sélectionnez la forêt ou le domaine souhaités.

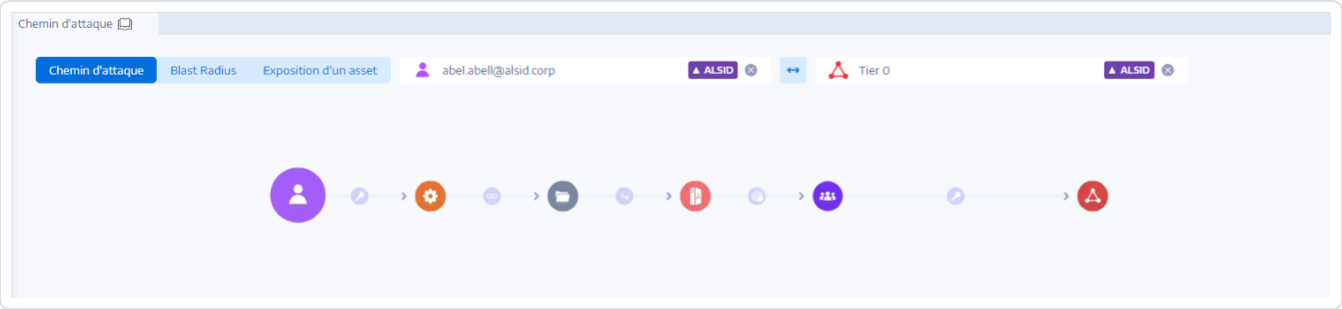
2. Cliquez sur **Filtrer sur la sélection**.

   Tenable Identity Exposure met à jour la liste des assets.

Pour explorer le chemin d'attaque :

- À la fin de la ligne du nom de l'asset, cliquez sur l'icône ↔.

  Tenable Identity Exposure ouvre la page Chemin d'attaque de l'asset sur tous les assets Tier 0. Pour plus d'informations, voir Chemin d'attaque et Relations d'attaque



Types de nœuds du chemin d'attaque

La fonctionnalité de chemin d'attaque dans Tenable Identity Exposure affiche un graphe indiquant les chemins d'attaque accessibles aux attaquants au sein de votre environnement Active Directory. Le graphe comprend des **arêtes** qui représentent des relations d'attaque, ainsi que des **nœuds** qui représentent des objets Active Directory (LDAP/SYSVOL).

La liste suivante décrit tous les types de nœuds que vous pouvez rencontrer dans les graphes de chemins d'attaque.

Type de nœud	Localisation	Icône	Description
Utilisateur	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `user` mais pas `computer`.

Groupe	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `group`.
Appareil	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `computer` mais pas `msDS-GroupManagedServiceAccount`. Son attribut `primaryGroupID` n'est pas égal à 516 (DC) ou 521 (RODC). **Remarque** : pour différencier les produits Tenable, cette catégorie est appelée « Appareil » au lieu de « Ordinateur », afin d'être plus générique.
Unité d'organisation (UO)	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `organizationalUnit`. Évitez de confondre les objets de la classe `container` et le fait que tout objet Active Directory (AD) puisse servir de conteneur, ce qui lui permet de contenir d'autres objets.
Domaine	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `domainDNS` et certains attributs.
Contrôleur de domaine (DC)	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `computer` et l'attribut `primaryGroupID` est égal à 516 (il ne s'agit donc pas d'un RODC).
Contrôleur de domaine en lecture seule (RODC)	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `computer` et l'attribut `primaryGroupID` est égal à 521 (il ne s'agit donc pas d'un DC normal).
Stratégie de groupe (GPC)	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `groupPolicyContainer`.

Fichier de GPO	SYSVOL		Fichier trouvé dans le partage SYSVOL d'une GPO spécifique (par exemple « `\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml` »)
Dossier de GPO	SYSVOL		Dossier trouvé dans le partage SYSVOL d'une GPO spécifique. Il y en a un pour chaque GPO (par exemple « `\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup` »)
Compte de service géré par groupe (gMSA)	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `msDS-GroupManagedServiceAccount`.
Magasin Enterprise NtAuth	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `certificationAuthority`.
Modèle de certificat de PKI	LDAP		Objet LDAP dont l'attribut `objectClass` contient la classe `pKICertificateTemplate`.
Principal de sécurité non résolu	LDAP		Objet LDAP dont l'attribut `objectSid` ou `DistinguishedName` est utilisé à un moment donné lors de la création de relations, mais pour lequel il existe un objet principal de sécurité LDAP correspondant inconnu (cas classique de « SID non résolu »). Il manque également des informations sur le type spécifique de principal de sécurité (Utilisateur, Ordinateur, Groupe, etc.) qui lui est associé ; seul son SID/DN est connu.

Identité spéciale	LDAP		Windows et Active Directory utilisent des identités bien connues en interne. Ces identités fonctionnent de manière similaire aux groupes, mais AD ne les déclare pas comme telles. Pour plus d'informations, voir Groupes d'identités spéciales.
Autres			Actuellement, tous les objets AD/SYSVOL qui ne correspondent pas aux catégories mentionnées.

Journaux d'activité

Les journaux d'activité de Tenable Identity Exposure permettent de visualiser les traces de toutes les activités qui se sont produites sur la plateforme Tenable Identity Exposure, liées à des adresses IP, des utilisateurs ou des actions spécifiques.

Remarque : en raison de limitations techniques, les journaux d'activités concernant des vues spécifiques, telles que la gestion des tenants (ajout, modification ou suppression), ne sont pas visibles actuellement.

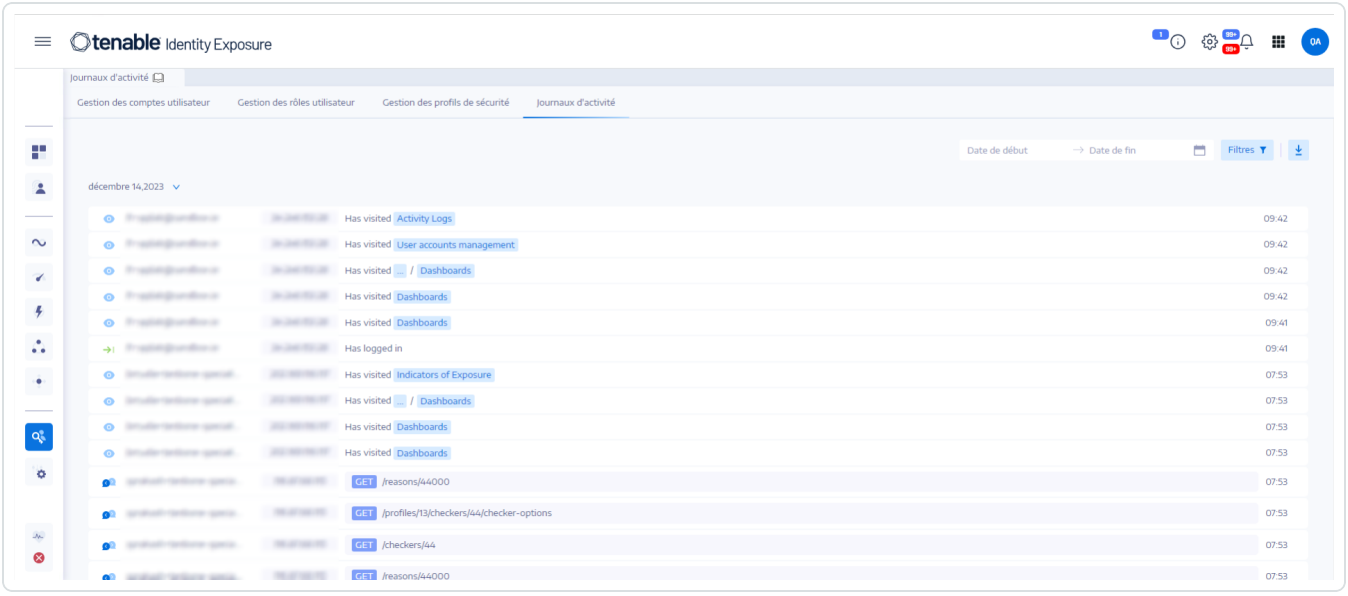
Pour afficher les journaux d'activités :

1. Dans Tenable Identity Exposure, cliquez sur l'icône **Comptes** dans le menu de navigation de gauche.

   Le volet **Gestion des comptes utilisateur** apparaît.

2. Sélectionnez l'onglet **Journaux d'activités**.

   Le volet Journaux d'activité apparaît.

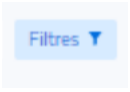


Pour afficher les journaux d'activité d'une période donnée :

1. En haut du volet du journal d'activités, cliquez sur le sélecteur de date.
2. Sélectionnez la date de début et la date de fin de la période souhaitée.
3. (Facultatif) Utilisez la barre de défilement pour sélectionner l'heure (par défaut : l'heure actuelle)
4. Cliquez sur **OK**.

   Tenable Identity Exposure affiche le journal d'activités de la période.

Pour filtrer les journaux d'activités :

1. En haut du volet des journaux d'activités, cliquez sur le bouton 

.

   Le volet **Filtres** apparaît.
2. Cliquez sur > dans les zones suivantes :
   - Adresse IP
   - Utilisateur
   - Action

3. Cliquez sur **Valider**.

   Tenable Identity Exposure affiche le journal d'activités correspondant au filtre que vous avez défini.

Pour supprimer des filtres :

- Au bas du volet **Filtres**, cliquez sur **Supprimer les filtres**.

  Tenable Identity Exposure affiche le journal d'activités non filtré.

Pour exporter les journaux d'activités :

- En haut du volet des journaux d'activités, cliquez sur l'icône .

  Tenable Identity Exposure télécharge le journal d'activité au format CSV sur votre ordinateur.

Définitions des entités privilégiées

Tenable Identity Exposure utilise le concept d'entités « **privilégiées** » dans divers indicateurs d'exposition, indicateurs d'attaque et autres fonctionnalités. La définition des entités privilégiées diffère entre Active Directory et Entra ID :

Active Directory

Les entités privilégiées peuvent englober les **utilisateurs privilégiés**, les **comptes d'ordinateur privilégiés**, les **comptes de service privilégiés**, les **groupes privilégiés**, les **principaux de sécurité privilégiés**, etc. Les entités privilégiées incluent l'utilisateur du système (local), les utilisateurs KRBTGT (ticket distributeur de tickets Kerberos) et tous les membres directs ou indirects (transitifs) des groupes avec les privilèges natifs suivants, identifiés en interne par leur RID/SID connu, quels que soient leurs noms.

- Opérateurs de compte
- Administrateurs
- Opérateurs de sauvegarde
- Éditeurs de certificats
- Administrateurs de domaine

- Contrôleurs de domaine
- Administrateurs d'entreprise
- Contrôleurs de domaine d'entreprise
- Administrateurs de clés d'entreprise
- Contrôleurs de domaine en lecture seule d'entreprise
- Propriétaires-créateurs de stratégies de groupe
- Administrateurs de clés
- Opérateurs d'impression
- Contrôleurs de domaine en lecture seule
- Réplicateurs
- Administrateurs de schéma
- Opérateurs de serveurs

Entra ID

- Un **droit** ou une **autorisation privilégiés** sont identifiés comme tels par Microsoft.
- Un **rôle privilégié** est un rôle Entra contenant au moins une autorisation privilégiée telle que définie par Microsoft.
- Les **entités privilégiées** (utilisateurs, groupes ou principaux de service) sont celles qui sont attribuées directement ou indirectement (de manière transitive via un groupe auquel peut être attribué un rôle) à un rôle Entra privilégié.

Configuration et administration de Tenable Identity Exposure

Les options et fonctionnalités décrites dans cette section sont destinées aux administrateurs et aux utilisateurs avancés qui cherchent à personnaliser, optimiser et maintenir leur installation ou leur déploiement de Tenable Identity Exposure.

Vous y trouverez des instructions spécialisées sur des sujets tels que la gestion d'Active Directory, la configuration du déploiement des indicateurs d'attaque, les paramètres d'authentification, les comptes utilisateur, les profils de sécurité, les rôles, les forêts, les domaines et les alertes. Cette section couvre également l'exécution des vérifications de l'état du système, l'utilisation du Centre de rapports, l'intégration avec Microsoft Entra ID (anciennement Azure AD), la gestion des licences et la résolution des problèmes.

Pour trouver des informations relatives à une tâche spécifique, cliquez sur les rubriques correspondantes dans le volet de menu sur le côté gauche de l'écran.

Autorisation : ces tâches nécessitent des privilèges d'accès administrateur.

Activation de la prise en charge de « Identités 360 », « Centre d'exposition » et « Microsoft Entra ID »

Pour activer la prise en charge de **Identités 360**, **Centre d'exposition** et **Microsoft Entra ID** :

Remarque : pour activer ces fonctionnalités, l'utilisateur de Tenable Cloud ayant créé les clés d'accès et secrètes doit disposer d'autorisations administrateur dans le conteneur Tenable Cloud référencé par la licence Tenable Identity Exposure. Pour plus d'informations, voir Licences Tenable Identity Exposure.

1. Dans Tenable Identity Exposure, cliquez sur l'icône **Systèmes**  dans le menu de navigation de gauche.
2. Cliquez sur l'onglet **Configuration**.

   La page **Configuration** apparaît.
3. Sous Services de l'application, cliquez sur **Tenable Cloud**.
4. Dans **Activer la prise en charge de : « Identités 360 », « Centre d'exposition » et « Microsoft Entra ID »**, cliquez sur le curseur pour activer l'option.

5. Si vous ne vous êtes pas déjà connecté à Tenable Cloud, cliquez sur le lien pour accéder à la page de connexion :

    a. Cliquez sur **Mot de passe oublié ?** pour demander la réinitialisation du mot de passe.

    b. Saisissez l'adresse e-mail associée à votre licence Tenable Identity Exposure et cliquez sur **Demander la réinitialisation du mot de passe**.

    Tenable envoie un e-mail à cette adresse avec un lien pour réinitialiser votre mot de passe.

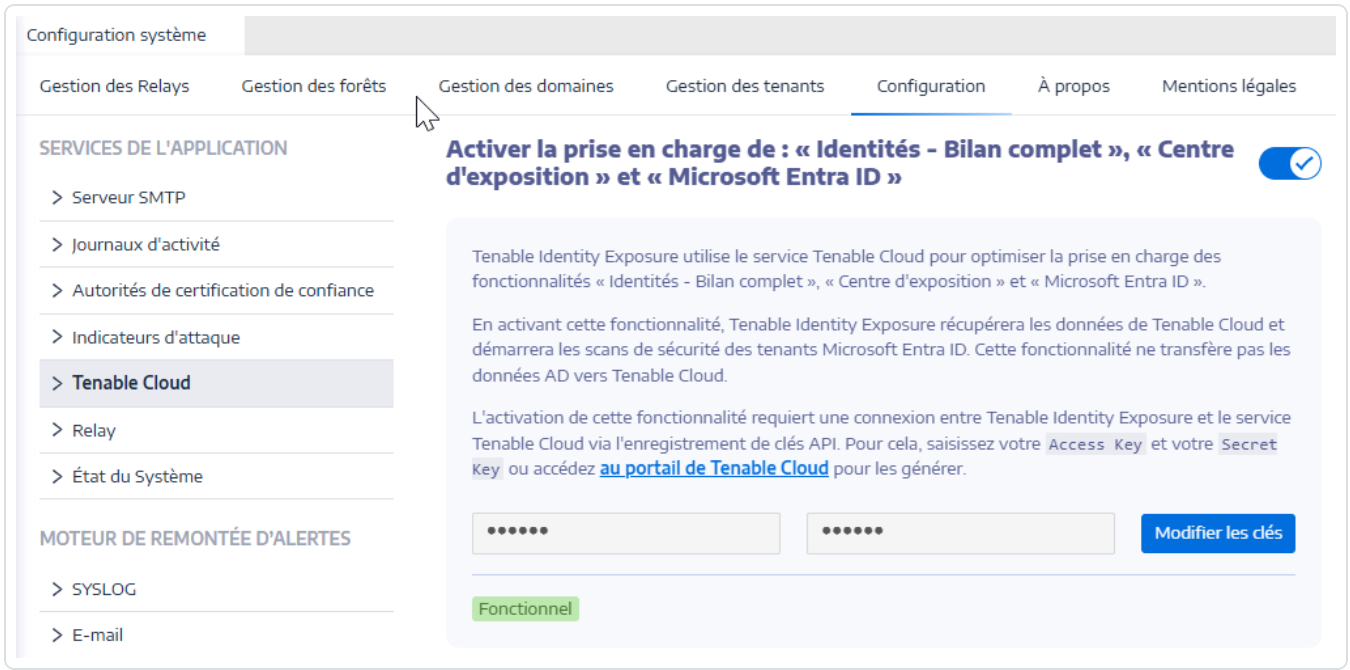
    > **Remarque** : si votre adresse e-mail n'est pas celle qui est associée à la licence Tenable Identity Exposure, contactez le support client pour obtenir de l'aide.

6. Connectez-vous à Tenable Vulnerability Management.

7. Pour générer des clés API dans Tenable Vulnerability Management, accédez à Tenable Vulnerability Management > **Paramètres** > **Mon compte** > **Clés API**.

8. Saisissez votre `clé d'accès` et votre `clé secrète` d'utilisateur « Administrateur » pour Tenable Vulnerability Management afin d'établir une connexion entre Tenable Identity Exposure et le service Tenable Cloud.

9. Cliquez sur **Modifier les clés** pour soumettre les clés API.



Tenable Identity Exposure affiche un message pour confirmer qu'il a mis à jour les clés API.

Attention : pour utiliser cette fonctionnalité, vous **ne devez pas** appliquer de filtrage d'adresses IP dans Tenable Vulnerability Management pour autoriser Tenable Identity Exposure à accéder aux API. Voir API Access Security (Sécurité de l'accès aux API) pour plus d'informations.

Configuration d'Active Directory

Tenable Identity Exposure nécessite une configuration dans l'infrastructure Active Directory surveillée pour permettre à certaines fonctionnalités de fonctionner :

- Accès aux objets ou conteneurs AD
- Accès pour l'analyse privilégiée
- Déploiement des indicateurs d'attaque

Accès aux objets ou conteneurs AD

Remarque : cette section s'applique uniquement à une licence Tenable Identity Exposure du module Indicateur d'exposition.

Tenable Identity Exposure ne nécessite pas de privilèges administratifs pour assurer sa surveillance de la sécurité.

Cette approche repose le fait que le compte utilisateur employé par Tenable Identity Exposure est capable de lire tous les objets Active Directory stockés dans un domaine (y compris les comptes utilisateur, les unités d'organisation, les groupes, etc.).

Par défaut, la plupart des objets ont un accès en lecture pour le groupe Utilisateurs de domaine que le compte de service Tenable Identity Exposure utilise. Cependant, vous devez configurer manuellement certains conteneurs pour autoriser l'accès en lecture pour le compte utilisateur Tenable Identity Exposure.

Le tableau suivant détaille les objets et conteneurs Active Directory qui nécessitent une configuration manuelle pour un accès en lecture sur chaque domaine que Tenable Identity Exposure doit surveiller.

Localisation du conteneur	Description
`CN=Objets supprimés,DC=<DOMAINE>,DC=<TLD>`	Conteneur qui héberge les objets supprimés.
`CN=Conteneur de paramètres de mot de passe,CN=Système, DC=<DOMAINE>,DC=<TLD>`	(Facultatif) Conteneur qui héberge les objets de paramètres de mot de passe.

Pour accorder l'accès aux objets et aux conteneurs AD :

- Dans la console PowerShell du contrôleur de domaine, exécutez les commandes suivantes pour accorder l'accès aux objets ou conteneurs Active Directory :

  Remarque : vous devez exécuter ces commandes sur chaque domaine surveillé par Tenable Identity Exposure.

  ```
  #Set Service Account $serviceAccount = "<SERVICE_ACCOUNT>" #Don't Edit after here $domain = Get-ADDomain @($domain.DeletedObjectsContainer, "CN=Password Settings Container,$($domain.SystemsContainer)") | ForEach-Object { & dsacls $_ /takeownership & dsacls $_ /g "$($serviceAccount):LCRP" /I:T }
  ```

  `<__SERVICE_ACCOUNT__>` désigne le compte de service utilisé par Tenable Identity Exposure.

Autrement, si PowerShell n'est pas disponible, vous pouvez également exécuter ces commandes pour chaque conteneur :

```
dsacls "<__CONTAINER__>" /takeownership
dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
```

Dans ces commandes :

- `<__CONTAINER__>` désigne le conteneur qui nécessite un accès.
- `<__SERVICE_ACCOUNT__>` désigne le compte de service que Tenable Identity Exposure utilise.

Accès pour l'analyse privilégiée

La fonctionnalité facultative Analyse privilégiée nécessite des privilèges administratifs. Vous devez attribuer des autorisations au compte de service que Tenable Identity Exposure utilise.

Pour plus d'informations, voir Analyse privilégiée.

Remarque : vous devez attribuer des autorisations sur chaque domaine où vous activez l'Analyse privilégiée.

Pour attribuer des autorisations à l'aide de la ligne de commande :

Exigence : pour attribuer des autorisations, vous devez utiliser un compte avec des droits d'administrateur de domaine ou l'équivalent.

- Dans l'interface de ligne de commande du contrôleur de domaine, exécutez la commande suivante pour ajouter les deux autorisations :

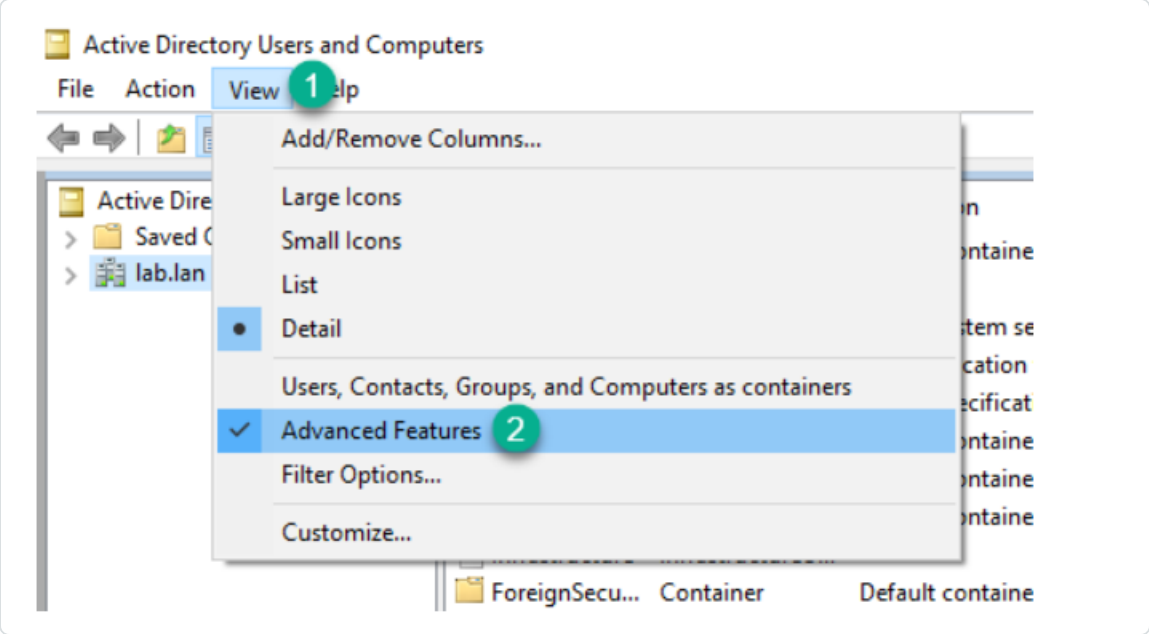
  ```
  dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
  SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
  ```

  Où :

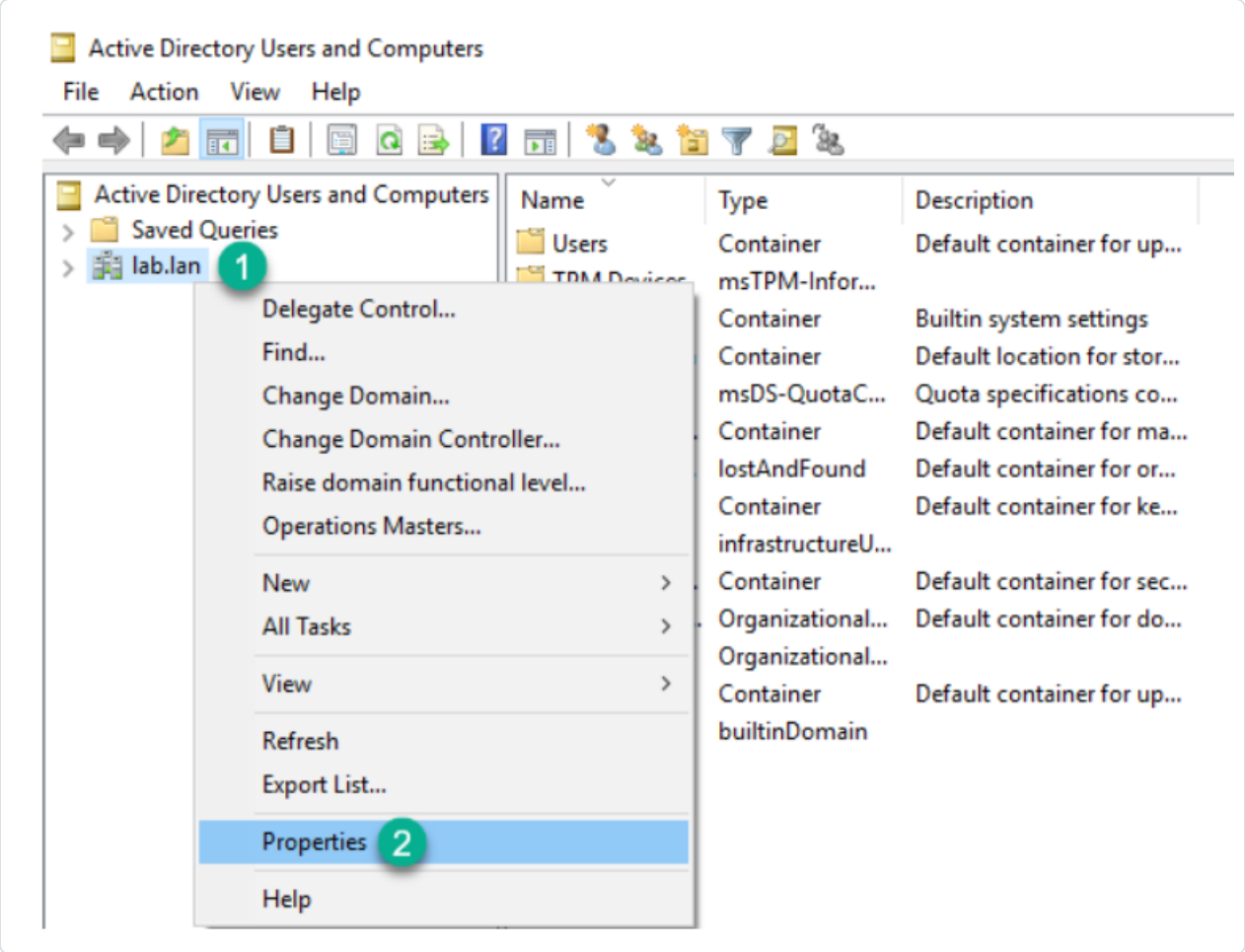
  - `<__DOMAIN_ROOT__>` fait référence au nom distinctif de la racine du domaine. Exemple : `DC=<DOMAIN>,DC=<TLD>`
  - `<__SERVICE_ACCOUNT__>` désigne le compte de service que Tenable Identity Exposure utilise. Exemple : `DOMAIN\tenablead`.

Pour attribuer des autorisations à l'aide de l'interface graphique :

1. Depuis le menu **Démarrer** de Windows, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Dans le menu **Affichage**, sélectionnez **Fonctions avancées**.

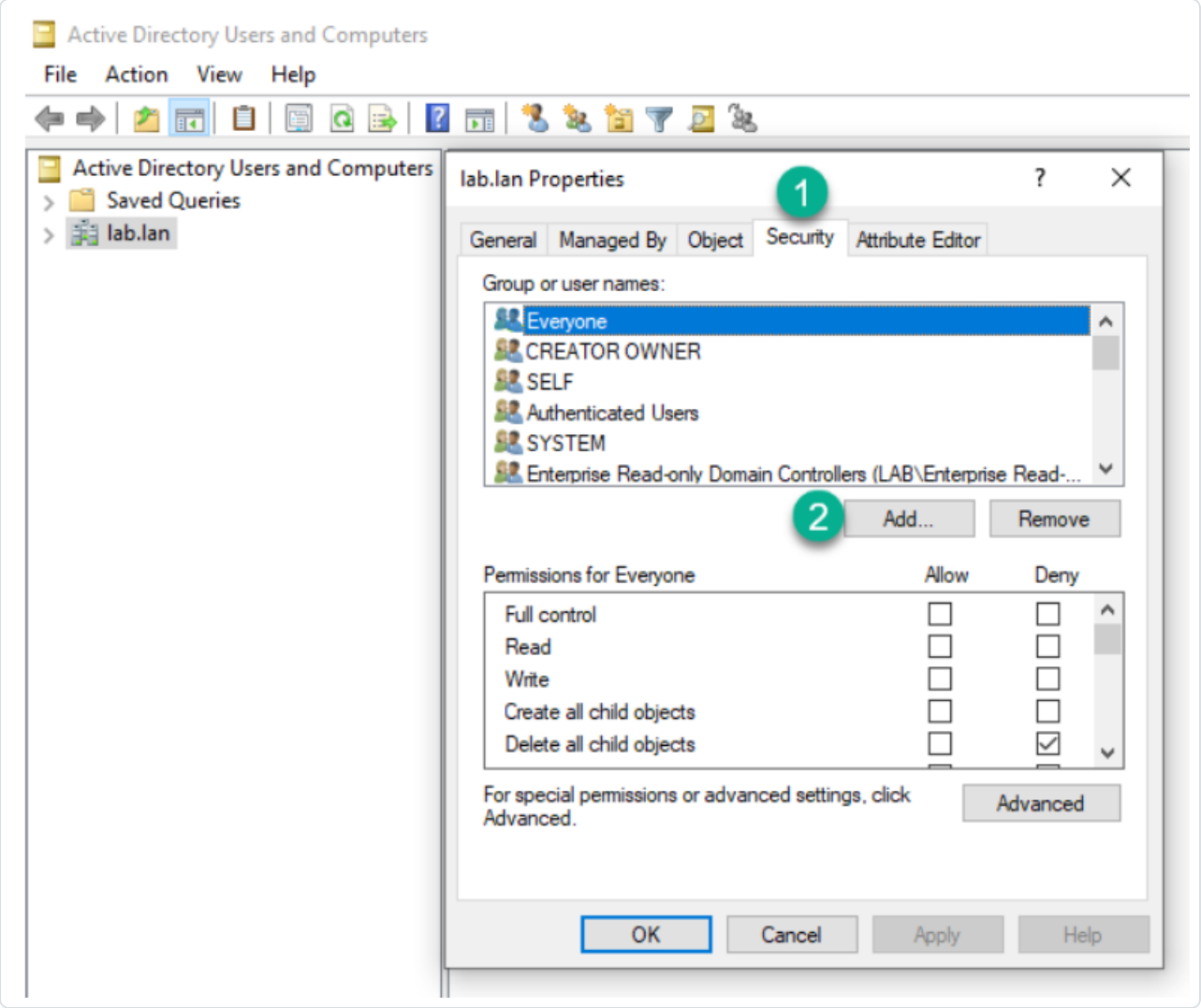


3. Cliquez avec le bouton droit sur la racine du domaine et sélectionnez **Propriétés**.



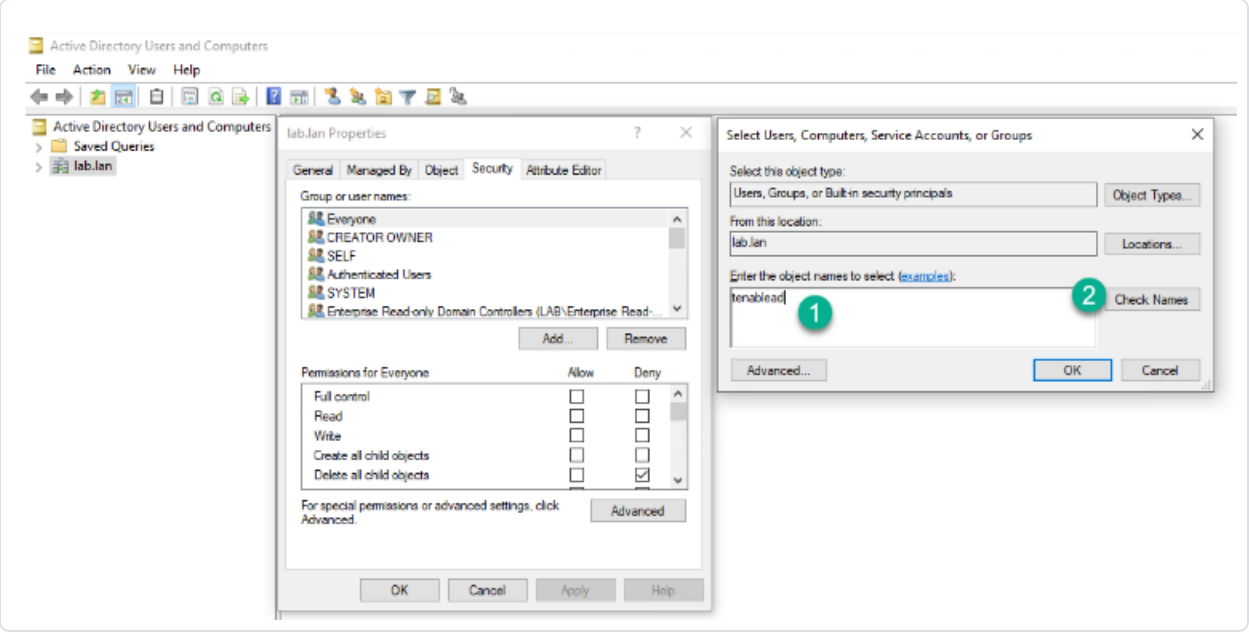
Le volet des propriétés de la racine du domaine apparaît.

4. Cliquez sur l'onglet **Sécurité** et sur **Ajouter**.

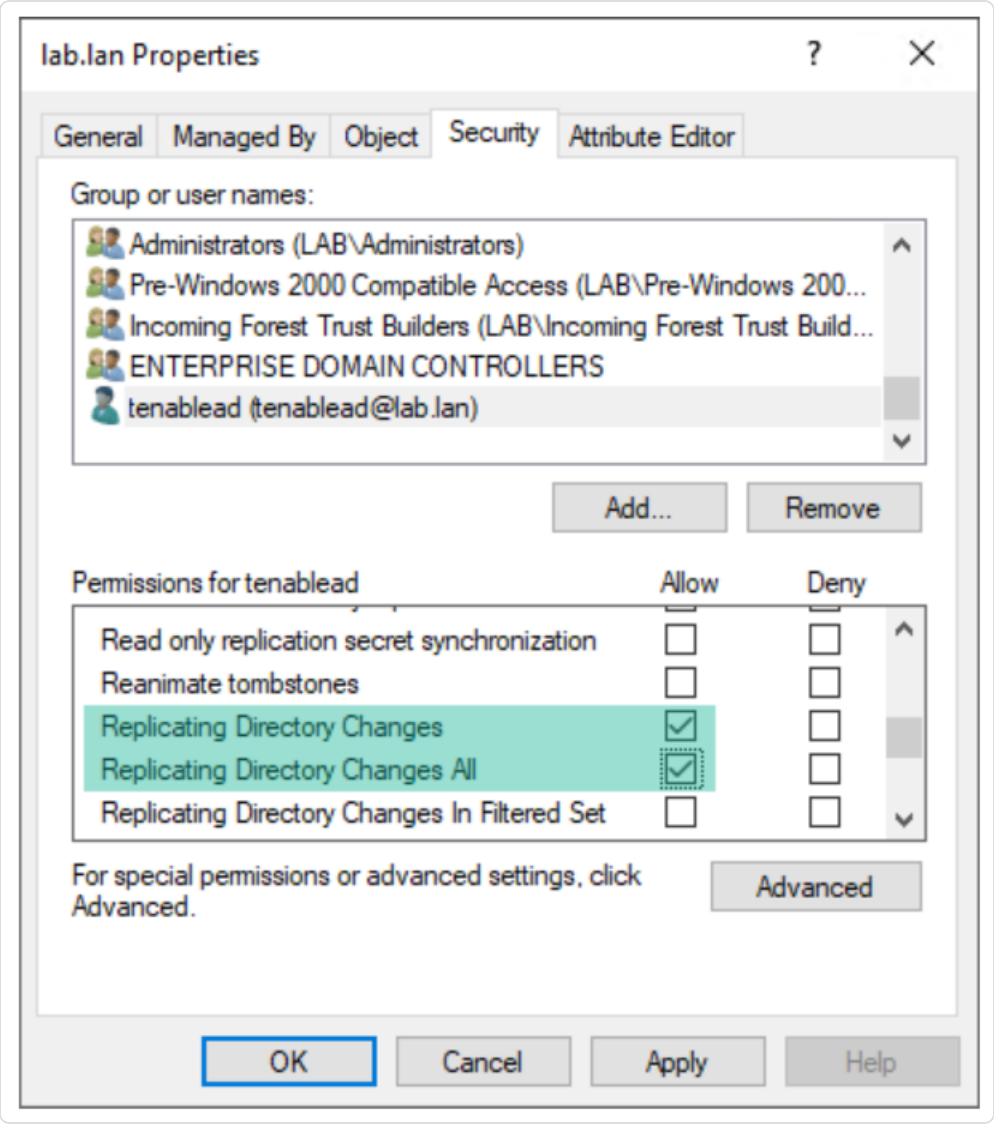


5. Localisez le compte de service Tenable Identity Exposure :

> **Remarque** : dans un environnement de forêt avec plusieurs domaines, le compte de service peut se trouver dans un domaine Active Directory différent.



6. Faites défiler la liste et désélectionnez toutes les autorisations définies par défaut.
7. Dans la colonne **Autoriser**, activez les autorisations *Réplication des modifications d'annuaire* et *Réplication de toutes les modifications de l'annuaire*.



8. Cliquez sur **OK**.

Remarques importantes

Tenable Identity Exposure ne nécessite qu'un seul compte de service par forêt. Par conséquent, lorsque vous attribuez des autorisations dans un domaine, il peut-être nécessaire de **rechercher le compte de service dans un autre domaine**.

Vous devez attribuer des autorisations supplémentaires **au niveau de la racine du domaine**.
Active Directory ne prend pas en charge les autorisations attribuées à une unité d'organisation ou à un utilisateur spécifique (par exemple, pour limiter l'analyse privilégiée à l'UO ou à l'utilisateur) et celles-ci n'ont donc aucun effet.

Ces autorisations confèrent au compte de service Tenable Identity Exposure beaucoup plus de pouvoir sur le domaine Active Directory. Vous devez alors le considérer comme un **compte privilégié (Tier 0)** et le protéger de la même manière qu'un compte d'administrateur de domaine. Pour la procédure complète, voir Protection des comptes de service.

Déploiement des indicateurs d'attaque

Remarque : ces informations ne concernent que les licences bénéficiant du module Indicateur d'attaque.

Les **indicateurs d'attaque** (IoA) de Tenable Identity Exposure permettent de détecter les attaques contre votre infrastructure Active Directory (AD). Chaque IoA nécessite des stratégies d'audit spécifiques que le script d'installation active automatiquement. Pour la liste complète des IoA Tenable Identity Exposure et savoir comment les implémenter, consultez le Guide de référence des indicateurs d'attaque Tenable Identity Exposure sur le portail des téléchargements Tenable.

Indicateurs d'attaque et Active Directory

Tenable Identity Exposure fonctionne de manière non intrusive et surveille une infrastructure Active Directory sans déployer d'agents, avec une modification de configuration minime de votre environnement.

Tenable Identity Exposure utilise un compte utilisateur standard sans autorisations administratives pour se connecter aux API standard et exécuter sa fonction de surveillance de la sécurité.

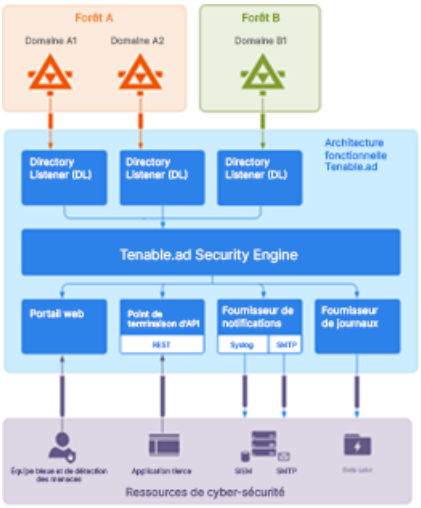
Tenable Identity Exposure utilise les mécanismes de réplication d'Active Directory pour récupérer les informations pertinentes, ce qui ne consomme que peu de bande passante entre le PDC de chaque domaine et le Directory Listener de Tenable Identity Exposure.

Pour détecter efficacement les incidents de sécurité à l'aide des indicateurs d'attaque, Tenable Identity Exposure utilise les informations de suivi des événements de Windows (ETW) et les mécanismes de réplication disponibles sur chaque contrôleur de domaine. Pour collecter ces informations, vous déployez une stratégie de groupe (GPO) dédiée à l'aide d'un script de Tenable Identity Exposure comme décrit dans Installer des indicateurs d'attaque.

Cette GPO active un observateur de journaux d'événements à l'aide des API Windows EvtSubscription dans tous les contrôleurs de domaine qui écrivent sur le volume système (SYSVOL) pour bénéficier du moteur de réplication AD et de la capacité de Tenable

Identity Exposure à écouter les événements SYSVOL. La GPO crée un fichier dans SYSVOL pour chaque contrôleur de domaine et vide son contenu régulièrement.

Pour lancer la surveillance de la sécurité, Tenable Identity Exposure doit contacter les API d'annuaire standard de Microsoft.



Contrôleur de domaine

Tenable Identity Exposure nécessite uniquement une communication avec l'émulateur de contrôleur de domaine principal (PDCe) à l'aide des protocoles réseau décrits dans la matrice de flux réseau.

Lorsque plusieurs domaines ou forêts sont surveillés, Tenable Identity Exposure doit atteindre le PDCe de chaque domaine. Pour optimiser les performances, Tenable recommande d'héberger Tenable Identity Exposure sur un réseau physique proche du PDCe à surveiller.

Compte utilisateur

Tenable Identity Exposure s'authentifie dans l'infrastructure surveillée à l'aide d'un compte utilisateur non-administrateur pour accéder au flux de réplication.

Un simple utilisateur Tenable Identity Exposure peut accéder à toutes les données collectées. Tenable Identity Exposure n'accède pas aux attributs secrets tels que les identifiants, les empreintes de mot de passe ou les clés Kerberos.

Tenable recommande de créer un compte de service membre du groupe « Utilisateurs de domaine » comme suit :

- Le compte de service doit se trouver dans le domaine surveillé principal.
- Le compte de service doit se trouver dans n'importe quelle unité d'organisation (UO), de préférence dans celle où vous créez d'autres comptes de service de sécurité.
- Le compte de service doit être un membre standard d'un groupe d'utilisateurs (par exemple, membre du groupe par défaut Utilisateurs de domaine AD).

Avant de commencer

- Vérifiez les limites et les impacts potentiels de l'installation des IoA, comme décrit dans Modifications techniques et impact potentiel.
- Vérifiez que les modules PowerShell pour Active Directory et GroupPolicy sont installés et disponibles sur le DC.

  Pour ce faire, exécutez la commande PowerShell suivante sur la machine cible (DC) où vous prévoyez de déployer le module IoA :

  ```
  if (-not (Get-Module -ListAvailable -Name GroupPolicy)) {
      Write-Error "The GroupPolicy module is not installed or not available on this machine. This
  is a requirement for this script and the IOAs to run, please install it and run this script
  again."
  }
  ```

  L'apparition d'une quelconque erreur dans votre console indique que cette exigence n'est pas validée dans votre environnement actuel.
- Vérifiez que la fonctionnalité RSAT-DFS-Mgmt-Con des outils de système de fichiers distribués est activée sur le DC, afin que le script de déploiement puisse vérifier le statut de la réplication, car il ne peut pas créer de GPO pendant que le DC est en cours de réplication.
- Tenable Identity Exposure recommande d'installer/mettre à niveau les IoA pendant les heures creuses pour limiter les interruptions de votre plateforme.
- Vérifier les autorisations – Pour installer des IoA, vous devez disposer d'un rôle utilisateur ayant les autorisations suivantes :

- Dans **Entités de type Données**, accès en « Lecture » à :
  - Tous les indicateurs d'attaque
  - Tous les domaines
- Dans **Entités de type Interface**, accès à :
  - Gestion > Système > Configuration
  - Gestion > Système > Configuration > Services de l'application > Indicateurs d'attaque
  - Gestion > Système > Configuration > Services de l'application > Indicateurs d'attaque > Télécharger le fichier d'installation

Pour plus d'informations sur les autorisations basées sur le rôle, voir Définir les autorisations d'un rôle.

Voir aussi

- Installer des indicateurs d'attaque
- Script d'installation des indicateurs d'attaque
- Modifications techniques et impact potentiel
- Programme d'installation de Microsoft Sysmon, un outil système Windows dont certains indicateurs d'attaque de Tenable Identity Exposure ont besoin pour obtenir des données système pertinentes.
- Dépanner les indicateurs d'attaque

Installer des indicateurs d'attaque

Rôle utilisateur requis : utilisateur d'organisation disposant des autorisations pour modifier la configuration des indicateurs d'attaqueTenable Identity Exposure. Pour plus d'informations, voir Définir les autorisations d'un rôle.

Le module Indicateurs d'attaque (IoA) de Tenable Identity Exposure nécessite d'exécuter un script d'installation PowerShell avec un compte d'administrateur capable de créer et de lier une nouvelle

stratégie de groupe (GPO) à une unité d'organisation (UO). Vous pouvez exécuter ce script à partir de n'importe quelle machine jointe à votre domaine Active Directory que Tenable Identity Exposure surveille et qui peut atteindre les contrôleurs de domaine via le réseau.

Remarque : vous devez redéployer le script d'installation des IoA à chaque nouvelle version majeure de Tenable Identity Exposure.

Remarque : la version recommandée de PowerShell est la version 5.1.

Vous n'avez à exécuter ce script d'installation qu'une seule fois pour chaque domaine AD, car la GPO nouvellement créée déploie automatiquement l'observateur d'événements sur tous les contrôleurs de domaine (DC) existants et nouveaux.

De plus, l'activation de l'option « Mises à jour automatiques » évite d'avoir à réexécuter le script d'installation, même si vous modifiez la configuration de l'IoA.

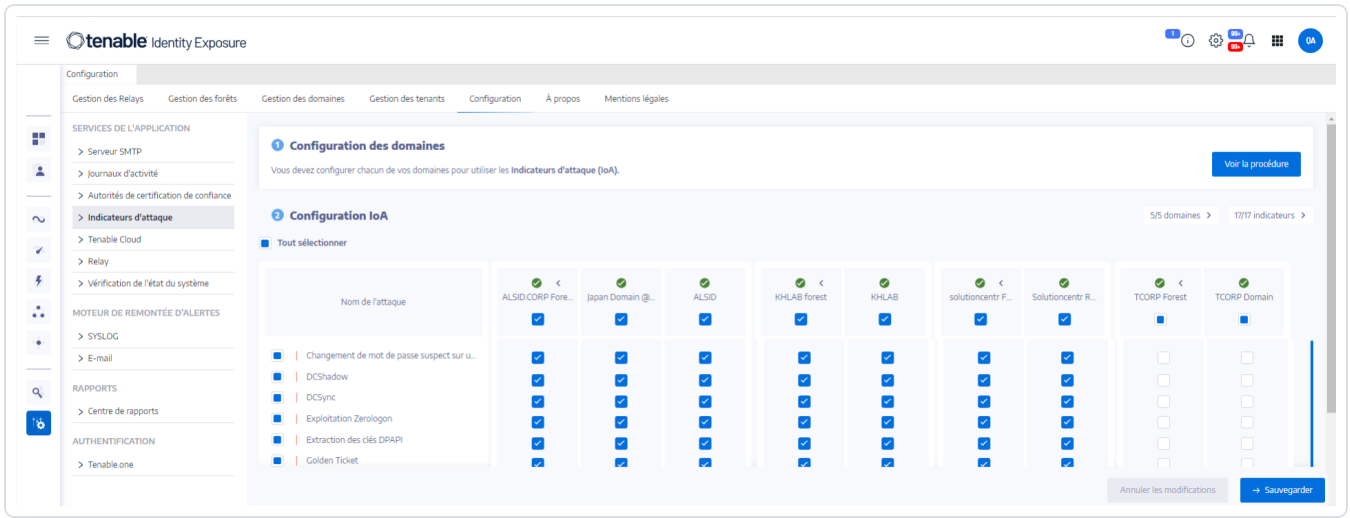
Pour configurer des domaines pour les IoA :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** dans la barre de menu de gauche et sélectionnez l'onglet **Configuration**.

   Le volet **Configuration** apparaît.

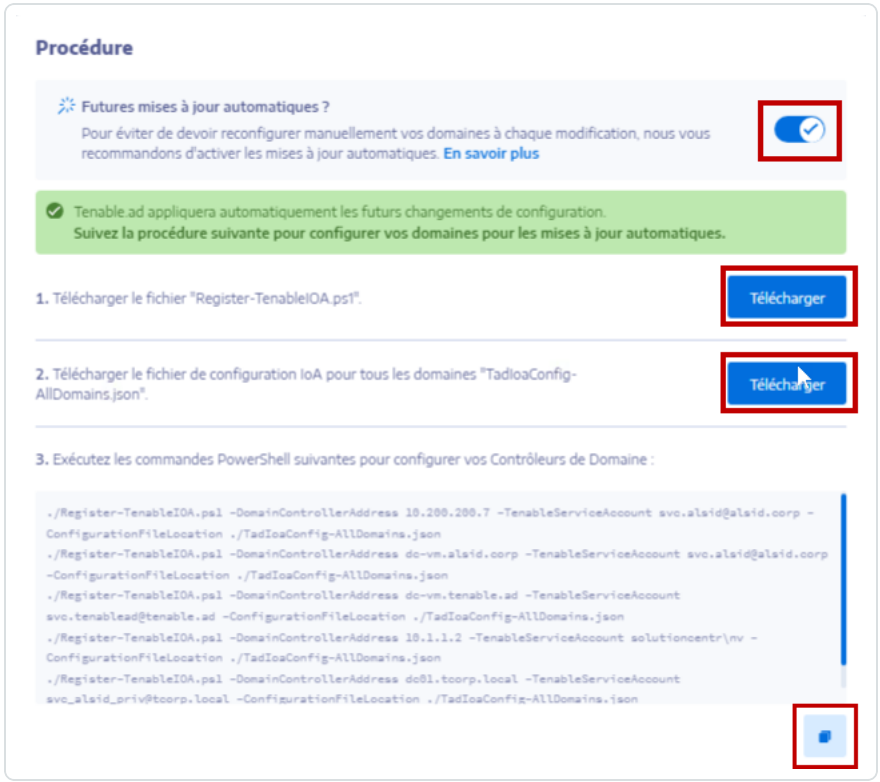
2. Cliquez sur **Indicateurs d'attaque**.

   Le volet de configuration IoA apparaît.



3. Dans **(1) Configuration des domaines**, cliquez sur **Voir la procédure**.

Une fenêtre de procédure apparaît.



4. Sous **Futures mises à jour automatiques ?** :
    - L'option par défaut **Activer** permet à Tenable Identity Exposure de mettre automatiquement à jour votre configuration IoA chaque fois que vous la modifiez dans Tenable Identity Exposure à l'avenir. Cela permet également d'analyser la sécurité en continu.
    - Si vous désactivez cette option, un message vous demande de l'activer pour obtenir les futures mises à jour automatiques. Cliquez sur **Voir la procédure** et cliquez sur le curseur pour le passer sur **Activer**.
5. Cliquez sur **Télécharger** pour télécharger le script à exécuter pour chaque domaine (`Register-TenableIOA.ps1`).
6. Cliquez sur **Télécharger** pour télécharger le fichier de configuration des domaines (`TadIoaConfig-AllDomains.json`).
7. Cliquez sur pour copier la commande Powershell permettant de configurer vos domaines.

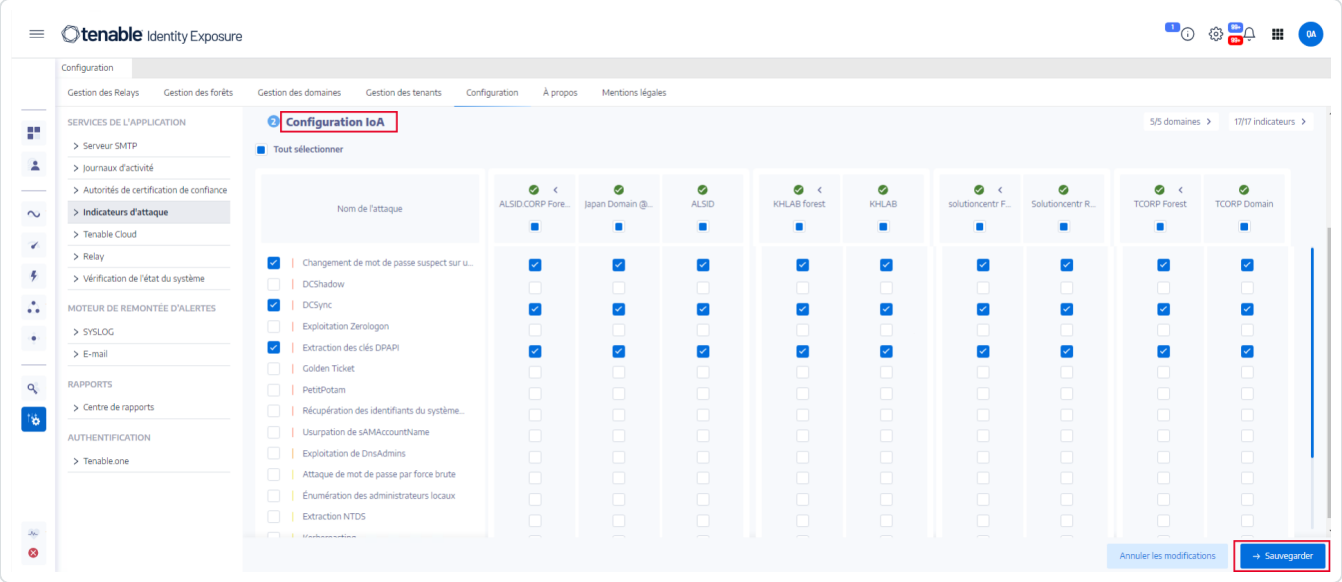
8. Cliquez en dehors de la fenêtre de procédure pour la fermer.

9. Ouvrez un terminal PowerShell avec des droits d'administration et exécutez les commandes pour configurer les contrôleurs de domaine pour les IoA.

> **Remarque** : le compte de service que vous utilisez pour installer les IoA et pour interroger les domaines doit disposer d'autorisations d'écriture dans le dossier GPO Tenable Identity Exposure (anciennement Tenable.ad). Le script d'installation ajoute cette autorisation automatiquement. Si vous supprimez cette autorisation, Tenable Identity Exposure affiche un message d'erreur, et les mises à jour automatiques ne fonctionnent plus. Pour plus d'informations, voir Script d'installation des indicateurs d'attaque.

Pour configurer vos IoA :

1. Dans le volet de configuration des IoA, sous **Configuration IoA**, sélectionnez les IoA à placer dans votre configuration.



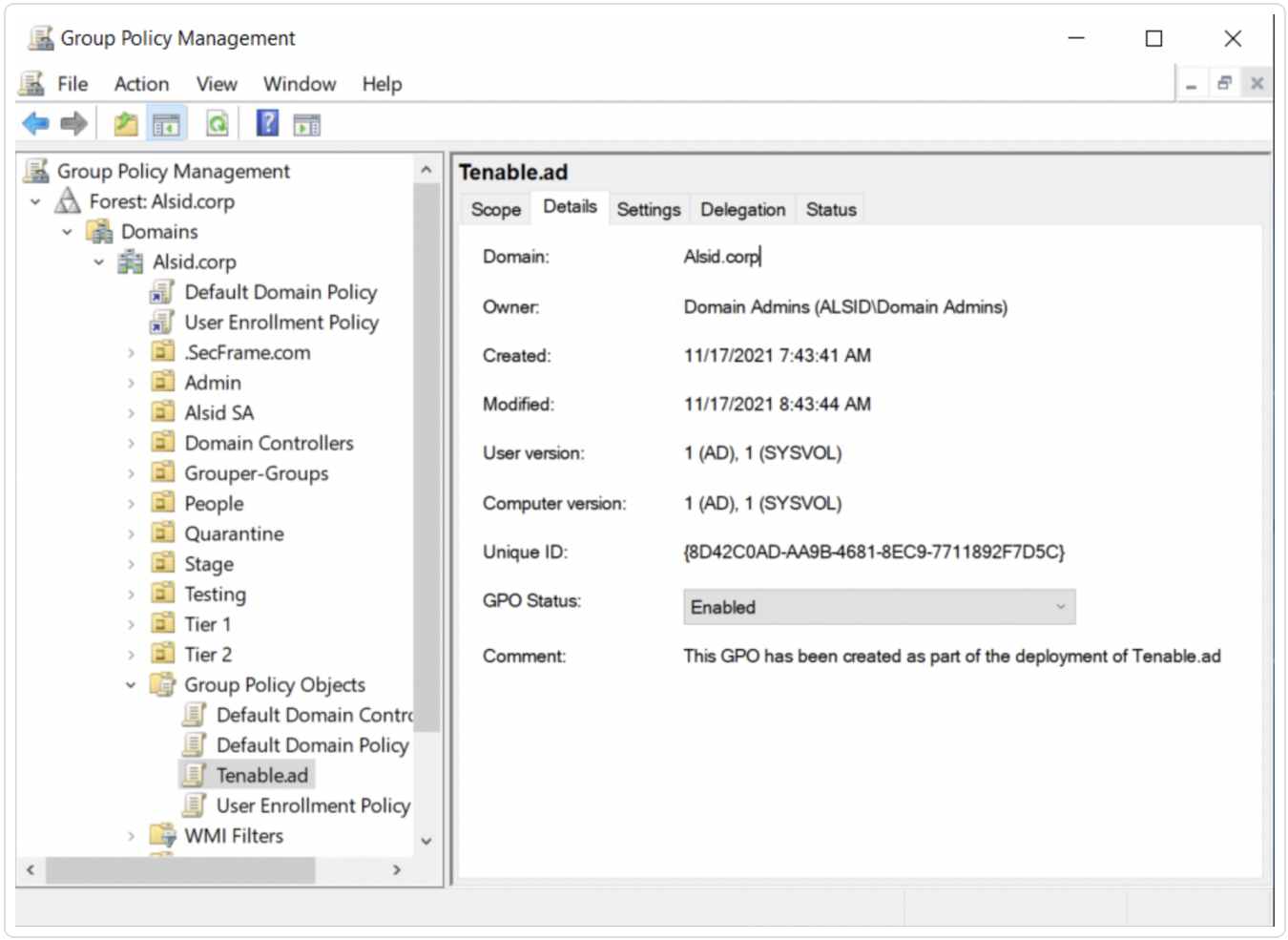
> **Conseil** : l'indicateur d'attaque (IoA) Zerologon **Exploitation** date de 2020. Si tous vos contrôleurs de domaine (DC) ont reçu des mises à jour au cours des trois dernières années, ils sont protégés contre cette vulnérabilité. Pour déterminer les correctifs requis pour sécuriser vos DC contre cette vulnérabilité, consultez les informations fournies par Microsoft dans Vulnérabilité d'élévation de privilège Netlogon. Une fois que vous avez confirmé la sécurité de vos DC, vous pouvez désactiver cet IoA en toute sécurité pour éviter des alertes inutiles.

2. Cliquez sur **Enregistrer**.

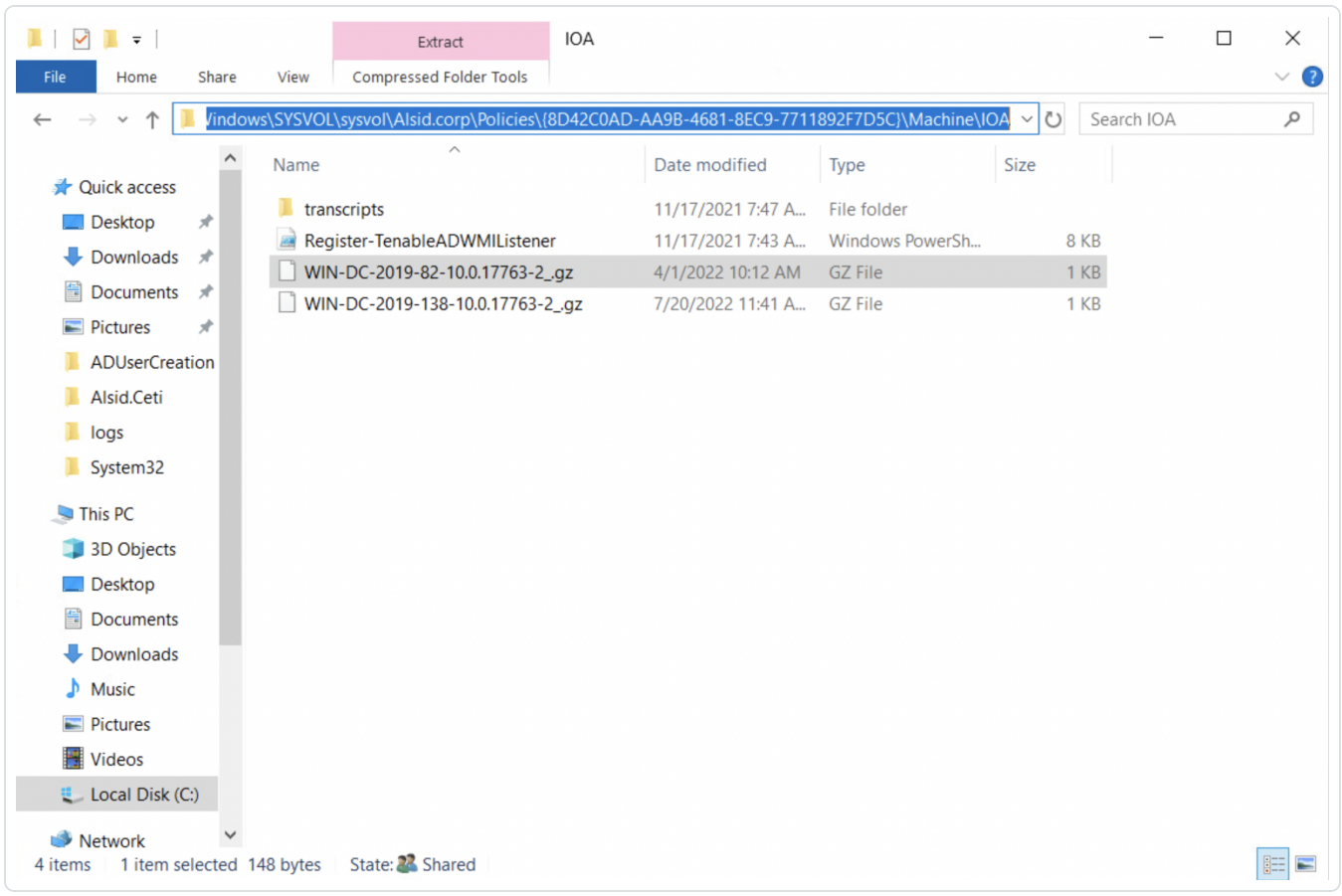
- Si vous avez activé les **mises à jour automatiques futures**, Tenable Identity Exposure enregistre et met automatiquement à jour votre nouvelle configuration. Attendez quelques minutes pour que cette mise à jour prenne effet.
- Si vous n'avez pas activé les **mises à jour automatiques futures**, une fenêtre de procédure apparaît pour vous guider Pour configurer des domaines pour les IoA :

Pour vérifier l'installation des IoA :

1. Dans la gestion des stratégies de groupe, vérifiez que la nouvelle GPO Tenable Identity Exposure existe et qu'elle est liée à l'OU `Contrôleurs de domaine` :



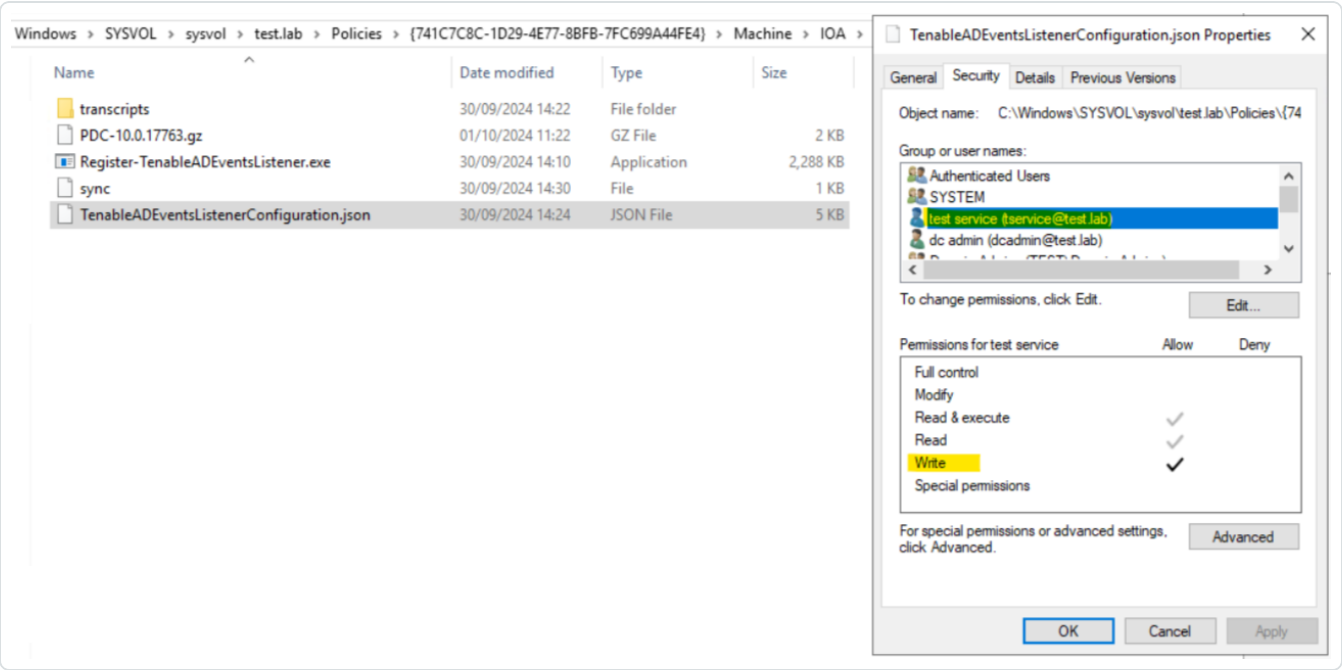
2. Accédez au chemin `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` et vérifiez que le fichier `.gz` existe pour **tous les contrôleurs de domaine** avant de tester les IoA :



Pour vérifier l'accès à l'autorisation « Écriture » sur le compte de service Tenable Identity Exposure :

1. Dans le gestionnaire de fichiers, accédez à `\\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\Machine\`.
2. Effectuez un clic droit sur le fichier `TenableADEventsListener Configuration.json` et sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Sécurité** et cliquez sur **Avancé**.
4. Cliquez sur l'onglet **Accès effectif**.
5. Cliquez sur **Sélectionner un utilisateur**.
6. Saisissez `<TENABLE-SERVICE-ACCOUNT-NAME>` et cliquez sur **OK**.
7. Cliquez sur **Afficher l'accès effectif**.

8. Vérifiez que l'autorisation « Écriture » est active pour le compte de service Tenable.



Vous pouvez également utiliser Powershell :

- Exécutez les commandes suivantes :

```
Install-Module -Name NTFSSecurity -RequiredVersion 4.2.3
```

```
Get-NTFSEffectiveAccess -Path \\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\IOA\ -
Account <TENABLE-SERVICE-ACCOUNT-NAME>
```

Pour calibrer les IoA :

Pour éviter de recevoir des faux positifs pour les attaques ou de ne pas pouvoir détecter les vraies attaques, vous devez calibrer vos IoA en fonction de votre environnement, les adapter à la taille de votre infrastructure Active Directory, mettre les outils connus sur liste blanche, etc.

1. Voir le Guide de référence des indicateurs d'attaque Tenable Identity Exposure pour plus d'informations sur les options et les valeurs recommandées à sélectionner.

2. Dans le profil de sécurité, appliquez les options et les valeurs à chaque IoA comme décrit dans Personnaliser un indicateur.

Résolution des problèmes

Les messages d'erreur suivants peuvent apparaître pendant le déploiement :

Message	Remédiation
« Tenable Identity Exposure cannot write to the configuration file because the target folder `<targetFolder>` does not exist. This indicates that the IoA module deployment may have failed. » (Tenable.ad ne peut pas écrire dans le fichier de configuration car le dossier cible <targetFolder> n'existe pas. Cette situation indique que le déploiement du module IoA a peut-être échoué.)	Désinstallez le script et cliquez sur « Voir la procédure » pour obtenir des instructions sur la réinstallation du script.
« Tenable Identity Exposure could not write to the configuration file located on `<targetFile>` to update it. This can be due to another process locking the file or permission changes. » (Tenable.ad n'a pas pu écrire dans le fichier de configuration situé sur <targetFile> pour le mettre à jour. Cette situation peut être due au fait qu'un autre processus a verrouillé le fichier ou à des modifications d'autorisations.)	• Vérifiez qu'aucun autre processus que le module IoA n'utilise le fichier de configuration. • Vérifiez que le compte de service est autorisé à modifier le contenu du fichier. • Si vous ne souhaitez pas accorder d'autorisation au compte de service, désactivez le curseur « Mises à jour automatiques » et cliquez sur « Voir la procédure » pour savoir comment effectuer une mise à jour manuelle chaque fois que vous modifiez votre configuration IoA.

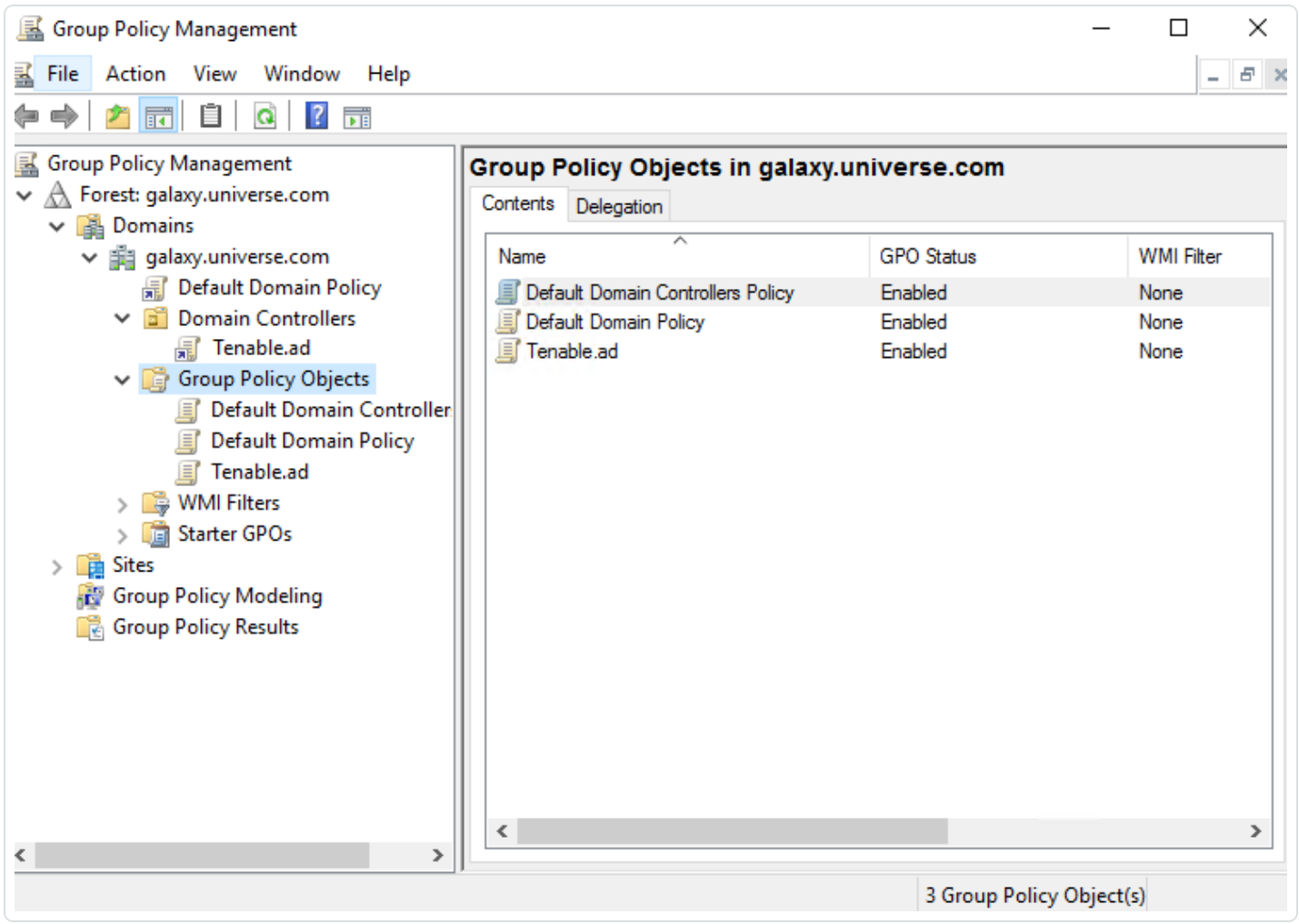
« The target folder `<targetFolder>` contains a version of Tenable Identity Exposure that cannot run automatic updates. » (Le dossier cible <targetFolder> contient une version de Tenable.ad qui ne peut pas exécuter de mises à jour automatiques.)	Le script actuellement installé est une ancienne version utilisant WMI. Désinstallez la version actuelle, téléchargez un nouveau script d'installation et exécutez ce script.
« The configuration file deployment ran into an unexpected error. » (Le déploiement du fichier de configuration a rencontré une erreur inattendue.)	Désinstallez le script et cliquez sur « Voir la procédure » pour obtenir des instructions sur la réinstallation du script. Si l'opération échoue, contactez votre représentant du support client.

Pour plus d'informations, voir :

- Script d'installation des indicateurs d'attaque
- Modifications techniques et impact potentiel
- Détection antivirus
- Précédence des configurations avancées de stratégie d'audit

Script d'installation des indicateurs d'attaque

Après avoir téléchargé et exécuté le fichier d'installation des indicateurs d'attaque (IoA), le script IoA crée un objet de stratégie de groupe (GPO) qui s'appelle `Tenable.ad` par défaut dans la base de données Active Directory (AD). Le système lie la GPO Tenable Identity Exposure uniquement à l'unité d'organisation (OU) des contrôleurs de domaine qui contient tous les contrôleurs de domaine (DC). La nouvelle stratégie se réplique automatiquement entre tous les DC en utilisant le mécanisme GPO.



Script d'installation (Tenable Identity Exposure v. 3.29 et versions ultérieures)

La GPO contient des scripts PowerShell que tous les DC exécutent localement pour collecter des données d'intérêt, comme suit :

- Le script configure un observateur de journaux d'événements sur chaque contrôleur de domaine à l'aide de l'API Windows EvtSubscribe. Le script permet de s'abonner à chaque canal de journal d'événements nécessaire, comme spécifié dans le fichier de configuration `TenableADventsListenerConfiguration.json`, en soumettant une demande et un rappel déclenché par EvtSubscribe pour chaque journal d'événements correspondant.
- L'observateur d'événements reçoit les journaux d'événements et les place en mémoire tampon avant de les vider régulièrement dans un fichier stocké dans un partage réseau appelé SYSVOL. Chaque DC se connecte à un fichier SYSVOL unique qui stocke les événements

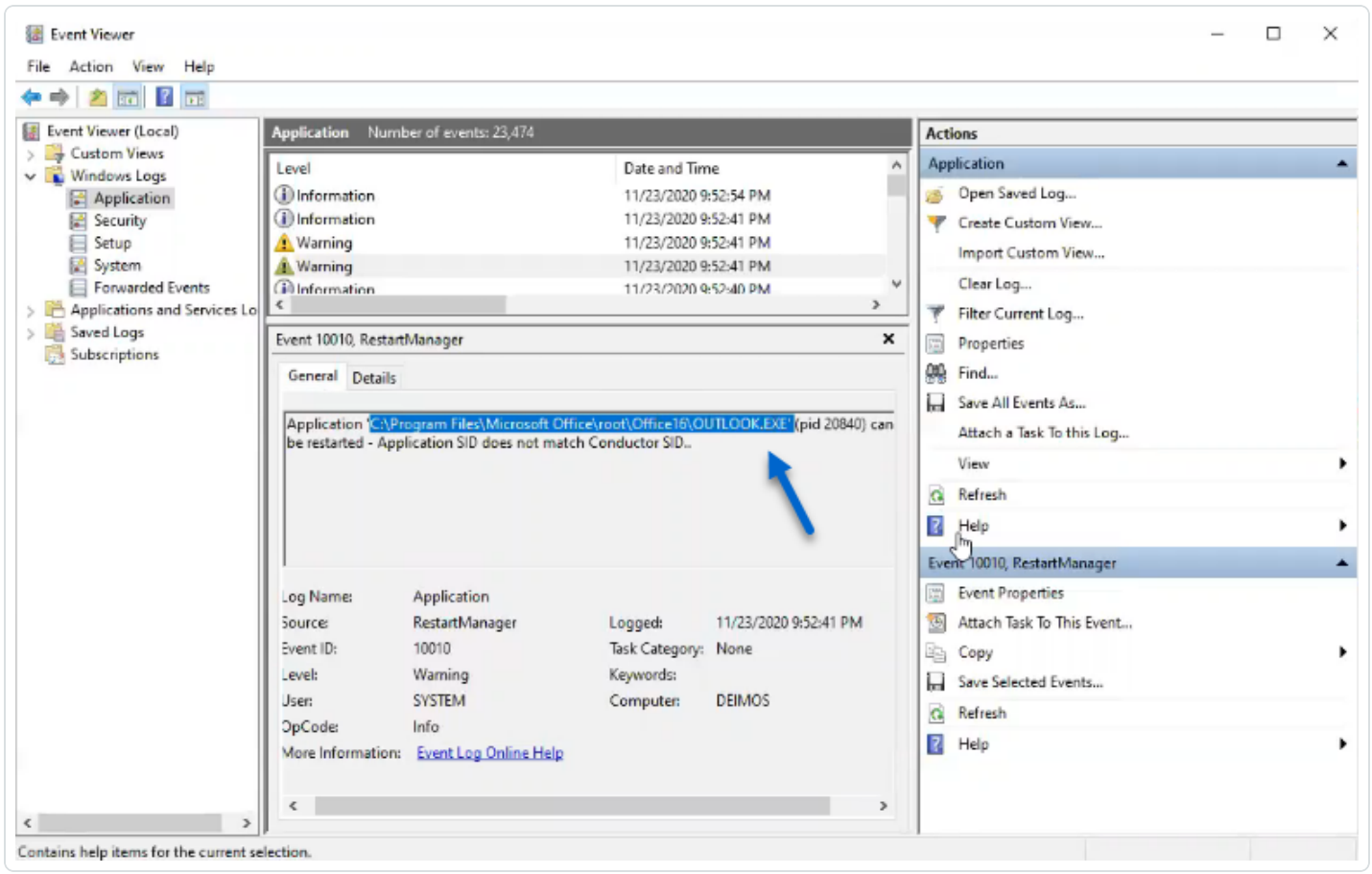
collectés et le réplique sur d'autres contrôleurs de domaine.

- Le script crée également un consommateur WMI pour que ce mécanisme persiste en réenregistrant l'abonné à l'événement lorsqu'un DC redémarre. WMI notifie le consommateur chaque fois qu'un contrôleur de domaine redémarre, afin de permettre au consommateur de réenregistrer l'observateur d'événements.
- À ce stade, la réplication du système de fichiers distribués (DFS) se produit et synchronise automatiquement les fichiers entre les contrôleurs de domaine. La plateforme de Tenable Identity Exposure écoute le trafic de réplication DFS entrant et utilise ces données pour collecter des événements, exécuter une analyse de sécurité, puis générer des alertes IoA.

Récupération de données locales

Les journaux d'événements Windows enregistrent tous les événements qui se produisent dans le système d'exploitation et ses applications. Les journaux d'événements utilisent un ensemble de composants intégrés à Windows.

À l'aide de l'API EvtSubscribe, l'observateur des journaux d'événements IoA Tenable Identity Exposure ne collecte que les segments de données utiles sous forme de chaînes d'insertion qu'il extrait des journaux d'événements. Tenable Identity Exposure écrit ces chaînes d'insertion dans un fichier stocké dans le dossier SYSVOL et les réplique via le moteur DFS. Ainsi, Tenable Identity Exposure collecte à partir des journaux d'événements la juste quantité de données de sécurité nécessaire pour exécuter une analyse et détecter les attaques.



Résumé du script IoA

Le tableau suivant offre un aperçu du déploiement du script Tenable Identity Exposure.

Étapes	Description	Composant impliqué	Action technique
1	Enregistrer le déploiement IoA de Tenable Identity Exposure	Gestion GPO	Crée la GPO `Tenable.ad` (nom par défaut) et la lie à l'OU Contrôleurs de domaine.

2	Lancer le déploiement de l'IoA de Tenable Identity Exposure sur le DC	Système local du DC	Chaque DC détecte la nouvelle GPO à appliquer, en fonction de la réplication AD et des intervalles d'actualisation de la stratégie de groupe.
3	Contrôler l'état de la politique de journalisation avancée	Système local du DC	Le système active la stratégie de journalisation avancée en définissant la clé de registre `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`.
4	Mettre à jour la stratégie de journalisation locale	Système local du DC	En fonction des IoA à détecter, Tenable Identity Exposure génère et active de manière dynamique des stratégies d'audit spécifiques. Cette stratégie ne désactive aucune stratégie de journalisation existante ; elle les enrichit uniquement si nécessaire. S'il détecte un conflit, le script d'installation de la GPO s'arrête et affiche le message « Tenable Identity Exposure requires the audit policy “...” but the current AD configuration prevents its usage » (Tenable.ad requiert la stratégie d'audit “...”, mais la configuration AD actuelle empêche son utilisation).
5	Inscrire un observateur d'événements et un producteur WMI	Système local du DC	Le système enregistre et exécute le script contenu dans la GPO. Ce script exécute un processus PowerShell pour s'abonner aux journaux d'événements à l'aide de l'API EvtSubscribe et pour créer une instance d'`ActiveScriptEventConsumer` à des fins de persistance. Tenable Identity Exposure utilise ces objets pour recevoir et stocker le contenu des journaux d'événements.

6	Collecter les messages des journaux d'événements	Système local du DC	Tenable Identity Exposure capture les messages pertinents du journal des événements, les met régulièrement en mémoire tampon et les enregistre dans des fichiers (un par DC) stockés dans le dossier SYSVOL associé à la GPO Tenable Identity Exposure (`...{GPO_GUID}\Machine\IOA<DC_name>`).
7	Répliquer les fichiers dans le dossier DC SYSVOL déclaré	Active Directory	À l'aide du DFS, l'infrastructure AD réplique les fichiers dans le domaine – plus précisément, dans le DC déclaré. La plateforme Tenable Identity Exposure reçoit une notification pour chaque fichier et lit son contenu.
8	Remplacer ces fichiers	Active Directory	Chaque contrôleur de domaine écrit automatiquement et en continu les événements régulièrement mis en mémoire tampon dans le même fichier.

Script d'installation (Tenable Identity Exposure v. 3.19.11 et versions antérieures)

La GPO contient des scripts PowerShell que tous les DC exécutent localement pour collecter des données d'intérêt, comme suit :

- Le script configure un observateur d'événements et un producteur/consommateur WMI (Windows Management Instrumentation) dans la mémoire de la machine. WMI est un composant Windows qui fournit des informations sur le statut des systèmes informatiques locaux ou distants.
- L'observateur d'événements reçoit les journaux d'événements et les place en mémoire tampon avant de les vider régulièrement dans un fichier stocké dans un partage réseau appelé SYSVOL. Chaque DC se connecte à un fichier SYSVOL unique qui stocke les événements collectés et le réplique sur d'autres contrôleurs de domaine.
- Le consommateur WMI rend ce mécanisme persistant en enregistrant à nouveau l'observateur d'événements lorsqu'un DC redémarre. Le producteur s'active et notifie le consommateur chaque fois qu'un DC redémarre. Par conséquent, le consommateur

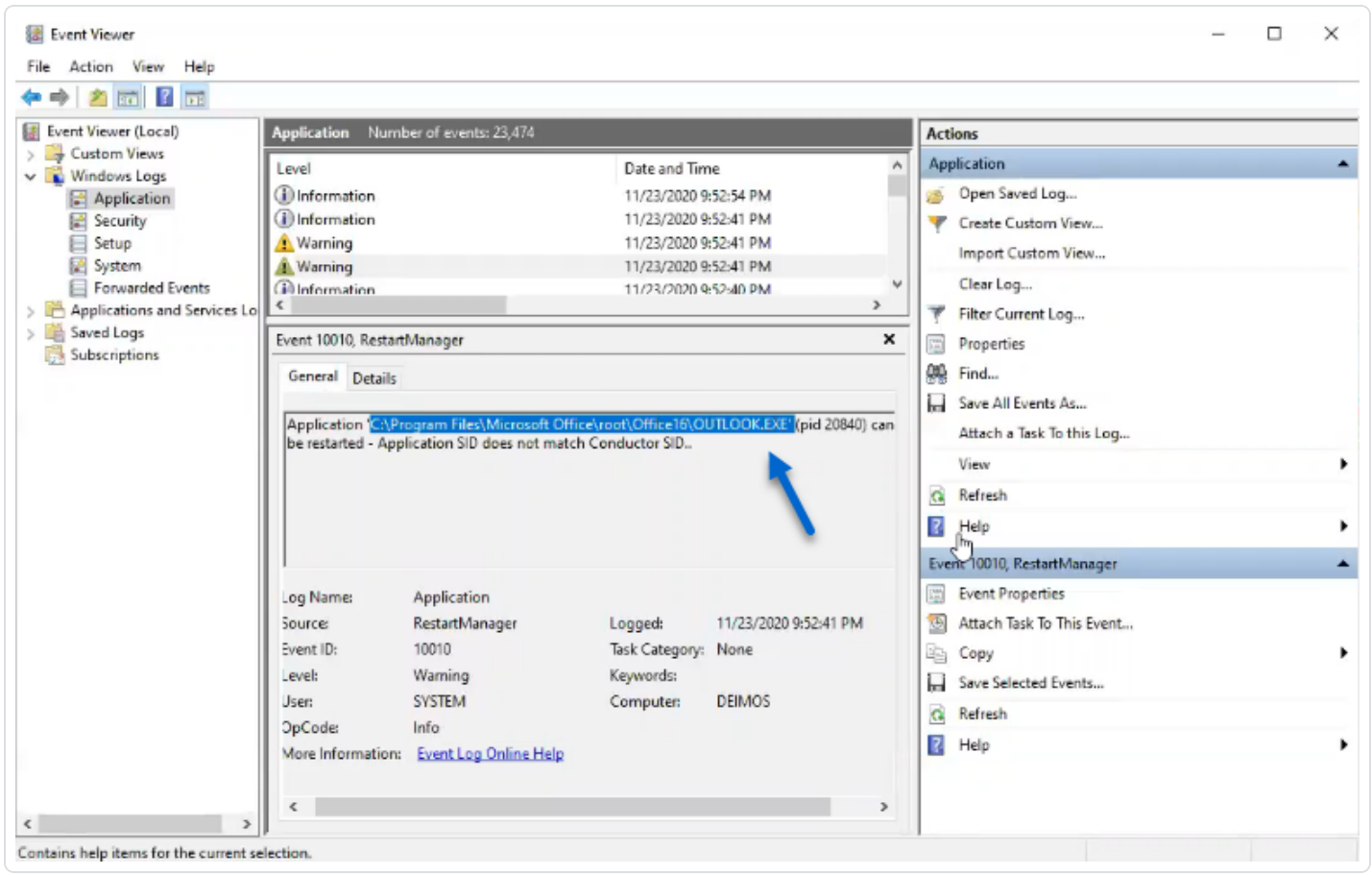
enregistre à nouveau l'observateur d'événements.

- À ce stade, la réplication du système de fichiers distribués (DFS) se produit et synchronise automatiquement les fichiers entre les contrôleurs de domaine. La plateforme de Tenable Identity Exposure écoute le trafic de réplication DFS entrant et utilise ces données pour collecter des événements, exécuter une analyse de sécurité, puis générer des alertes IoA.

Récupération de données locales

Les journaux d'événements Windows enregistrent tous les événements qui se produisent dans le système d'exploitation et ses applications. Les journaux d'événements, appelés Event Tracing for Windows (ETW), utilisent un ensemble de composants intégrés dans Windows. ETW se trouve dans le noyau et produit des données stockées localement sur les DC et qui ne sont pas répliquées par les protocoles AD.

En utilisant le moteur WMI, Tenable Identity Exposure ne collecte que les segments de données ETW utiles sous forme de chaînes d'insertion qu'il extrait des journaux d'événements. Tenable Identity Exposure écrit ces chaînes d'insertion dans un fichier stocké dans le dossier SYSVOL et les réplique via le moteur DFS. Ainsi, Tenable Identity Exposure peut collecter juste la bonne quantité de données de sécurité à partir d'ETW pour exécuter une analyse de sécurité et détecter les attaques.



Résumé du script IoA

Le tableau suivant offre un aperçu du déploiement du script Tenable Identity Exposure.

Étapes	Description	Composant impliqué	Action technique
1	Enregistrer le déploiement IoA de Tenable Identity Exposure	Gestion GPO	Crée la GPO `Tenable.ad` (nom par défaut) et la lie à l'OU Contrôleurs de domaine.
2	Lancer le déploiement de l'IoA de Tenable	Système local du DC	Chaque DC détecte la nouvelle GPO à appliquer, en fonction de la réplication AD et des intervalles d'actualisation de la stratégie de groupe.

	Identity Exposure sur le DC		
3	Inscrire un observateur d'événements et un producteur/consommateur WMI	Système local du DC	Le système enregistre et exécute une tâche immédiate. Cette tâche exécute un processus PowerShell pour créer des instances `ManagementEventWatcher` et `ActiveScriptEventConsumer`. Tenable Identity Exposure utilise ces objets pour recevoir et stocker les messages ETW.
4	Contrôler l'état de la politique de journalisation avancée	Système local du DC	Le système active la stratégie de journalisation avancée en définissant la clé de registre `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`.
5	Mettre à jour la stratégie de journalisation locale	Système local du DC	En fonction des IoA à détecter, Tenable Identity Exposure génère et active de manière dynamique une stratégie de journalisation avancée. Cette stratégie ne désactive aucune stratégie de journalisation existante ; elle les enrichit uniquement si nécessaire. S'il détecte un conflit, le script d'installation de la GPO s'arrête et affiche le message « Tenable Identity Exposure requires the audit policy “...” but the current AD configuration prevents its usage » (Tenable.ad requiert la stratégie d'audit “...”, mais la configuration AD actuelle empêche son utilisation).
6	Collecter les messages ETW	Système local du DC	Tenable Identity Exposure capture les messages ETW pertinents, les met régulièrement en mémoire tampon et les enregistre dans des fichiers (un par DC) stockés dans le dossier SYSVOL associé à la GPO Tenable Identity Exposure (`...{GPO_`

			GUID}\Machine\IOA<DC_name>).
7	Répliquer les fichiers vers la plateforme Tenable Identity Exposure	Active Directory	À l'aide du DFS, l'infrastructure AD réplique les fichiers dans le domaine. La plateforme Tenable Identity Exposure reçoit également les fichiers.
8	Remplacer ces fichiers	Active Directory	Chaque contrôleur de domaine écrit automatiquement et en continu les événements régulièrement mis en mémoire tampon dans le même fichier.

Voir aussi

- Installer des indicateurs d'attaque
- Modifications techniques et impact potentiel

Modifications techniques et impact potentiel

Le script d'installation du module Indicateurs d'attaque (IoA) crée une GPO qui applique les changements suivants de manière transparente sur les DC surveillés :

- Création d'une nouvelle GPO, nommée « Tenable.ad » par défaut et liée à l'unité d'organisation (UO) du contrôleur de domaine par défaut.
- Modification d'une clé de registre pour activer la stratégie de journalisation Microsoft Advanced.
- Activation d'une nouvelle stratégie de journal des événements pour obliger les contrôleurs de domaine à générer les informations ETW requises par les IoA.

> **Remarque** : la stratégie Journal des événements est obligatoire pour que le moteur ETW puisse générer les chaînes d'insertion requises par Tenable Identity Exposure. Cette stratégie ne désactive aucune stratégie de journalisation existante, mais y ajoute des informations. En cas de conflit, le script de déploiement s'arrête avec un message d'erreur.

- Ajout d'une autorisation d'écriture pour le compte de service Tenable Identity Exposure qui permet les « mises à jour automatiques » de la configuration IoA stockée dans le dossier GPO.

Limitations et impacts potentiels

Le module **Indicateur d'attaque** (IoA) peut poser les limitations suivantes :

- Le module IoA utilise les données ETW et fonctionne dans les limites définies par Microsoft.
- La GPO installée doit être répliquée sur l'ensemble du domaine, et le délai d'actualisation de la GPO doit s'écouler pour que le processus d'installation soit terminé. Pendant cette période de réplication, des faux positifs et des faux négatifs peuvent se produire, même si Tenable Identity Exposure réduit cet effet en ne lançant pas immédiatement les vérifications dans le moteur d'indicateur d'attaque.
- Tenable utilise le partage de fichiers SYSVOL pour récupérer les informations ETW des contrôleurs de domaine. Lors de la réplication de SYSVOL sur tous les contrôleurs du domaine, une augmentation significative de l'activité de réplication apparaît pendant un pic élevé d'activité Active Directory.
- La réplication des fichiers entre les contrôleurs de domaine et Tenable Identity Exposure consomme également de la bande passante réseau. Tenable Identity Exposure contrôle ces impacts avec la suppression automatique des fichiers qu'il collecte et limite la taille de ces fichiers (500 Mo maximum par défaut.)
- Problèmes de réplication lente ou interrompue du système de fichiers distribués (DFS). Pour plus d'informations, voir Atténuation des problèmes liés à la réplication DFS.

Voir aussi

- Indicators of Attack and the Active Directory
- Installer des indicateurs d'attaque
- Script d'installation des indicateurs d'attaque
- Dépanner les indicateurs d'attaque

Scénarios d'attaque (< v. 3.36)

Attention : cette fonctionnalité de mise à jour de la configuration d'indicateur d'attaque ne s'applique plus aux versions > 3.36 de Tenable Identity Exposure.

Rôle utilisateur requis : utilisateur d'organisation disposant des autorisations pour modifier la configuration des indicateurs d'attaque.

Vous définissez des scénarios d'attaque en sélectionnant les types d'attaques que Tenable Identity Exposure doit surveiller dans des domaines spécifiques.

Avant de commencer

Pour pouvoir modifier le scénario d'attaque, vous devez disposer d'un rôle utilisateur ayant les autorisations suivantes :

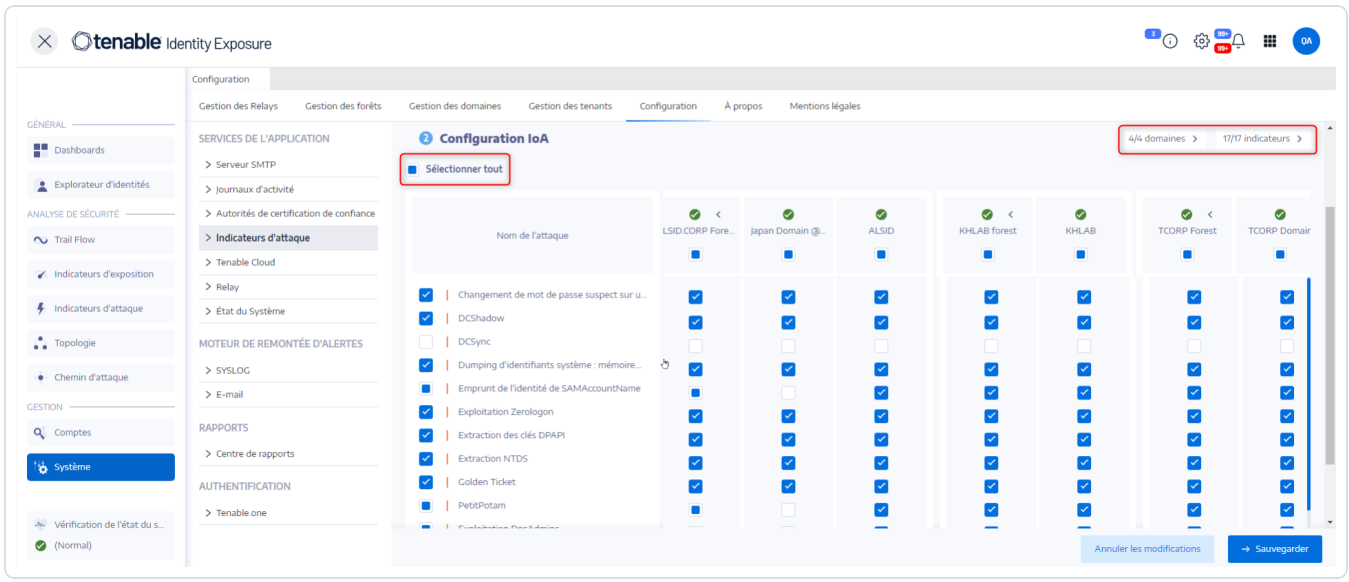
- Dans **Entités de type Données**, accès « Lecture » à :
  - Tous les indicateurs d'attaque
  - Tous les domaines
- Dans **Entités de type Interface**, accès à :
  - Gestion > Système > Configuration
  - Gestion > Système > Configuration > Services de l'application > Indicateurs d'attaque
  - Gestion > Système > Configuration > Services de l'application > Indicateurs d'attaque > Télécharger le fichier d'installation

Pour plus d'informations sur les autorisations basées sur le rôle, voir Définir les autorisations d'un rôle.

Pour définir un scénario d'attaque :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration** > **Indicateurs d'attaque**.

   Le volet **Définition des scénarios d'attaque** apparaît.



2. Sous **Nom de l'attaque**, sélectionnez l'attaque à surveiller.
3. Sélectionnez le domaine dans lequel l'attaque sélectionnée doit être surveillée.
4. Vous pouvez également effectuer l'une des opérations suivantes :
    - Cliquez sur **Tout sélectionner** pour surveiller toutes les attaques dans tous les domaines.
    - Cliquez sur **n/n domaines** ou **n/n indicateurs** pour filtrer des domaines spécifiques à surveiller pour des attaques spécifiques.
5. Cliquez sur **Enregistrer**.

    Un message de confirmation indique que Tenable Identity Exposure efface le statut d'activité de chaque attaque une fois la configuration enregistrée.
6. Cliquez sur **Confirmer**.

    Un message confirme que Tenable Identity Exposure a mis à jour la configuration de l'indicateur d'attaque.
7. Cliquez sur **Télécharger le fichier d'installation**.
8. Pour que la nouvelle configuration d'attaque soit appliquée, exécutez le fichier d'installation :

a. Copiez et collez le fichier d'installation téléchargé sur le contrôleur du domaine surveillé.

b. Ouvrez un terminal PowerShell avec des droits d'administration.

c. Dans Tenable Identity Exposure, copiez les commandes sous la section Indicateurs d'attaque en bas de la fenêtre.



d. Dans la fenêtre PowerShell, collez les commandes pour exécuter le script.

Quota de charge de travail

Attention : la fonctionnalité de quota de charge de travail ne s'applique plus aux versions > 3.36 de Tenable Identity Exposure.

Rôle utilisateur requis : utilisateur d'organisation disposant des autorisations pour modifier le quota de charge de travail.

Chaque indicateur d'attaque dans Tenable Identity Exposure est associé à un quota de charge de travail qui comptabilise les ressources requises pour analyser les données d'une attaque.

Tenable Identity Exposure calcule le quota de charge de travail pour limiter le nombre d'indicateurs d'attaque (IoA) exécutés simultanément, ce qui a un impact sur la bande passante et l'utilisation du processeur pour la génération d'événements sur les contrôleurs de domaine.

Après avoir modifié la limite de quota de charge de travail, effectuez les opérations suivantes :

- Augmentation : surveillez les statistiques après une augmentation pour assurer une marge confortable.

- Diminution : désactivez certains IoA pour rester sous ce quota, en sachant que cela réduit la couverture de sécurité contre les attaques.

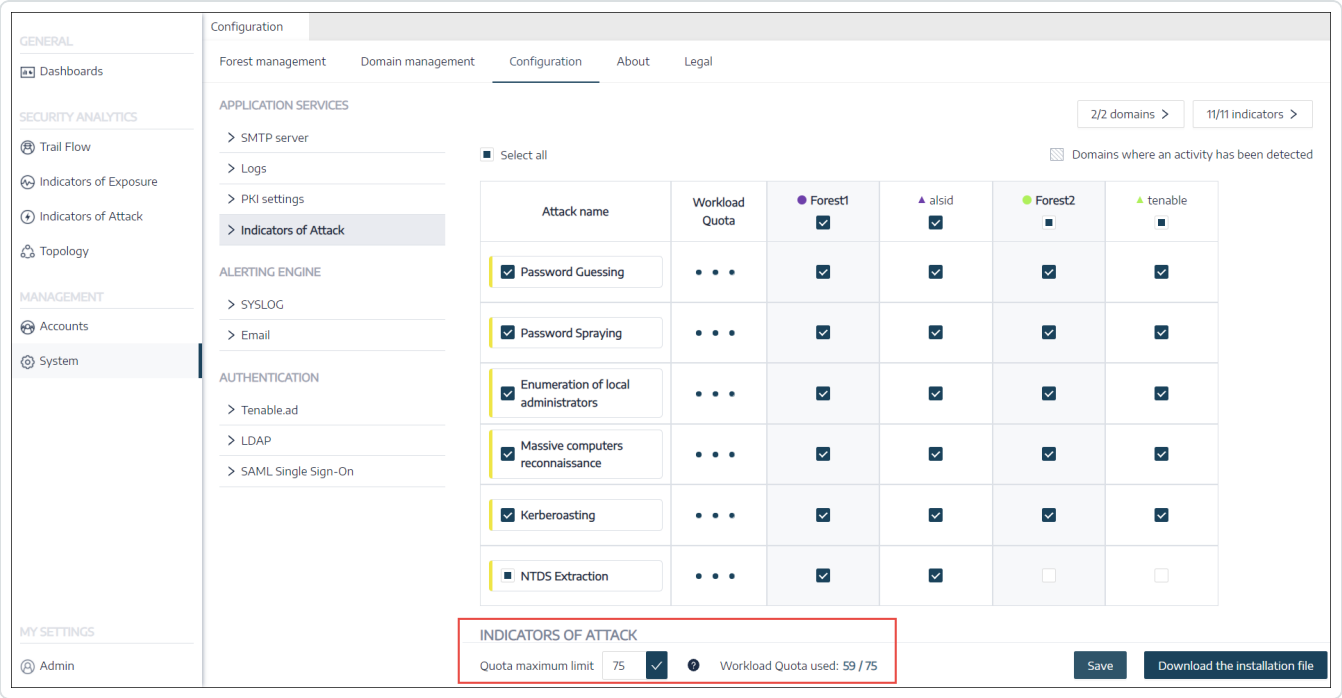
Pour modifier la limite de quota de charge de travail :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration** > **Indicateurs d'attaque**.

   Le volet **Configuration IoA** apparaît.

2. Sélectionnez les IoA que vous souhaitez pour votre configuration.

3. Sous **Indicateurs d'attaque**, dans la zone **Limite maximale de quota**, saisissez une valeur de limite de quota de charge de travail.



4. Cliquez sur la coche à côté de la valeur que vous avez saisie.

   Un message vous informe des impacts de la modification sur Tenable Identity Exposure.

   > **Remarque** : si vous saisissez une limite maximale de quota inférieure à ce qu'exige la configuration d'attaque actuelle, vous devez ajuster le nombre d'indicateurs d'attaque actifs ou augmenter la limite.

5. Cliquez sur **Confirmer**.

   Un message confirme que Tenable Identity Exposure a mis à jour la limite maximale de quota.

6. Cliquez sur **Enregistrer**.

   Un message de confirmation indique que Tenable Identity Exposure efface le statut d'activité de chaque attaque une fois la configuration enregistrée.

7. Cliquez sur **Confirmer**.

   Un message confirme que Tenable Identity Exposure a mis à jour la configuration de l'indicateur d'attaque.

8. Cliquez sur **Télécharger le fichier d'installation**.

9. Pour que la nouvelle configuration d'attaque soit appliquée, exécutez le fichier d'installation :

   a. Copiez et collez le fichier d'installation téléchargé sur le contrôleur du domaine surveillé.

   b. Ouvrez un terminal PowerShell avec des droits d'administration.

   c. Dans Tenable Identity Exposure, copiez les commandes sous la section Indicateurs d'attaque en bas de la fenêtre.



   d. Dans la fenêtre PowerShell, collez les commandes pour exécuter le script.

Programme d'installation de Microsoft Sysmon

Certains indicateurs d'attaque (IoA) de Tenable Identity Exposure nécessitent d'activer le service Microsoft System Monitor (Sysmon).

Sysmon surveille et consigne l'activité du système dans le journal des événements Windows, afin de fournir davantage d'informations de sécurité à l'infrastructure de suivi des événements de Windows (ETW).

Comme l'installation d'un service et d'un pilote Windows supplémentaires peut affecter les performances des contrôleurs de domaine hébergeant l'infrastructure Active Directory, Tenable ne déploie pas automatiquement Microsoft Sysmon. Vous devez l'installer manuellement ou utiliser une GPO dédiée.

Les IoA suivants nécessitent Microsoft Sysmon.

Nom	Raison
Récupération des identifiants système : mémoire LSASS	Détecte l'injection de processus

Remarque : si vous choisissez d'installer Sysmon, vous devez l'installer sur tous les contrôleurs de domaine et pas uniquement sur le PDC pour collecter tous les événements nécessaires.

Remarque : testez votre installation Sysmon, afin d'identifier les problèmes de compatibilité avant un déploiement complet de Tenable Identity Exposure.

Conseil : veillez à mettre à jour Sysmon régulièrement après l'installation pour bénéficier de tous les correctifs qui corrigent les vulnérabilités possibles. La plus ancienne version compatible avec Tenable Identity Exposure est Sysmon 12.0.

Pour installer Sysmon :

1. Téléchargez Sysmon à partir du site web de Microsoft.
2. Dans l'interface de ligne de commande, exécutez la commande suivante pour installer Microsoft Sysmon sur l'ordinateur local :

   ```
   .\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
   ```

   Remarque : voir le fichier de configuration Sysmon commenté pour des explications sur la configuration.

3. Exécutez la commande suivante pour ajouter une clé de registre afin d'indiquer aux filtres WMI que Sysmon est installé :

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Pour désinstaller Sysmon :

1. Ouvrez un terminal PowerShell.
2. Accédez au dossier qui contient `Sysmon64.exe`.
3. Saisissez la commande suivante :

```
PS C:\> .\Sysmon64.exe -u
```

Pour supprimer la clé de registre :

- Dans l'interface de ligne de commande, saisissez la commande suivante sur toutes les machines qui exécutent Sysmon :

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Fichier de configuration de Sysmon

Remarque :
- Copiez et enregistrez le fichier de configuration de Sysmon sous la forme d'un fichier XML avant de l'utiliser. En cas d'erreur, vous pouvez également télécharger le fichier de configuration directement ici.
- Déverrouillez le fichier dans les propriétés du fichier avant de l'exécuter.

```
<Sysmon schemaversion="4.40">
  <EventFiltering>

    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
```

```
    </RuleGroup>

    <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM
[FileCreateTime]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>

    <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessTerminate>
    </RuleGroup>

    <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DriverLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </ImageLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
    <RuleGroup name="" groupRelation="or">
      <CreateRemoteThread onmatch="include">
        <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      </CreateRemoteThread>
    </RuleGroup>

    <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RawAccessRead>
    </RuleGroup>

    <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <RuleGroup name="" groupRelation="or">
        <ProcessAccess onmatch="include">
```

```
          <!-- Detect Access to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1FFFFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1F1FFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1010</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x143A</GrantedAccess>
          </Rule>

          <!-- Detect process hollowing to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0800</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x800</GrantedAccess>
          </Rule>

          <!-- Detect process process injection to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0820</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x820</GrantedAccess>
          </Rule>
        </ProcessAccess>
    </RuleGroup>

    <!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
    <RuleGroup name="" groupRelation="or">
      <RegistryEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
```

```
      </RegistryEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateStreamHash onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateStreamHash>
    </RuleGroup>

    <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
    <RuleGroup name="" groupRelation="or">
      <PipeEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </PipeEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
    <RuleGroup name="" groupRelation="or">
      <WmiEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </WmiEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
    <RuleGroup name="" groupRelation="or">
      <DnsQuery onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DnsQuery>
    </RuleGroup>

    <!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileDelete>
    </RuleGroup>

  </EventFiltering>
</Sysmon>
```

Désinstaller les indicateurs d'attaque

Rôle requis : administrateur sur l'ordinateur local.

Pour désinstaller le module Indicateurs d'attaque (IoA), vous exécutez une commande qui crée une stratégie de groupe (GPO) appelée « Tenable Identity Exposure cleaning ».

Le processus de désinstallation utilise cette nouvelle GPO par défaut pour nettoyer les GPO précédemment installées et ses fichiers SYSVOL, le paramètre de registre, la stratégie de journalisation avancée et les filtres WMI.

Remarque : si vous avez modifié le nom de la GPO initiale, vous devez le transmettre au programme de désinstallation pour qu'il sache quelle GPO il doit désinstaller. Pour transmettre le nouveau nom de GPO, utilisez le paramètre `-GpoDisplayName`.

Pour désinstaller le module IoA :

1. Dans l'interface de ligne de commande, exécutez la commande suivante pour désinstaller le module IoA :

   ```
   Register-TenableIOA.ps1 -Uninstall
   ```

2. Répliquez cette nouvelle GPO dans l'ensemble du domaine. Le script impose un délai de 4 heures pour l'exécution de la réplication.

3. Exécutez la commande suivante pour supprimer la GPO de nettoyage :

   ```
   Remove-GPO -Guid <GUID> -Domain "<DOMAIN>"
   ```

4. Facultatif : exécutez la commande suivante pour vérifier que la GPO n'existe plus :

   ```
   (Get-ADDomainController -Filter *).Name | Foreach-Object {Get-GPO -Name "Tenable.ad cleaning"}
   | Select Displayname| measure
   ```

Vous avez terminé la désinstallation des IoA. Cependant, leurs entrées de registre peuvent persister si une autre GPO ne les définit pas. Voici les entrées de registre utilisées par l'IoA « Reconnaissance massive d'ordinateurs » (elles peuvent varier en fonction de votre configuration IoA spécifique) :

- `HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\AuditReceivingNTLMTraffic (valeur : 2)`
- `HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\RestrictSendingNTLMTraffic (valeur : 1)`

- `HKLM\MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\AuditNTLMInDomain (valeur : 7)`

Pour supprimer ces entrées de registre, exécutez le script PowerShell suivant sur tous vos contrôleurs de domaine :

```
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name
"AuditReceivingNTLMTraffic"
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name
"RestrictSendingNTLMTraffic"
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\Netlogon\Parameters" -Name
"AuditNTLMInDomain"
```

Suppression manuelle des dossiers de GPO obsolètes de SYSVOL

Dans certains cas, lors de la réinstallation de la GPO IoA, d'anciens dossiers peuvent rester dans le répertoire SYSVOL en raison d'une fonctionnalité Microsoft. Si le Directory Listener considère ces dossiers obsolètes comme étant le dossier IoA, cela peut entraîner des échecs de détection.

Effectuez la procédure suivante pour assurer la bonne suppression des dossiers obsolètes de la GPO IoA, et ainsi éviter les problèmes de détection lors de la réinstallation.

Pour supprimer les dossiers obsolètes de la GPO IoA :

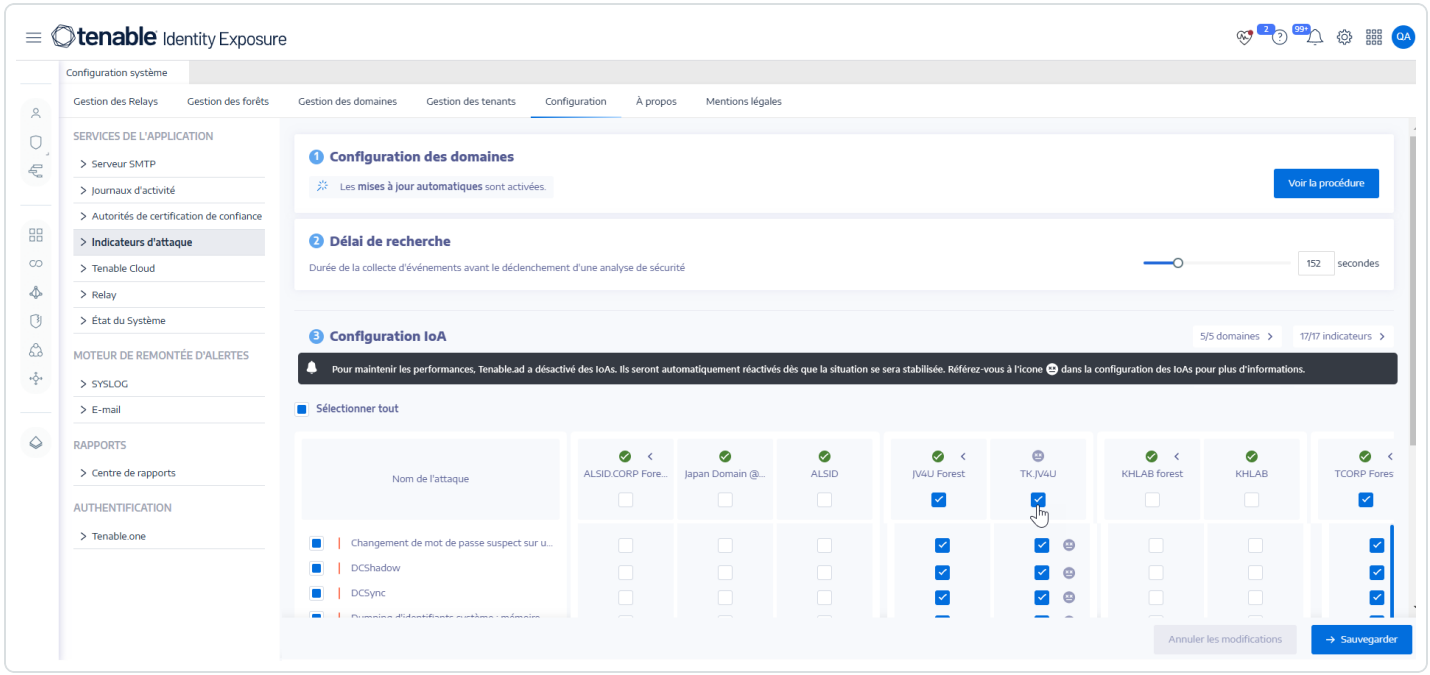
Supprimez manuellement tous les dossiers IoA obsolètes du répertoire SYSVOL qui ne correspondent pas au GUID de la dernière GPO IoA. En veillant à conserver uniquement la stratégie de groupe (GPO) la plus récente, vous pouvez maintenir la cohérence et prévenir les conflits de politiques potentiels.

Si vous avez besoin de conseils supplémentaires ou si vous rencontrez des problèmes, contactez le service d'assistance pour obtenir de l'aide.

Indicateurs d'attaque désactivés

Occasionnellement, Tenable Identity Exposure peut désactiver certains indicateurs d'attaque (IoA) de manière temporaire pour maintenir des performances optimales.

Lorsqu'un indicateur est désactivé, l'icône est affichée en regard.



Icônes de statut IoA

Statut de l'icône de la première ligne

- Icône grise – Indique qu'au moins un IoA est temporairement désactivé.
- Icône en forme de coche verte – Indique que tous les IoA configurés sont activés.

Statut de l'icône des autres lignes

- Icône grise – Apparaît en regard des domaines spécifiques où les IoA sont désactivés.

Informations des info-bulles

Lorsque vous placez le curseur de la souris sur les icônes de statut, vous pouvez voir les info-bulles suivantes :

- Icône grise  – « Un ou plusieurs IoA sont temporairement désactivés »
- Icône en forme de coche verte  – « Tous les IoA configurés sont activés »
- Icône grise  sur les autres lignes : « IoA temporairement désactivé (depuis le jj-mm-aaaa hh:mm) pour maintenir les performances. »

Message d'alerte

Lorsque Tenable Identity Exposure désactive les IoA, un message d'alerte apparaît au-dessus du tableau des IoA :

« Pour maintenir les performances, Tenable Identity Exposure a désactivé certains IoA. Ils seront réactivés automatiquement une fois que la situation se sera stabilisée. Reportez-vous à l'icône dans votre configuration IoA pour plus d'informations. »

Règles de visibilité

Le statut désactivé est visible à la fois au niveau du domaine et de la forêt.

- Si vous décochez un domaine comportant une icône de désactivation et qu'aucun autre domaine n'est associé à cette icône, elle disparaît pour le domaine lié.
- Si tous les domaines liés à une forêt ne comportent plus d'icônes de désactivation, l'icône disparaît pour la forêt liée.

Réactivation automatique

Tenable Identity Exposure réactive automatiquement les IoA désactivés une fois les performances du système stabilisées. Aucune intervention manuelle n'est requise.

La désactivation temporaire des IoA est une fonction intégrée conçue pour maintenir les performances du système. Tenable Identity Exposure ajuste dynamiquement les IoA actifs pour assurer un fonctionnement optimal sans compromettre les capacités de surveillance de la sécurité.

Réagir à l'icône « Désactivé » grise

Si vous voyez l'icône « Désactivé » grise :

1. Attendez que la situation soit résolue : dans la plupart des cas, il suffit d'attendre. Tenable Identity Exposure réactive automatiquement les IoA désactivés une fois les performances du système stabilisées.
2. Pour les déploiements sur site :
    - Si vous remarquez que cela se produit fréquemment, malgré les recommandations de la matrice des ressources, vous devrez peut-être ajouter des ressources à la machine hébergeant le service Cygni.
    - Envisagez d'augmenter la puissance du processeur, la RAM ou l'espace disque selon les besoins pour améliorer les performances globales du système.
3. Fréquence de surveillance : notez la fréquence à laquelle cette icône est visible. Si elle apparaît régulièrement, cela peut indiquer que vos ressources actuelles sont constamment sous pression.
4. Passez en revue votre configuration IoA : en attendant la réactivation, pensez à examiner votre configuration IoA actuelle pour vous assurer qu'elle correspond à vos besoins de sécurité et aux ressources disponibles.

Dépanner les indicateurs d'attaque

- Précédence des configurations avancées de stratégie d'audit
- Détection antivirus
- Fichiers journaux Tenable Identity Exposure
- Validation de l'observateur des journaux d'événements
- Atténuation des problèmes liés à la réplication DFS
- Rétention du journal des événements Windows
- Entrées de type « Inconnu » dans les alertes d'indicateurs d'attaque
- Indicateurs d'attaque opérationnels
- Délais de détection des indicateurs d'attaque

Détection antivirus

Tenable et Microsoft ne recommandent pas d'installer un antivirus, une EPP (plateforme de protection des terminaux) ou un logiciel EDR (Détection et réponse des terminaux) sur les contrôleurs de domaine (ou tout autre outil avec une console de gestion centrale). Si vous le faites, votre antivirus/EPP/EDR pourrait détecter et même bloquer ou supprimer les éléments requis pour la collecte des événements d'indicateur d'attaque (IoA) sur les contrôleurs de domaine.

Le script de déploiement de Tenable Identity Exposure pour les indicateurs d'attaque n'inclut pas de code malveillant et n'est même pas brouillé. Cependant, les détections occasionnelles sont normales, étant donné son utilisation de PowerShell et WMI, ainsi que la nature sans agent de l'implémentation.

Si vous rencontrez des problèmes tels que :

- Messages d'erreur lors de l'installation
- Détection de faux positifs ou de faux négatifs

Pour dépanner la détection des scripts d'installation par les antivirus :

1. Examinez les journaux de sécurité de votre antivirus/EPP/EDR pour vérifier si composants Tenable Identity Exposure sont détectés, bloqués ou supprimés. Un antivirus/EPP/EDR peuvent affecter les composants suivants :
    - Le fichier `ScheduledTasks.xml` dans la GPO Tenable Identity Exposure appliquée aux contrôleurs de domaine.
    - La tâche planifiée Tenable Identity Exposure sur les contrôleurs de domaine qui lance PowerShell.exe.
    - Le processus Tenable Identity Exposure `Register-TenableADEventsListener.exe` lancé sur les contrôleurs de domaine.
2. Ajoutez des exceptions de sécurité dans vos outils pour les composants affectés.
    - En particulier, la protection des terminaux Symantec peut détecter `CL.Downloader!gen27` pendant le processus d'installation de l'IoA. Vous pouvez ajouter ce risque connu spécifique à votre politique d'exceptions.
    - Une fois le planificateur de tâches configuré, exécutez PowerShell pour lancer le processus `Register-TenableADEventsListener.exe`. Le logiciel antivirus/EPP/EDR

peut potentiellement bloquer ce script PowerShell, entravant la bonne exécution des indicateurs d'attaque. Suivez attentivement ce processus et assurez-vous qu'il ne s'exécute qu'une seule fois sur tous les contrôleurs de domaine surveillés.

Exemples de chemins de fichier à exclure pour votre antivirus/EPP/EDR :

```
Register-TenableADEventsListener.exe process
 "\\"domain"\sysvol\"domain"\Policies\{"GUID_Tenable.ad}\Machine\IOA\Register-
TenableADEventsListener.exe"
```

```
ScheduledTasks.xml file
    C:\Users\<User Name>\AppData\Local\Temp\4\Tenable.ad\
{GUID}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    C:\Windows\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    \\[DOMAIN.FQDN]\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
```

Précédence des configurations avancées de stratégie d'audit

La stratégie de groupe (GPO) que Tenable Identity Exposure crée pour permettre la journalisation des événements requis est liée aux contrôleurs de domaine de l'unité d'organisation (UO) avec le mode « Enforced » (Appliqué).

Cela donne à la GPO une priorité élevée, mais une GPO appliquée configurée à un niveau supérieur (tel que domaine ou site) aura tout de même la précédence.

Si la GPO de priorité supérieure qui définit les paramètres de configuration avancée de stratégie d'audit est en conflit avec les besoins de Tenable Identity Exposure, elle prend le pas sur les autres et Tenable Identity Exposure ne reçoit pas les événements requis pour la détection d'attaque.

Comme Windows fusionne les paramètres de configuration avancée de stratégie d'audit définis par les GPO, différentes GPO peuvent définir différents paramètres.

Cependant, à chaque niveau de configuration, il n'utilise que la valeur définie par la GPO ayant la priorité la plus élevée. Par exemple, Tenable Identity Exposure a besoin des valeurs Succès et échec pour le paramètre Auditer la validation des informations d'identification. Toutefois, si une GPO avec une priorité plus élevée définit uniquement la réussite pour la propriété Auditer la

validation des informations d'identification, Windows ne collecte que les événements de réussite, et Tenable Identity Exposure ne voit pas les événements d'échec dont il a besoin.

Pour vérifier la précédence des GPO

1. Dans l'interface de ligne de commande, exécutez la commande suivante sur un contrôleur de domaine.

   Elle affiche la configuration avancée de stratégie d'audit appliquée après avoir pris en compte toutes les GPO et leur priorité.

   ```
   auditpol.exe /get /category:*
   ```

2. Comparez la sortie avec les exigences de stratégie d'audit avancée Tenable Identity Exposure. Pour chaque paramètre requis par Tenable Identity Exposure, vérifiez que la stratégie en vigueur le couvre également.

   - Que la stratégie en vigueur soit plus exhaustive, par exemple, lorsque Tenable Identity Exposure a besoin de « Succès » ou « Échec » et que le paramètre est « Succès et Échec », ne pose pas de problème.
   - Si la stratégie appliquée est insuffisante, cela signifie qu'une GPO avec une priorité plus élevée définit des paramètres en conflit.

Pour fixer la priorité d'une GPO :

1. Recherchez les GPO liées à des niveaux supérieurs (domaine ou site) en mode « appliqué » qui définissent la configuration avancée de stratégie d'audit.
2. Dans l'interface de ligne de commande, exécutez la commande suivante sur un contrôleur de domaine pour localiser la GPO prioritaire :

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. Modifiez le paramètre de configuration avancée de stratégie d'audit correspondant dans la GPO pour qu'elle réponde aux exigences minimales de Tenable Identity Exposure. Par exemple :

- Si Tenable Identity Exposure nécessite « Succès » et que la GPO de priorité la plus élevée définit « Échec », remplacez la valeur par « Succès et Échec ».
- Si Tenable Identity Exposure nécessite « Succès et Échec » et que la GPO ayant la priorité la plus élevée définit « Succès », remplacez la valeur par « Succès et Échec ».

4. Après avoir modifié le paramètre, vous pouvez attendre que la GPO mise à jour s'applique ou forcer son application avec la commande `gpupdate`.
5. Répétez la procédure « Pour vérifier la précédence des GPO » pour vérifier la nouvelle stratégie en vigueur.

Validation de l'observateur des journaux d'événements

Le script d'installation de l'indicateur d'attaque configure un observateur d'événements et un producteur/consommateur WMI (Windows Management Instrumentation) dans la mémoire de la machine. WMI est un composant Windows qui fournit des informations sur le statut des systèmes informatiques locaux ou distants.

Pour vérifier que l'inscription WMI est correcte :

- Dans PowerShell, exécutez la commande suivante :

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter
= ""__EventFilter.name='AlsidForAD-Launcher'"""
```

- S'il existe au moins un consommateur, vous obtenez ce type de sortie :

```
> Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter
"Filter = ""__EventFilter.name='AlsidForAD-Launcher'"""


__GENUS                 : 2
__CLASS                 : __FilterToConsumerBinding
__SUPERCLASS            : __IndicationRelated
__DYNASTY               : __SystemClass
__RELPATH               : __
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name=\"AlsidForAD-Launcher\"",F
                            ilter="__EventFilter.Name=\"AlsidForAD-Launcher\""
__PROPERTY_COUNT        : 7
__DERIVATION            : {__IndicationRelated, __SystemClass}
__SERVER                : DC-999
__NAMESPACE             : ROOT\subscription
__PATH                  : \\DC-999\ROOT\subscription:__
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name
```

```
                          =\"AlsidForAD-Launcher\"",Filter="__EventFilter.Name=\"AlsidForAD-
Launcher\""
Consumer                : ActiveScriptEventConsumer.Name="AlsidForAD-Launcher"
CreatorSID              : {1, 1, 0, 0...}
DeliverSynchronously    : False
DeliveryQoS             :
Filter                  : __EventFilter.Name="AlsidForAD-Launcher"
MaintainSecurityContext : False
SlowDownProviders       : False
PSComputerName          : DC-999
```

- S'il n'existe pas de consommateur WMI enregistré, la commande ne retourne rien.
- Il s'agit d'une condition préalable pour que le processus s'exécute sur le contrôleur de domaine pour WMI.

Pour récupérer l'observateur des journaux d'événements (pour les versions = ou > 3.29) :

- Dans PowerShell, exécutez la commande suivante :

```
gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}
```

- Exemple de résultat valide :

```
PS C:\IOAInstall> gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}

ProcessId Name                                HandleCount WorkingSetSize VirtualSize

5748      Register-TenableADEventsListener.exe 152         4096000        4384534528
```

Pour récupérer le processus WMI (pour les versions = ou < 3.19) :

- Dans PowerShell, exécutez la commande suivante :

```
gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

- Exemple de résultat valide :

```
> gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}

ProcessId Name           HandleCount WorkingSetSize VirtualSize
--------- ----           ----------- -------------- -----------
952       powershell.exe 502         26513408       2199678185472
```

Fichiers journaux Tenable Identity Exposure

Si vous ne voyez toujours pas d'alertes d'indicateurs d'attaque après avoir validé la GPO et le consommateur WMI, vous pouvez consulter les journaux internes de Tenable Identity Exposure.

Journal Ceti

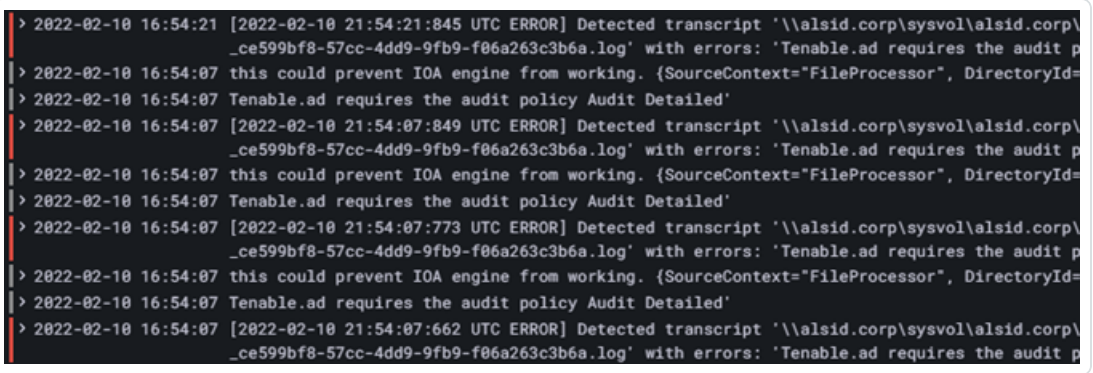
- Vérifiez le message d'erreur suivant dans le journal CETI :

```
[2022-02-22 22:23:27:570 UTC WARNING] Some domain controllers are not generating IOA
events: 'CORP-DC'. {SourceContext="DirectoryEventToCetiAdObjectMessageMapper",
DirectoryId=2, Dns="corp.bank.com", Host="10.10.20.10", Source=SYSVOL, Version="3.11.5"}
```

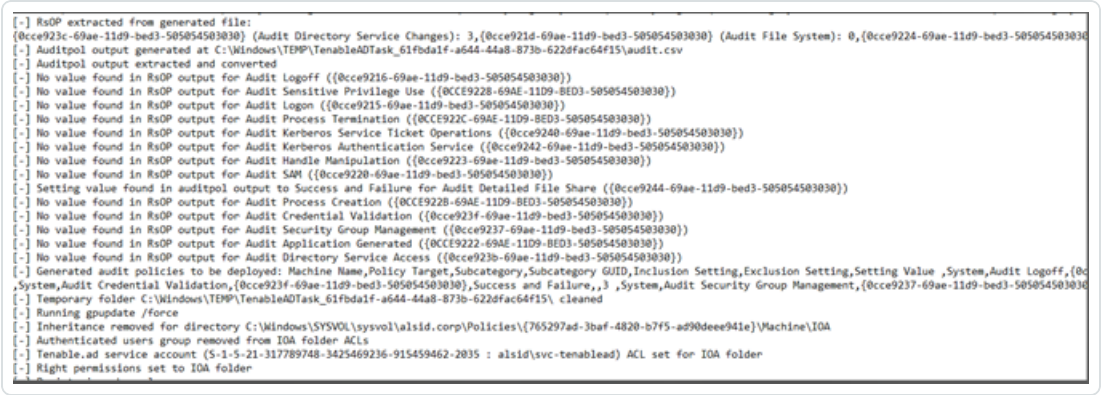
- Si vous voyez ce message, vérifiez que les paramètres GPO et le consommateur WMI sont exécutés sur le contrôleur de domaine (DC) indiqué dans le message d'erreur ci-dessus.

Paramètres d'audit

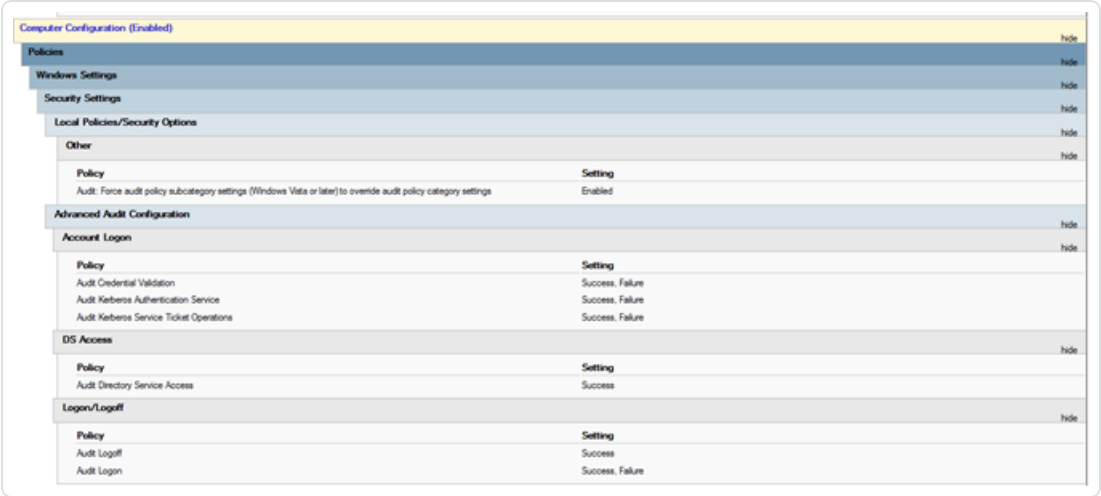
- Si vous constatez une erreur similaire à : « Tenable Identity Exposure requires the Audit Policy… » (Tenable.ad nécessite la stratégie d'audit...), vérifiez vos GPO existantes pour vous assurer que vous n'avez pas défini les stratégies d'audit requises sur « No Auditing » (Pas d'audit).



- Si vous obtenez une erreur « RSOP... » :



- Vérifiez les stratégies d'audit et consultez le fichier de transcription dans le dossier SYSVOL pour déterminer si des problèmes se sont produits lors de l'installation.



Journal Cygni

Cygni enregistre l'attaque et indique le fichier `.gz` spécifique que Tenable Identity Exposure a appelé pour générer l'alerte.

I-DCSync

```
2022-03-15 11:39:31
[2022-03-15 15:39:30:759 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCSync' and Event '110052' {SourceContext="AttackEngine", CodeName="I-DCSync", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-GoldenTicket

```
2022-03-15 11:40:31
[2022-03-15 15:40:31:490 UTC INFORMATION] Anomaly 'Logon' has been raised for Indicator 'I-
GoldenTicket' and Event '110061' {SourceContext="AttackEngine", CodeName="I-GoldenTicket",
ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ProcessInjectionLsass

```
022-03-15 12:47:09
[2022-03-15 16:47:09:811 UTC INFORMATION] Anomaly 'ProcessAccess' has been raised for Indicator 'I-
ProcessInjectionLsass' and Event '115948' {SourceContext="AttackEngine", CodeName="I-
ProcessInjectionLsass", ProfileId=1, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-DC Shadow

```
2022-03-15 11:30:30
[2022-03-15 15:30:30:657 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCShadow' and Event '109948' {SourceContext="AttackEngine", CodeName="I-DCShadow", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-BruteForce

```
2022-03-15 08:02:11
[2022-03-15 12:02:11:231 UTC INFORMATION] Anomaly 'An account failed to log on' has been raised for
Indicator 'I-BruteForce' and Event '109082' {SourceContext="AttackEngine", CodeName="I-BruteForce",
ProfileId=6, AdObjectId="3:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{765297AD-3BAF-4820-B7F5-
AD90DEEE941E}\\Machine\\IOA\\dc-vm-10.0.17763-8_.gz", Event.Id=0, Version="3.16.0"}
```

I-PasswordSpraying

```
2022-03-15 12:39:43
[2022-03-15 16:39:43:793 UTC INFORMATION] Anomaly 'An account failed to log on.' has been raised for
Indicator 'I-PasswordSpraying' and Event '115067' {SourceContext="AttackEngine", CodeName="I-
PasswordSpraying", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-PetitPotam

```
2022-03-15 12:43:02
[2022-03-15 16:43:02:737 UTC INFORMATION] Anomaly 'PetitPotamEFSError' has been raised for Indicator
'I-PetitPotam' and Event '115844' {SourceContext="AttackEngine", CodeName="I-PetitPotam",
ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ReconAdminsEnum

```
022-03-15 12:55:31
[2022-03-15 16:55:31:638 UTC INFORMATION] Anomaly 'LocalAdmin enumeration (BloodHound/SharpHound).
Version 2016+' has been raised for Indicator 'I-ReconAdminsEnum' and Event '116085'
{SourceContext="AttackEngine", CodeName="I-ReconAdminsEnum", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-Kerberoasting

```
022-03-15 12:51:30
[2022-03-15 16:51:30:236 UTC INFORMATION] Anomaly 'Kerberos TGS requested on honey account' has been
raised for Indicator 'I-Kerberoasting' and Event '116013' {SourceContext="AttackEngine", CodeName="I-
Kerberoasting", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-
7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-NtdsExtraction

```
2022-03-15 12:03:51
[2022-03-15 16:03:50:949 UTC INFORMATION] Anomaly 'Shadow copy created on 2012 and above' has been
raised for Indicator 'I-NtdsExtraction' and Event '111168' {SourceContext="AttackEngine",
CodeName="I-NtdsExtraction", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

Journal Cephei

Les entrées de journal suivantes confirment que Cephei écrit des attaques. La valeur de la clé est l'**assetTypeID** qui spécifie le type d'attaque que vous pouvez utiliser pour assurer la corrélation avec les entrées Cygni :

I-DCSync attackTypeID:1

```
2022-03-15 11:39:52
2022-03-15T15:39:52.037023041Z stdout F [2022-03-15 15:39:52:035 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 32.16 ms : Request Body=
{"timestamp":"1647358722449","directoryId":5,"profileId":4,"attackTypeId":1,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-GoldenTicket attackTypeID:2

```
2022-03-15 11:40:52
2022-03-15T15:40:52.084931986Z stdout F [2022-03-15 15:40:52:084 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.6607 ms : Request Body=
{"timestamp":"1647358773608","directoryId":5,"profileId":4,"attackTypeId":2,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ProcessInjectionLsass attackTypeID:3

```
2022-03-15 12:47:52
2022-03-15T16:47:52.29927328Z stdout F [2022-03-15 16:47:52:298 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 35.7532 ms : Request Body=
{"timestamp":"1647362812784","directoryId":5,"profileId":1,"attackTypeId":3,"count":2}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-DCShadow attackTypeID:4

```
2022-03-15 11:30:52
2022-03-15T15:30:51.949399295Z stdout F [2022-03-15 15:30:51:944 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.2605 ms : Request Body=
{"timestamp":"1647358182800","directoryId":5,"profileId":3,"attackTypeId":4,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-BruteForce attackTypeID:5

```
2022-03-15 08:02:54
2022-03-15T12:02:54.698814039Z stdout F [2022-03-15 12:02:54:698 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 30.7623 ms : Request Body=
{"timestamp":"1647345728023","directoryId":3,"profileId":6,"attackTypeId":5,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PasswordSpraying attackTypeID:6

```
2022-03-15 12:39:52
2022-03-15T16:39:52.187309945Z stdout F [2022-03-15 16:39:52:186 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.9422 ms : Request Body=
{"timestamp":"1647362356837","directoryId":5,"profileId":4,"attackTypeId":6,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PetitPotam attackTypeID:7

```
022-03-15 12:43:52
2022-03-15T16:43:52.226125918Z stdout F [2022-03-15 16:43:52:223 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 15.8402 ms : Request Body=
{"timestamp":"1647362570534","directoryId":5,"profileId":1,"attackTypeId":7,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ReconAdminsEnum attackTypeID:8

```
2022-03-15 12:55:52
2022-03-15T16:55:52.399889635Z stdout F [2022-03-15 16:55:52:399 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 40.6632 ms : Request Body=
{"timestamp":"1647363305295","directoryId":5,"profileId":4,"attackTypeId":8,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-Kerberoasting attackTypeID:10

```
2022-03-15 12:51:52
2022-03-15T16:51:52.352432644Z stdout F [2022-03-15 16:51:52:351 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.0547 ms : Request Body=
{"timestamp":"1647363026345","directoryId":5,"profileId":4,"attackTypeId":10,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-NtdsExtraction attackTypeID:11

```
022-03-15 12:03:52
2022-03-15T16:03:52.137547488Z stdout F [2022-03-15 16:03:52:137 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 13.0304 ms : Request Body=
{"timestamp":"1647360224606","directoryId":5,"profileId":4,"attackTypeId":11,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

Journal Electra

Vous devez voir l'entrée suivante :

[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-alert (namespace=electra)

```
[2022-03-15T14:04:39.151Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-
alert (namespace=electra)
[2022-03-15T14:04:39.168Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Sending ws message to listeners.
alertIoA (namespace=electra)
```

Journal Eridanis

Vous devez voir l'entrée suivante :

```
022-03-15T14:04:39.150Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2010 200
122 - 7ms (namespace=hapi)
[2022-03-15T14:04:39.165Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: notifyAttackAndAttackAlertCreation
success { attackId: 2011 } (namespace=eridanis)
[2022-03-15T14:04:39.170Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2011 200
122 - 6ms (namespace=hapi)
```

Atténuation des problèmes liés à la réplication DFS

Dans le script de déploiement de l'indicateur d'attaque, un paramètre supplémentaire (`-EventLogsFileWriteFrequency X`) vous permet de résoudre les problèmes potentiels de lenteur ou d'interruption de la réplication dans le système de fichiers distribués (DFS).

Ce paramètre est facultatif. Tenable recommande de ne l'utiliser que si vous rencontrez des problèmes de réplication DFS ou que vous en avez remarqués depuis le déploiement du script IoA. Dans des conditions normales, le paramètre conserve sa valeur par défaut, et vous n'avez pas besoin de l'inclure dans la ligne de commande lors de l'exécution du script.

Dans quelles circonstances modifier le paramètre

La valeur [X] du paramètre `-EventLogsFileWriteFrequency X` désigne l'intervalle auquel l'écouteur Tenable Identity Exposure génère un fichier de journaux d'événements sur les contrôleurs de domaine (DC) non-PDCe. La valeur par défaut et recommandée, utilisée par l'écouteur Tenable Identity Exposure, est de 15 secondes. Cependant, la valeur personnalisée ne s'applique pas aux DC PDCe, et la valeur d'intervalle par défaut de 15 secondes est utilisée pour que les fonctionnalités de détection d'attaque soient totalement opérationnelles. Tenable recommande d'utiliser ce paramètre et d'augmenter sa valeur par défaut de 15 secondes à

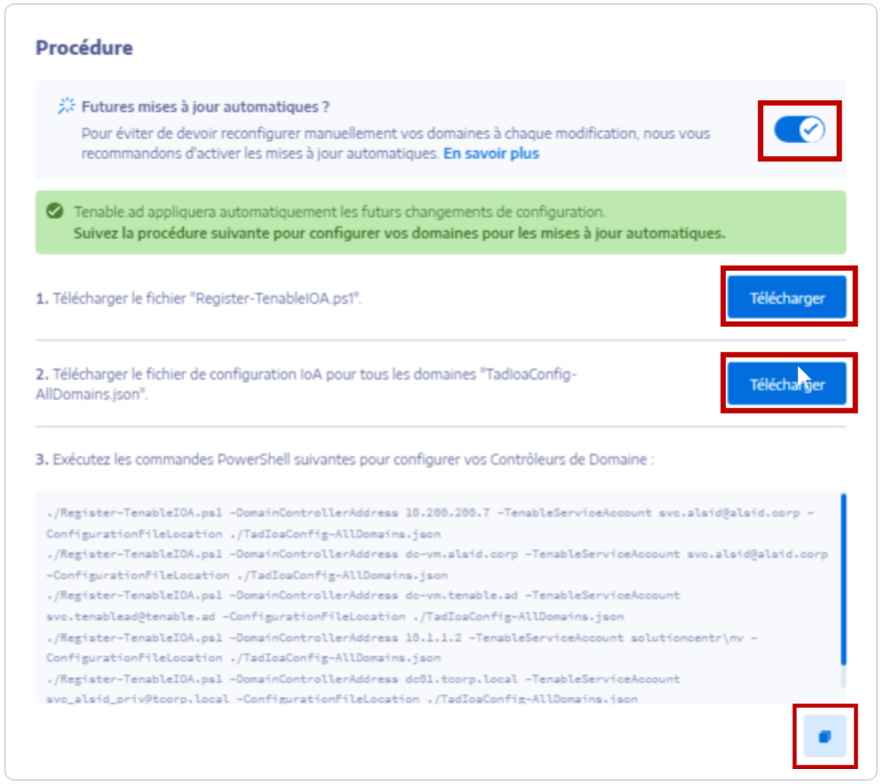
300 secondes (5 minutes) maximum uniquement si votre infrastructure est sujette à des problèmes de réplication DFS.

Recommandations

Notez que l'augmentation de l'intervalle d'écriture du fichier journal des événements générera le fichier moins souvent. Autrement dit, le délai de détection d'attaque va augmenter (par exemple, si le fichier est généré toutes les 30 secondes et non pas toutes les 15 secondes comme c'est le cas par défaut sur les CD non-PDCe). De plus, l'augmentation du délai augmente la taille des fichiers journaux d'événements générés dans les limites définies dans Modifications techniques et impact potentiel. Par conséquent, utilisez ce paramètre uniquement comme stratégie d'atténuation et non pas pour remplacer l'examen des problèmes de réplication DFS.

Pour appliquer le paramètre :

1. Configurez vos domaines pour les IoA comme décrit dans la procédure. Pour plus d'informations, voir Installer des indicateurs d'attaque.



2. Ouvrez un terminal PowerShell avec des droits d'administration.

3. Exécutez le script pour configurer vos contrôleurs de domaine pour les IoA et ajoutez le paramètre `X -EventLogsFileWriteFrequency X`, où [X] est l'intervalle que vous souhaitez définir pour les fichiers des journaux d'événements.

Rétention du journal des événements Windows

Bien que Tenable Identity Exposure s'efforce de traiter autant de journaux d'événements Windows que possible pour prendre en charge l'analyse de sécurité au sein de la fonction Indicateur d'attaque, il existe des limitations techniques, telles que la mémoire disponible sur la machine qui exécute les services.

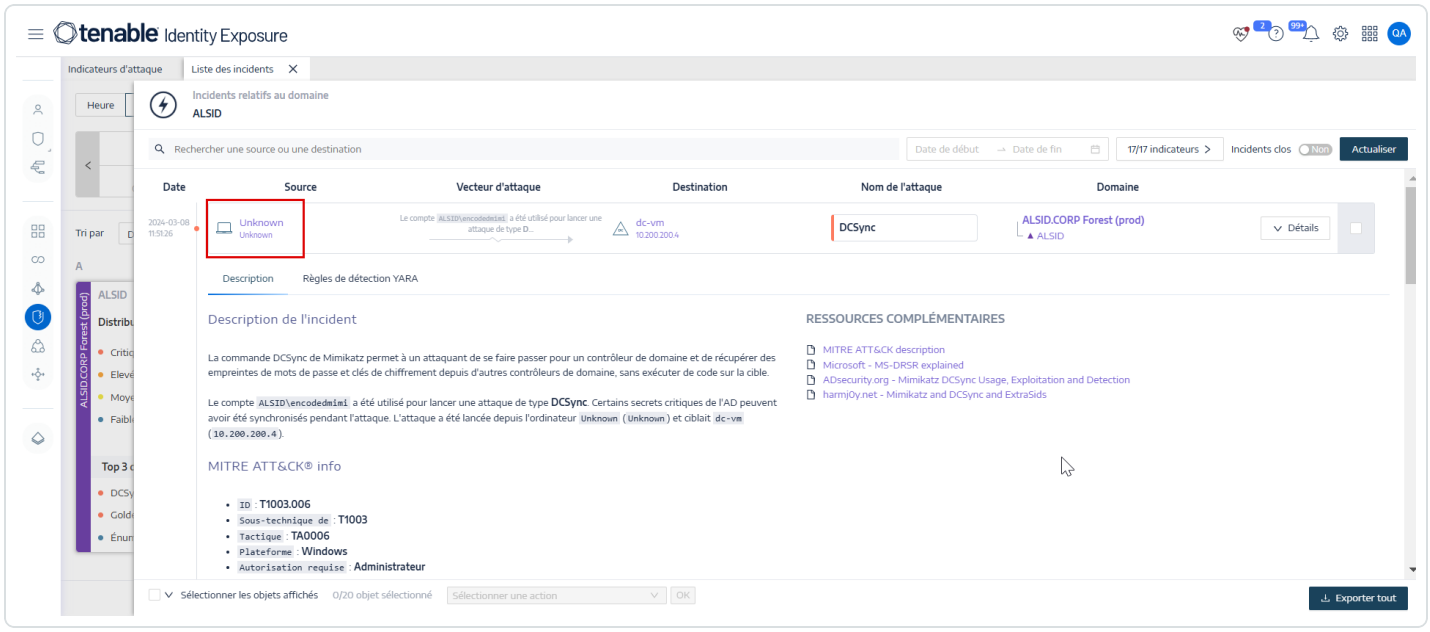
La **période de rétention globale par défaut** est de 5 minutes. Cependant, des journaux d'événements Windows spécifiques ont des périodes de rétention prolongées pour atténuer les problèmes de corrélation que le moteur de sécurité peut rencontrer :

- `SYSMON 5722` et `5723` : conservés pendant 6 heures.
- `Microsoft-Windows-security-auditing/4624` : la période de rétention de ce journal est dynamique, car il est fortement utilisé dans les indicateurs d'attaque pour la détection et la corrélation. Le système ajuste la rétention en fonction de l'utilisation de la mémoire pour équilibrer le traitement des événements avec les ressources système :
    - **Première heure** : le service d'analyse de sécurité applique la période de rétention par défaut de 5 minutes.
    - **Après la première heure**, le système évalue la mémoire restante et ajuste la rétention comme suit :
        - Si la mémoire disponible est **supérieure à 50 %** : 1 jour.
        - Si la mémoire disponible est de **35 % à 50 %** : 6 heures.
        - Si la mémoire disponible est de **20 % à 35 %** : 1 heure.
        - Si la mémoire disponible est de **10 % à 20 %** : 10 minutes.
        - Si la mémoire disponible est **inférieure à 10 %** : 5 minutes par défaut.

Cette approche dynamique garantit que le système peut gérer efficacement les événements entrants tout en conservant une mémoire adéquate pour l'analyse de sécurité.

Entrées de type « Inconnu » dans les alertes d'indicateurs d'attaque

Dans certains cas, vous pouvez rencontrer des entrées « Inconnu » dans les alertes d'indicateurs d'attaque (IoA), comme illustré sur l'image suivante :



Ces entrées sont généralement dues aux scénarios clés suivants :

1. **DNS externe en dehors d'Active Directory (AD)**

   Si votre organisation utilise des serveurs DNS en dehors du domaine Active Directory (AD), notez que le produit ne prend pas en charge les environnements DNS non AD. Autrement dit, lorsque certaines requêtes ou demandes DNS sont acheminées par des serveurs DNS externes qui ne font pas partie d'AD, Tenable Identity Exposure ne peut pas les identifier, ce qui entraîne des entrées libellées « Inconnu » dans la liste des alertes IoA.

   De telles « inconnues » sont normales dans ces situations et n'indiquent aucun dysfonctionnement ni aucune erreur au sein de Tenable Identity Exposure. Cela est dû à la nature de l'intégration avec Active Directory, qui nécessite que les enregistrements DNS soient gérés au sein de l'environnement AD pour assurer une visibilité et un suivi complets.

   Solution

   - Pour minimiser l'apparition de ces entrées « Inconnu », assurez-vous que votre infrastructure DNS est entièrement intégrée à AD pour les domaines et les ressources indispensables à la surveillance de l'exposition des identités.

- Si les requêtes DNS doivent sortir d'AD, sachez simplement que les libellés « Inconnu » continueront d'apparaître, car Tenable Identity Exposure ne peut pas les résoudre.

2. **Autorisations insuffisantes pour le compte Tenable Identity Exposure**

   Une autre raison de la présence d'entrées de type « Inconnu » dans les alertes IoA pourrait être que le compte utilisé par Tenable Identity Exposure ne dispose pas des autorisations suffisantes pour lire les entrées DNS. Le service Tenable Identity Exposure nécessite des autorisations de lecture pour accéder aux enregistrements DNS dans Active Directory et les analyser correctement.

   Solutions

   Pour résoudre ce problème, assurez-vous que le compte utilisé par Tenable Identity Exposure bénéficie d'un accès en lecture aux entrées DNS nécessaires dans AD. Plus précisément, ce compte doit être autorisé à interroger les serveurs DNS et à accéder aux enregistrements dont il a besoin pour effectuer une analyse d'exposition des identités.

   Si le compte Tenable Identity Exposure ne dispose pas des autorisations de lecture appropriées, vous pouvez les lui accorder en suivant les procédures suivantes.

   > Conseil : dans le script, vous devez uniquement modifier le nom du compte utilisé par Tenable Identity Exposure. Les autorisations de lecture sont incluses dans les attributs suivants :
   >
   > - `distinguishedName`
   > - `dnsRecord (contient l'adresse IP)`
   > - `name`
   > - `ntSecurityDescriptor`
   > - `objectCategory`
   > - `objectClass`
   > - `objectGUID`

   Vous disposez des **deux** options suivantes pour utiliser des scripts PowerShell :

   a. Dans Active Directory Manager, définissez les autorisations de lecture sur le conteneur (`dnsZone`) et propagez-le à tous les enfants `dnsNode` (solution recommandée le cas

échéant) :

```
Import-Module ActiveDirectory

$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }

# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-
00c04fb96050')

$dnsZones = Get-ADObject -LDAPFilter "(objectClass=dnsZone)" -SearchBase
$dnsZonePartition

ForEach ($dnsZone in $dnsZones) {
    $acl = Get-Acl -Path "AD:\$dnsZone"

    ForEach ($guid in $guids) {
      $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [guid]$guid,
        [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
        [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
        )

      $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
        [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
        )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsZone" -AclObject $acl
}
```

b. Définissez les autorisations de lecture sur tous les objets `dnsNode` existants (sur la `dnsZone` affectant tous les dnsNode enfants) :

```
Import-Module ActiveDirectory

$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
```

```
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }

# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-
00c04fb96050')

$dnsNodes = Get-ADObject -LDAPFilter "(objectClass=dnsNode)" -SearchBase
$dnsZonePartition

ForEach ($dnsNode in $dnsNodes) {
    $acl = Get-Acl -Path "AD:\$dnsNode"

    ForEach ($guid in $guids) {
      $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [guid]$guid
        )

      $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow
        )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsNode" -AclObject $acl
}
```

3. **Partitions DNS prises en charge**

   Tenable Identity Exposure n'effectue pas de résolution DNS active. Au lieu de cela, il s'appuie sur des entrées DNS extraites des partitions `ForestDnsZones` et `DomainDnsZones`. Si vous utilisez des partitions DNS personnalisées, Tenable Identity Exposure ne les analysera pas et ne stockera pas leurs entrées DNS.

Indicateurs d'attaque opérationnels

Il est essentiel de s'assurer que les processus des indicateurs d'attaque fonctionnent correctement pour garantir la précision de la détection et de la réponse. Cette section fournit des instructions pas à pas pour vérifier que les composants des IoA sont opérationnels, résoudre les difficultés courantes et corriger efficacement les problèmes. Suivez les étapes ci-dessous pour vérifier que tout fonctionne comme prévu.

- Assurez-vous que la surveillance des indicateurs d'attaque (IoA) est opérationnelle sur vos contrôleurs de domaine.
    - Vérifiez la connectivité au domaine – Assurez-vous que la connectivité au domaine est fonctionnelle en vérifiant la configuration. Pour plus d'informations, voir Domaines.
- Vérifiez le dossier de la GPO de l'IoA dans SYSVOL :
    - Vérifiez le dossier de la GPO de l'IoA dans le répertoire SYSVOL pour confirmer que chaque contrôleur de domaine produit un fichier `.gz` à jour.
    - Si un contrôleur de domaine ne génère pas ce fichier `.gz` , passez aux étapes suivantes.
- Vérifiez que le processus de l'observateur d'événements IoA est en cours d'exécution :
    - Vérifiez que le processus `Register-TenableADEventsListener.exe` est en cours d'exécution.
    - Dans les dernières versions, outre `Register-TenableADEventsListener.exe`, ce processus est répertorié comme « Tenable - IOA Events Listener » dans le gestionnaire de tâches.

      Pour plus d'informations, voir Validation de l'observateur des journaux d'événements.
- Si le processus n'est pas en cours d'exécution :
    - Assurez-vous qu'un logiciel EDR/antivirus présent sur les contrôleurs de domaine ne bloque pas le processus `Register-TenableADEventsListener.exe`.

      Pour plus d'informations, voir Détection antivirus.
- Lancez le processus manuellement :
    - Modifiez la tâche associée (`TenableADTask_*`) dans le planificateur de tâches et cliquez sur **OK** pour redémarrer le processus.
- Faites remonter le problème s'il persiste – Si les étapes ci-dessus ne permettent pas de résoudre le problème, déposez une demande d'assistance auprès de Tenable. Un problème sous-jacent empêche peut-être l'exécution du processus `Register-TenableADventsListener.exe`.

Délais de détection des indicateurs d'attaque

Tenable Identity Exposure ajuste automatiquement la fenêtre d'analyse lorsqu'il détecte des pertes ou des retards d'événements, provoqués notamment par la longueur de la réplication des fichiers GZ ou le volume élevé de données générées.

Il analyse généralement les données dans des fenêtres de 5 minutes, mais il peut étendre la fenêtre jusqu'à une heure pour prendre en compte les événements arrivés en retard. Cet ajustement peut retarder la détection d'une attaque jusqu'à une heure après qu'elle ait eu lieu.

Authentification

Un utilisateur Tenable Identity Exposure peut être authentifié de différentes manières :

- Authentification à l'aide d'un compte Tenable Identity Exposure
- Authentification à l'aide de LDAP
- Authentification à l'aide de SAML

Authentification à l'aide de Tenable One

Licence requise : Tenable One

Remarque : avec une licence Tenable One, vous gérez tous vos paramètres d'authentification dans Tenable Vulnerability Management. Pour plus d'informations, voir Contrôle d'accès dans le *Guide de l'utilisateur Tenable Vulnerability Management*.

Pour configurer l'authentification à l'aide de Tenable One :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration**.

   Le volet Configuration apparaît.

2. Dans la section **Authentification**, cliquez sur **Tenable One**.

3. Dans la zone déroulante **Profil par défaut**, sélectionnez le profil de l'utilisateur.

4. Dans la zone **Rôles par défaut**, sélectionnez les rôles de l'utilisateur.

   Conseil : les utilisateurs authentifiés dans Tenable One qui ne se sont pas préalablement connectés à Tenable Identity Exposure reçoivent automatiquement un compte lorsqu'ils se connectent à Tenable Identity Exposure. Le profil et le rôle par défaut sont automatiquement appliqués à

l'utilisateur. **Exception** : les utilisateurs ayant le rôle « Administrateur » dans Tenable Vulnerability Management ont également le rôle « Administrateur global » dans Tenable Identity Exposure.

5. Cliquez sur **Enregistrer**.

Authentification à l'aide d'un compte Tenable Identity Exposure

La méthode d'authentification la plus simple consiste à utiliser un compte Tenable Identity Exposure qui nécessite un nom d'utilisateur et un mot de passe.

Cette méthode d'authentification propose une stratégie de verrouillage par défaut, un contrôle de sécurité destiné à atténuer les attaques par force brute contre les mécanismes d'authentification. Elle verrouille les comptes utilisateur après trop grand nombre de tentatives de connexion infructueuses. Lorsqu'un compte est verrouillé, les utilisateurs n'ont pas accès aux API Tenable Identity Exposure.

Pour configurer l'authentification en utilisant un compte Tenable Identity Exposure :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration**.

   Le volet Configuration apparaît.

2. Dans la section **Authentification**, cliquez sur **Tenable Identity Exposure**.
3. Dans la zone déroulante **Profil par défaut**, sélectionnez le profil de l'utilisateur.
4. Dans la zone **Rôles par défaut**, sélectionnez les rôles de l'utilisateur.
5. Configurez les paramètres de la politique de verrouillage :

Paramètre	Description	Valeur par défaut
Activé	• **Activé** – Tenable Identity Exposure verrouille le compte après un nombre défini de tentatives de connexion infructueuses. • **Désactivé**– Tenable Identity Exposure ne	Activé

	verrouille pas le compte après des tentatives de connexion infructueuses.	
Durée de verrouillage	Durée pendant laquelle Tenable Identity Exposure empêche le compte de se connecter. Tenable Identity Exposure déverrouille automatiquement le compte après ce délai pour permettre à l'utilisateur de se connecter à nouveau. Pour configurer la durée du verrouillage : 1. Cliquez sur le curseur pour définir une durée du verrouillage. 2. Sélectionnez **Infinie** si vous ne souhaitez pas déverrouiller le compte automatiquement après une durée définie. **Remarque** : si tous les comptes du groupe « Administrateur global » sont verrouillés, Tenable Identity Exposure déverrouille le compte d'administrateur par défaut après 10 secondes.	300 secondes
Nombre de tentatives avant verrouillage	Nombre de tentatives de connexion infructueuses avant que Tenable Identity Exposure ne verrouille le compte.	3
Période de rédemption	Période pendant laquelle Tenable Identity Exposure compte le nombre de tentatives de connexion infructueuses. Après un nombre spécifié de tentatives de connexion infructueuses, Tenable Identity Exposure verrouille le compte. Pour définir une période de rédemption :	900 secondes

	1. Cliquez sur le curseur pour définir une période. 2. Sélectionnez « Infinie » si vous ne souhaitez pas définir de période de comptabilisation des tentatives de connexion infructueuses avant que Tenable Identity Exposure verrouille le compte.	

6. Cliquez sur **Enregistrer**.

Pour désactiver la politique de verrouillage :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration**.

   Le volet Configuration apparaît.

2. Cliquez sur le curseur **Activé** pour désactiver la stratégie de verrouillage.

Remarque : si vous désactivez la politique de verrouillage, les comptes utilisateur verrouillés peuvent tenter de se reconnecter.

Pour afficher la liste des comptes verrouillés :

- Dans Tenable Identity Exposure, accédez à **Comptes** > **Gestion des comptes utilisateur**.

  Dans la liste des utilisateurs, Tenable Identity Exposure affiche les comptes verrouillés ayant une icône de cadenas rouge. Tenable Identity Exposure affiche le message suivant à l'attention des utilisateurs dont les comptes sont verrouillés : « Votre compte est bloqué en raison d'un trop grand nombre de tentatives d'authentification échouées. Veuillez contacter un administrateur ».

Pour déverrouiller un compte :

Vous devez disposer des autorisations appropriées de modification des utilisateurs pour déverrouiller des comptes.

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des comptes utilisateur**.

   Le volet Gestion des comptes utilisateur apparaît.

2. Dans la liste des utilisateurs, localisez le compte verrouillé.

3. Cliquez sur l'icône de crayon pour modifier le compte utilisateur verrouillé.

   Le volet des informations de l'utilisateur apparaît.

4. Cliquez sur le bouton **Supprimer le verrouillage**.

Pour accorder aux rôles utilisateur l'autorisation de configurer la stratégie de verrouillage :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des rôles**.

   Le volet **Gestion des rôles** apparaît.

2. Cliquez sur l'icône de crayon à côté d'un nom de rôle pour modifier le rôle.

   Le volet **Modifier un rôle** apparaît.

3. Cliquez sur l'onglet **Entités de type Configuration système**.

4. Sous la section **Gestion des autorisations**, cochez la case **Stratégie de verrouillage des comptes**.

5. Cliquez sur le curseur pour activer **Interdit** ou **Autorisé**.

   Un message confirme que Tenable Identity Exposure a mis à jour les autorisations de l'utilisateur.

   > **Remarque** : Tenable Identity Exposure désactive les paramètres de stratégie de verrouillage pour les utilisateurs qui n'ont qu'une autorisation de lecture dans ce volet.

Authentification à l'aide de LDAP

Tenable Identity Exposure vous permet de vous authentifier à l'aide du protocole Lightweight Directory Access Protocol (LDAP).

Pour activer l'authentification LDAP, vous devez disposer des éléments suivants :

- Un compte de service pré-configuré avec un utilisateur et un mot de passe pour accéder à Active Directory.
- Un groupe Active Directory pré-configuré.

Après avoir configuré l'authentification LDAP, l'option LDAP apparaît dans un onglet sur la page de connexion.

Pour configurer l'authentification LDAP :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration**.

   Le volet Configuration apparaît.

2. Dans la section **Authentification**, cliquez sur **LDAP**.
3. Cliquez sur le curseur **Activer l'authentification LDAP** pour activer l'option « activé ».

   Un formulaire d'informations LDAP apparaît.

4. Fournissez les informations suivantes :

   - Dans la zone **Adresse du serveur LDAP**, saisissez l'adresse IP du serveur LDAP commençant par `ldap://` et se terminant par le nom de domaine et le numéro de port.

     > **Remarque** : si vous utilisez un serveur LDAPS, saisissez son adresse commençant par `ldaps://` et se terminant par le nom de domaine et le numéro de port. Utilisez cette procédure pour effectuer la configuration de LDAPS.

   - Dans la zone **Compte de service utilisé pour interroger le serveur LDAP**, saisissez le nom distinctif (DN), SamAccountName ou UserPrincipalName que vous utilisez pour accéder au serveur LDAP.
   - Dans la zone **Mot de passe du compte de service**, saisissez le mot de passe du compte de service.
   - Dans la zone **Préfixe LDAP pour la recherche**, saisissez l'annuaire LDAP que Tenable Identity Exposure utilise pour rechercher les utilisateurs qui tentent de se connecter, commençant par `DC=` ou `OU=`. Il peut s'agir d'un répertoire racine ou d'une unité d'organisation spécifique.

- Dans la zone **Filtre de recherche LDAP**, saisissez l'attribut que Tenable Identity Exposure utilise pour filtrer les utilisateurs. L'attribut `sAMAccountname={{login}}` est un attribut standard pour l'authentification dans Active Directory. La valeur de `login` est celle que fournit l'utilisateur au moment de l'authentification.

5. Pour **activer les liaisons SASL**, effectuez l'une des actions suivantes :

   - Si vous utilisez `SamAccountName` pour le compte de service, cliquez sur le curseur **Activer les liaisons SASL** pour le passer sur **activé**.
   - Si vous utilisez le `Nom distinctif` ou `UserPrincipalName` pour le compte de service, laissez les options **Activer les liaisons SASL désactivées**.

     > **Remarque importante pour Windows Server 2025** :
     >
     > **Windows Server 2025** présente une limitation à cause de laquelle une configuration LDAP avec les liaisons SASL désactivées **ne fonctionne que si LDAPS est activé.**
     >
     > Pour que la configuration fonctionne comme prévu :
     >
     > - Si vous utilisez l'**UPN** ou le **DN** pour le compte de service Tenable, vous pouvez **activer les liaisons SASL** dans la configuration LDAP pour obtenir le comportement attendu.
     > - Si vous préférez **garder les liaisons SASL désactivées**, vous devez **activer LDAPS** pour que LDAP fonctionne correctement.

6. Sous la section **Profil et rôles par défaut**, cliquez sur **Ajouter un groupe LDAP** pour spécifier les groupes autorisés à s'authentifier.

   Un formulaire d'information sur les groupes LDAP apparaît.

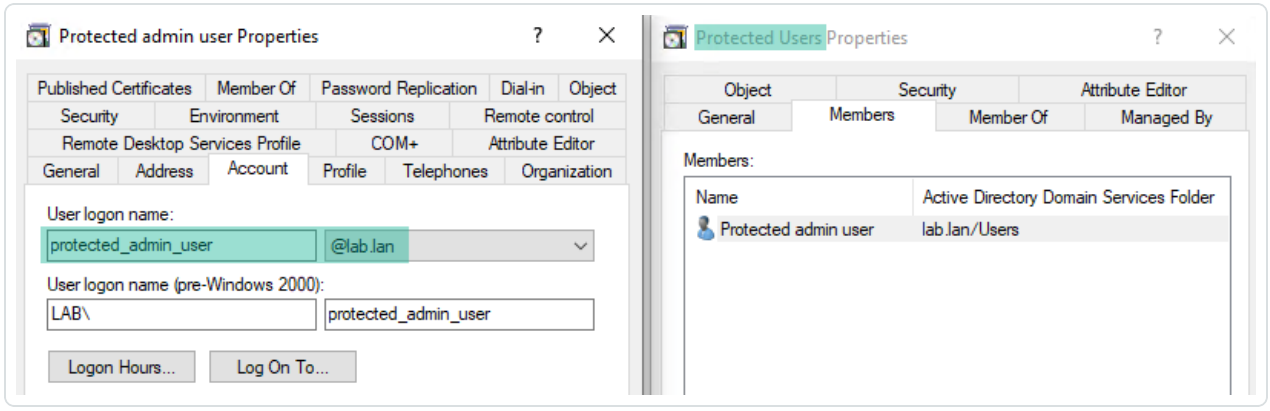
   - Dans la zone **Nom du groupe LDAP**, saisissez le nom distinctif du groupe (exemple : `CN=TAD_User,OU=Groupes,DC=Tenable,DC=ad`)
   - Dans la zone déroulante **Profil par défaut**, sélectionnez le profil du groupe autorisé.
   - Dans la zone **Rôles par défaut**, sélectionnez les rôles du groupe autorisé.

7. Si nécessaire, cliquez sur l'icône **+** pour ajouter un nouveau groupe autorisé.
8. Cliquez sur **Enregistrer**.

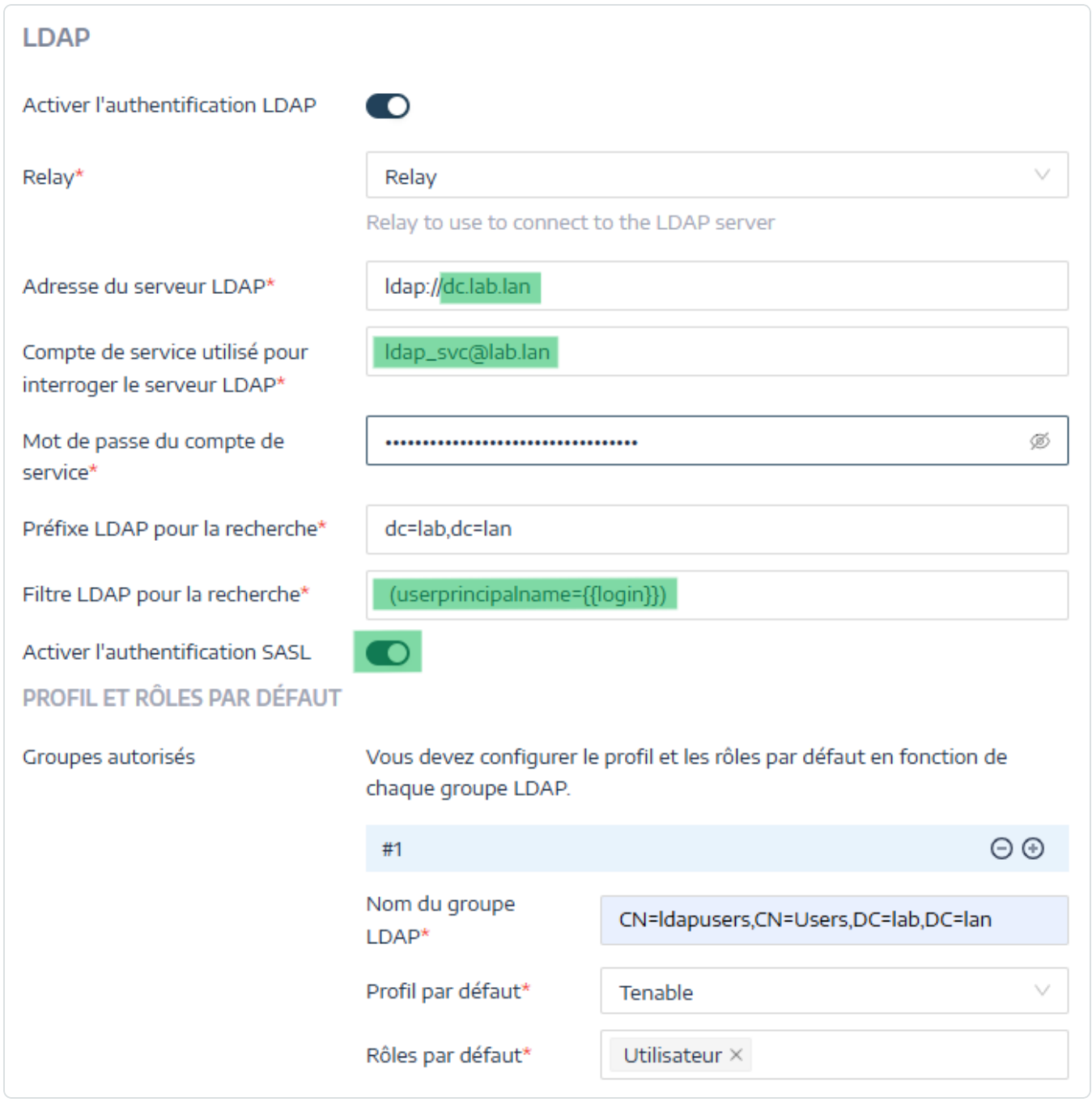
Pour utiliser LDAP avec les membres du groupe « Protected Users » dans AD :

Étant donné que les membres du groupe Protected Users ne peuvent pas utiliser NTLM, vous devez veiller à configurer correctement l'authentification LDAP pour utiliser Kerberos à la place.

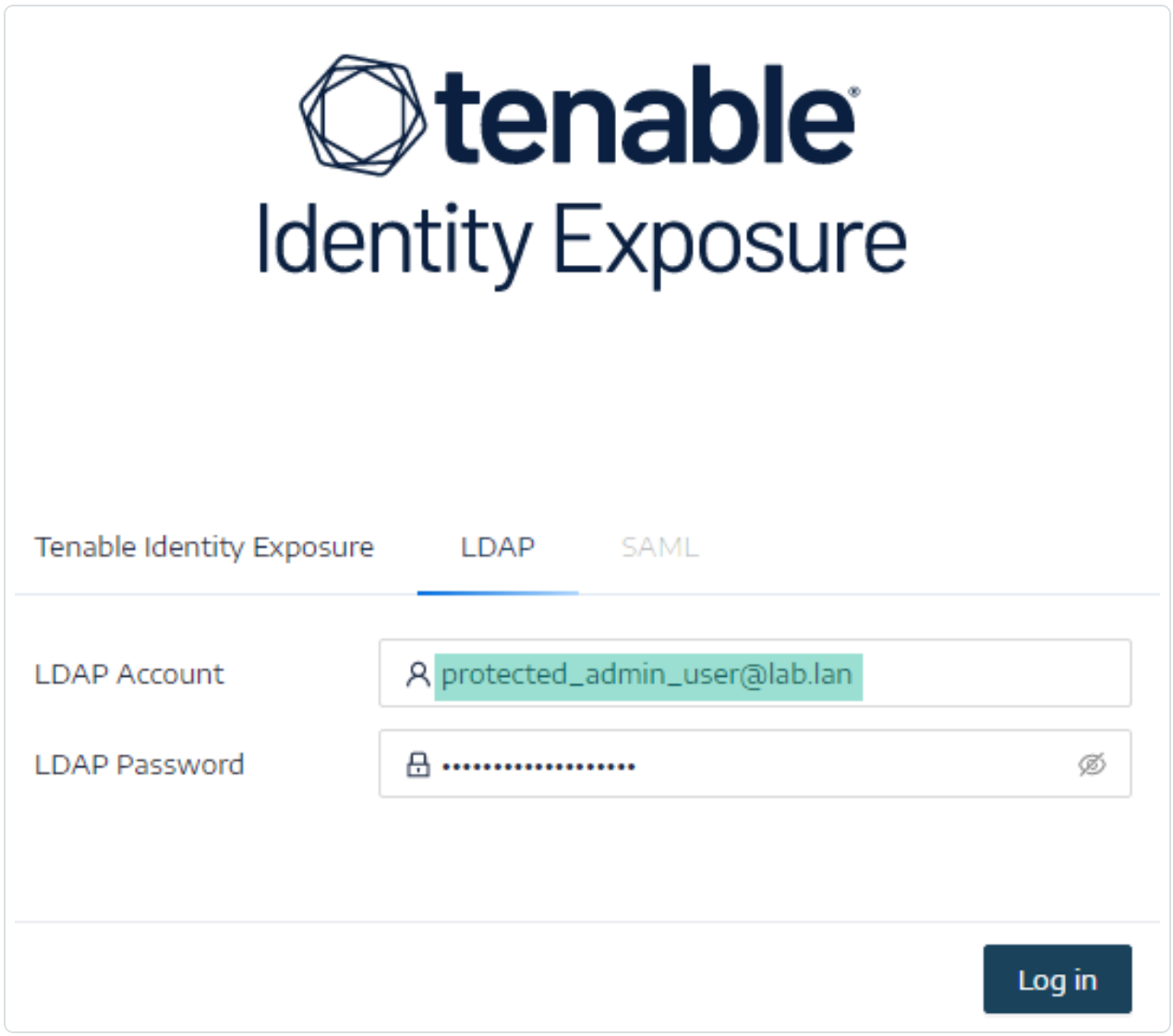
1. **Conditions préalables** : vous devez déjà avoir configuré un nom principal d'utilisateur (UPN) dans Microsoft Active Directory. Le format de nom d'utilisateur est similaire à une adresse e-mail. Il est généralement de la forme nom_utilisateur@domaine.com, où « nom_utilisateur » est le nom du compte de l'utilisateur et « domaine.com » est le domaine où le compte est situé.



2. Connectez-vous à Tenable Identity Exposure avec vos identifiants.
3. Configurez les options LDAP suivantes :
    - Utilisez le nom de domaine complet (FQDN) pour l'adresse du serveur LDAP (assurez-vous que Secure Relay peut le résoudre).
    - Utilisez un compte de service au format UPN (par exemple login@domaine.com).
    - Définissez `(userprincipalname={{login}})` comme filtre de recherche LDAP.
    - Définissez les liaisons SASL sur « on ».



4. Connectez-vous à Tenable Identity Exposure à l'aide d'identifiants LDAP en tant que membre du groupe « Protected Users » avec la syntaxe Nom principal d'utilisateur.



Pour ajouter un certificat émis par une autorité de certification (CA) de confiance personnalisée pour LDAPS :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes**.
2. Cliquez sur l'onglet **Configuration** pour afficher le volet de configuration.
3. Dans la section **Services de l'application**, cliquez sur **Autorités de certification de confiance**.
4. Dans la zone **Certificats CA supplémentaires**, collez le certificat CA de confiance encodé PEM de votre entreprise que Tenable Identity Exposure doit utiliser .
5. Cliquez sur **Enregistrer**.

Problèmes d'authentification LDAP

Une fois que vous avez terminé et enregistré la configuration, l'option LDAP doit apparaître sur la page de connexion. Pour confirmer que la configuration est valide, vous devez pouvoir vous connecter à l'aide d'un compte LDAP.

Messages d'erreur

Deux messages d'erreur peuvent s'afficher à ce stade :

- Une erreur s'est produite lors du processus d'authentification. Veuillez réessayer.
    - Dans ce cas, le problème concerne la configuration.
    - Vérifiez une fois de plus la configuration complète.
    - Vérifiez que le serveur qui héberge Tenable Identity Exposure peut accéder au serveur LDAP.
    - Vérifiez que le compte utilisé pour la recherche peut activer une liaison avec le serveur LDAP.
    - Pour plus d'informations, consultez les journaux d'application.
- Compte ou mot de passe incorrect.
    - Vérifiez que la touche de verrouillage des majuscules n'est pas activée, puis saisissez à nouveau le nom d'utilisateur et le mot de passe testés.
    - Cela peut être dû à un problème lié au filtre de groupe, au filtre de recherche ou aux champs de préfixe pour la recherche.
    - Essayez de supprimer temporairement tout filtrage de groupe. Pour plus d'informations, consultez les journaux d'application.

Pour plus d'informations sur les profils et les rôles de sécurité, voir :

- Profils de sécurité
- Rôles utilisateur

Authentification à l'aide de SAML

Vous pouvez configurer l'authentification SAML pour que les utilisateurs Tenable Identity Exposure puissent utiliser l'authentification unique (SSO) initiée par le fournisseur d'identité lorsqu'ils se connectent à Tenable Identity Exposure.

Avant de commencer

- Consultez le Tenable SAML Configuration Quick-Reference (Guide de référence rapide Configuration SAML de Tenable, en anglais) pour connaître les étapes permettant de configurer SAML pour l'utiliser avec Tenable Identity Exposure.
- Vérifiez que vous disposez des éléments suivants pour le fournisseur d'identité (IDP) :
  - SAML v2 uniquement.
  - L'option « Chiffrer l'assertion » (Assertion encryption) est activée.
  - Groupes IDP que Tenable Identity Exposure utilise pour y accorder l'accès dans le portail web Tenable Identity Exposure.
  - URL du serveur SAML.
  - Autorités de certification (CA) de confiance ayant signé le certificat du serveur SAML au format encodé PEM, commençant par `-----BEGIN CERTIFICATE-----` et se terminant par `-----END CERTIFICATE-----`.

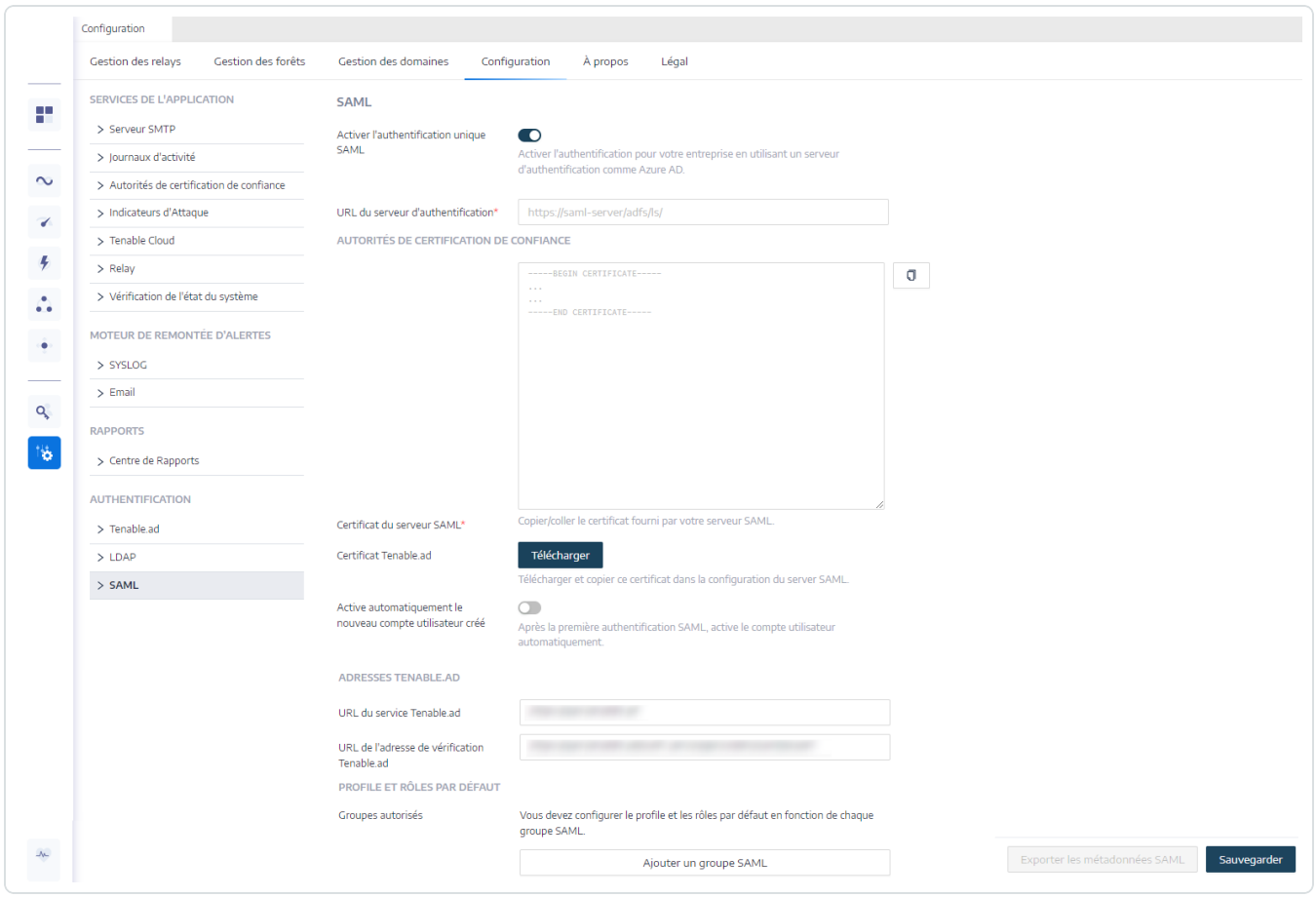
Pour configurer l'authentification SAML :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration**.

   Le volet Configuration apparaît.

2. Dans la section **Authentification**, cliquez sur **SAML**.
3. Cliquez sur le curseur **Activer l'authentification unique SAML**.

   Un formulaire d'informations SAML apparaît.



4. Fournissez les informations suivantes :

    - Dans la zone **URL du serveur SAML**, saisissez l'URL complète du serveur SAML de l'IDP auquel Tenable Identity Exposure doit se connecter.
    - Dans la zone **Autorités de certification de confiance**, collez la CA ayant signé le certificat du serveur SAML.

5. Dans la zone **Certificat Tenable Identity Exposure**, cliquez sur **Générer et télécharger**. Un nouveau certificat auto-signé est généré, la configuration SAML est mise à jour dans la base de données et un nouveau certificat à télécharger est renvoyé.

    Attention : l'utilisation de ce bouton perturbe votre configuration SAML, car Tenable Identity Exposure s'attend à ce que l'IDP s'authentifie immédiatement avec le certificat généré le plus récemment, alors que l'IDP utilise toujours un certificat précédent, s'il en existe un. Si vous générez un nouveau certificat Tenable Identity Exposure, vous devez reconfigurer votre IDP pour qu'il utilise le nouveau certificat.

6. Cliquez sur le curseur **Activer automatiquement le nouveau compte utilisateur créé** pour activer les nouveaux comptes utilisateur après la première connexion SAML.
7. Sous **Terminaux Tenable Identity Exposure**, fournissez les informations suivantes :
    - URL du fournisseur de service Tenable Identity Exposure
    - Terminal d'assertion du fournisseur de services de Tenable Identity Exposure
8. Dans la section **Profil et rôles par défaut**, cliquez sur **Ajouter un groupe SAML** pour spécifier les groupes autorisés à s'authentifier.

    Un formulaire d'informations de groupe SAML apparaît.
9. Fournissez les informations suivantes :
    - Dans la zone **Nom du groupe SAML**, saisissez le nom du groupe autorisé tel qu'il apparaît sur le serveur SAML.
    - Dans la zone déroulante **Profil par défaut**, sélectionnez le profil du groupe autorisé.
    - Dans la zone **Rôles par défaut**, sélectionnez les rôles du groupe autorisé.
10. Si nécessaire, cliquez sur l'icône **+** pour ajouter un nouveau groupe autorisé.
11. Cliquez sur **Enregistrer**.

    Après avoir configuré l'authentification SAML, l'option SAML apparaît dans un onglet sur la page de connexion.

Pour plus d'informations sur les profils et les rôles de sécurité, voir :

- Profils de sécurité
- Rôles utilisateur

Comptes utilisateur

La page **Gestion des comptes utilisateur** offre la possibilité d'ajouter, de modifier, de supprimer ou d'afficher les détails des comptes utilisateur Tenable Identity Exposure.

Les utilisateurs appartiennent à deux catégories :

- Administrateur global – Rôle administrateur qui inclut toutes les autorisations.
- Utilisateur – Rôle utilisateur basique ayant des autorisations en lecture seule sur les données métier.

Attention

Si vous disposez d'une **licence Tenable Identity Exposure autonome**, vous pouvez choisir d'envoyer des données à la plateforme Tenable via vos paramètres. Ce faisant, vous activez les fonctionnalités Identités 360 et Security Engine de Tenable Identity Exposure.

Pour faciliter la communication avec la plateforme Tenable et suivre les actions des utilisateurs, Tenable Identity Exposure crée automatiquement les objets suivants dans la plateforme Tenable, visibles dans les paramètres du conteneur Tenable Vulnerability Management :

- Un groupe nommé avec le modèle `TIE – Utilisateurs générés automatiquement -{random_string}`
- Une autorisation nommée `TIE – Généré automatiquement – Peut afficher tous les assets – {random_string}` appliquée au groupe `TIE – Utilisateurs générés automatiquement – {random_string}`. Elle permet aux utilisateurs de voir les assets que Tenable Identity Exposure a exportés vers la plateforme Tenable.
- Pour chaque utilisateur Tenable Identity Exposure, un utilisateur nommé selon le modèle `tie-{username}-{random_string}` qui est membre du groupe `TIE – Utilisateurs générés automatiquement -{random_string}`. Cet utilisateur a un mot de passe aléatoire robuste et vous ne devez **pas** l'utiliser pour vous authentifier auprès du conteneur Tenable Vulnerability Management. Il dispose de droits en lecture seule `Standard` dans le conteneur Tenable Vulnerability Management.

Un administrateur peut voir ces objets mais **ne doit pas les modifier**, car des changements pourraient perturber les fonctionnalités Identités 360 et Security Engine.

Pour créer un utilisateur :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des comptes utilisateur**.

   Le volet **Gestion des comptes utilisateur** apparaît.

2. Cliquez sur le bouton **Créer un utilisateur** sur la droite.

   Le volet **Créer un utilisateur** apparaît.

3. Dans la section **Informations principales**, saisissez les informations sur l'utilisateur :

- Prénom
- Nom de famille
- E-mail
- Mot de passe : nécessite au moins 12 caractères, parmi lesquels au moins :
  1 minuscule, 1 majuscule, 1 chiffre et 1 caractère spécial
- Confirmation du mot de passe
- Service
- Biographie

4. Cliquez sur le curseur **Autoriser l'authentification** pour activer l'utilisateur.
5. Dans la section **Gestion des rôles**, sélectionnez un rôle à appliquer à l'utilisateur.
6. Cliquez sur **Create** (Créer).

   Un message confirme que Tenable Identity Exposure a créé l'utilisateur avec le rôle sélectionné.

Pour modifier un utilisateur :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des comptes utilisateur**.

   Le volet **Gestion des comptes utilisateur** apparaît.
2. Dans la liste des utilisateurs, survolez la ligne où figure le nom de l'utilisateur et cliquez sur l'icône  à la fin de la ligne.

   Le volet **Modifier un utilisateur** apparaît.
3. Dans la section **Informations principales**, modifiez les informations sur l'utilisateur selon vos besoins :
   - Prénom
   - Nom de famille
   - E-mail
   - Mot de passe : nécessite au moins 8 caractères

- Confirmation du mot de passe
- Service
- Biographie

4. Dans la section **Gestion des rôles**, modifiez le rôle de l'utilisateur selon les besoins.
5. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour l'utilisateur avec le rôle sélectionné.

Pour désactiver un utilisateur :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des comptes utilisateur**.

   Le volet **Gestion des comptes utilisateur** apparaît.
2. Dans la liste des utilisateurs, survolez la ligne où figure le nom de l'utilisateur et cliquez sur l'icône à la fin de la ligne.

   Le volet **Modifier un utilisateur** apparaît.
3. Cliquez sur le curseur **Autoriser l'authentification** pour désactiver l'utilisateur.
4. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour l'utilisateur.

Pour supprimer un utilisateur :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des comptes utilisateur**.

   Le volet **Gestion des comptes utilisateur** apparaît.
2. Dans la liste des utilisateurs, survolez la ligne où figure le nom de l'utilisateur à supprimer et cliquez sur l'icône à la fin de la ligne.

   Un message demande de confirmer la suppression.
3. Cliquez sur **Supprimer**.

   Un message confirme que Tenable Identity Exposure a supprimé l'utilisateur.

Profils de sécurité

Rôle utilisateur requis : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

Les profils vous permettent de créer et de personnaliser votre propre vue des risques qui affectent votre infrastructure Active Directory.

Chaque profil affiche des scénarios d'exposition et d'attaque configurés pour les utilisateurs ayant ce profil. Par exemple, la vue générale de l'analyse des données d'un administrateur informatique peut être différente de celle de l'équipe de sécurité qui affiche une vue complète de tous les risques auxquels les infrastructures AD sont confrontées.

L'application d'un profil de sécurité permet à différents types d'utilisateurs d'examiner l'analyse des données sous différents angles, tels que définis par les indicateurs du profil de sécurité.

Le volet Gestion des profils de sécurité permet de gérer différents types d'utilisateurs qui peuvent consulter l'analyse de la sécurité sous différents angles. Les profils de sécurité permettent de personnaliser le comportement des indicateurs d'exposition et des indicateurs d'attaque.

Remarque : Tenable Identity Exposure fournit un profil de sécurité par défaut appelé « Tenable ». **Vous ne pouvez pas modifier ni supprimer le profil Tenable**, mais vous pouvez l'utiliser comme modèle pour créer d'autres profils de sécurité avec des paramètres adaptés à vos besoins.

Pour créer un profil de sécurité :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des profils de sécurité**.

   Le volet **Gestion des profils de sécurité** apparaît.

2. Cliquez sur le bouton **Créer un profil** sur la droite.

   Le volet **Créer un profil** apparaît.

3. À partir de la liste déroulante Action, vous pouvez effectuer l'une ou l'autre des opérations suivantes :

- **Créer un profil**.
- **Copier** un profil de sécurité existant à partir duquel vous pouvez créer un nouveau profil (par exemple, le profil « Tenable »).

4. Dans la zone **Nom du nouveau profil**, saisissez le nom du nouveau profil.

   Remarque : Tenable Identity Exposure accepte uniquement des caractères alphanumériques et des tirets bas.

5. Cliquez sur le bouton **Créer** dans l'angle inférieur droit.

   Un message indique que Tenable Identity Exposure a créé le profil. Le volet **Configuration du profil** apparaît.

Pour supprimer un profil de sécurité :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des profils de sécurité**.

   Le volet **Gestion des profils de sécurité** apparaît.

2. Dans la liste des profils de sécurité, survolez celui que vous souhaitez supprimer et cliquez sur l'icône en fin de ligne.

   Un message demande de confirmer la suppression.

3. Cliquez sur **Supprimer**.

   Un message confirme que Tenable Identity Exposure a supprimé le profil.

Que faire ensuite

Pour terminer la création du profil, voir Personnaliser un indicateur pour plus d'informations.

Pour plus d'informations, voir :

- Personnaliser un indicateur
- Affiner la personnalisation sur un indicateur

Personnaliser un indicateur

Rôle utilisateur requis : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

Vous pouvez personnaliser des indicateurs d'exposition et des indicateurs d'attaque pour un profil de sécurité.

Chaque profil de sécurité fonctionne indépendamment pour ne pas affecter les résultats d'un autre. Vous devez utiliser le profil « Tenable » uniquement comme référence, car vous ne pouvez pas le personnaliser ni l'utiliser pour placer des déviances sur liste blanche. Vous devez créer vos propres profils personnalisés pour répondre à des exigences spécifiques.

Le terme « Configuration globale » dans le volet de personnalisation des indicateurs **s'applique à tous les domaines** et non pas à tous les profils. Par conséquent, tous les paramètres que vous appliquez à la « Configuration globale » pour un profil de sécurité n'impactent pas le profil « Tenable » ou un autre profil.

Conseil : pour afficher les paramètres du profil de sécurité « Tenable », cliquez sur l'icône en fin de ligne.

Pour personnaliser un indicateur :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des profils de sécurité**.

   Le volet **Gestion des profils de sécurité** apparaît.

2. Dans la liste des profils de sécurité, survolez celui qui contient l'indicateur à personnaliser. Cliquez sur l'icône à la fin de la ligne où figure le nom du fichier du profil de sécurité.

   Le volet **Configuration du profil** apparaît.

3. Sélectionnez l'onglet **Indicateurs d'exposition** ou **Indicateurs d'attaque**.

4. (Facultatif) Dans la zone **Rechercher un indicateur**, saisissez le nom d'un indicateur.

5. Cliquez sur le nom de l'indicateur à personnaliser.

   Le volet **Personnalisation de l'indicateur**apparaît.

6. Sélectionnez les options dans le tableau « Options ».

Conseil : pour activer le **mode agressif** pour les indicateurs d'attaque, cliquez sur le curseur pour régler l'option « Mode agressif » sur « Oui ».

Conseil : certaines options d'indicateur nécessitent d'utiliser des expressions régulières (regex). Les regex appliquent une correspondance de type « contient » et non pas « égale ».
- Pour obtenir une correspondance exacte, vous devez utiliser la syntaxe Regex utilisant les caractères spéciaux (« `^...$` »).
- Vous devez également échapper les caractères spéciaux avec une barre oblique inverse lorsque vous utilisez une Regex. Par exemple : pour déclarer « `domain\user` » et « `CN=Vincent C (Test),DC=tenable,DC=corp` », vous devez saisir « `domain\\user` » et « `CN=Vincent C. \(Test\),DC=tenable,DC=corp` ».

7. Cliquez sur **Enregistrer comme brouillon**.

   Un message confirme que Tenable Identity Exposure a enregistré les options de personnalisation.

Pour appliquer la personnalisation :

1. Vous pouvez procédez de l'une ou l'autre des manières suivantes :

   - Dans le volet **Configuration du profil**, cliquez sur **Appliquer la personnalisation en cours** dans l'angle inférieur droit, ou bien,
   - Dans le volet **Gestion des profils de sécurité**, cliquez sur l'icône ✓ à la fin de la ligne où figure le nom du fichier du profil de sécurité.

   Un message apparaît pour indiquer que l'application de la personnalisation efface toutes ses données et nécessite une analyse complète de l'infrastructure Active Directory surveillée, ce qui peut prendre un certain temps.

2. Cliquez sur **OK**.

   Un message confirme que Tenable Identity Exposure a appliqué les options de personnalisation. Dans la colonne *Analyse de la sécurité* du tableau **Gestion des profils de sécurité**, **En attente** indique que l'analyse selon votre profil de sécurité est en attente d'exécution.

Pour supprimer une personnalisation :

- Vous pouvez procéder de l'une ou l'autre des manières suivantes :
  - Dans le volet **Configuration du profil**, cliquez sur **Annuler la personnalisation en cours** dans l'angle inférieur gauche, ou bien,
  - Dans le volet **Gestion des profils de sécurité**, cliquez sur l'icône ↺ à la fin de la ligne où figure le nom du fichier du profil de sécurité.

  Un message confirme que Tenable Identity Exposure a annulé les options de personnalisation.

Voir aussi

- Affiner la personnalisation sur un indicateur

Affiner la personnalisation sur un indicateur

Rôle utilisateur requis : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

La personnalisation supplémentaire d'un indicateur d'un profil de sécurité permet de sélectionner des options d'indicateur pour des domaines spécifiques. Par défaut, la configuration globale s'applique à tous les domaines.

Pour affiner la personnalisation sur un indicateur :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des profils de sécurité**.

   Le volet **Gestion des profils de sécurité** apparaît.

2. Dans la liste des profils de sécurité, survolez celui qui contient l'indicateur à personnaliser. Cliquez sur l'icône ✎ à la fin de la ligne où figure le nom du fichier du profil de sécurité.

   Le volet **Configuration du profil** apparaît.

3. Sélectionnez l'onglet **Indicateurs d'exposition** ou **Indicateurs d'attaque**.

4. (Facultatif) Dans la zone **Rechercher un indicateur**, saisissez le nom d'un indicateur.

5. Cliquez sur le nom de l'indicateur à personnaliser.

   Le volet **Personnalisation de l'indicateur**apparaît.

6. À côté de l'onglet **Configuration globale**, cliquez sur l'icône **+**.

   L'onglet **Configuration n° 1** apparaît.

7. Cochez la case **Appliquer sur**.

   Le volet **Forêts et domaines** apparaît.

8. (Facultatif) Dans la zone de recherche, saisissez le nom d'une forêt ou d'un domaine.
9. Sélectionnez le domaine.
10. Cliquez sur **Filtrer sur la sélection**.
11. Apportez une personnalisation supplémentaire, si nécessaire, à l'indicateur du domaine sélectionné.
12. Cliquez sur **Enregistrer comme brouillon**.

Pour supprimer une personnalisation affinée :

1. Cliquez sur l'onglet de la personnalisation.
2. Cliquez sur **Supprimer cette configuration** en bas du volet.

Voir aussi

- Personnaliser un indicateur

Rôles utilisateur

Tenable Identity Exposure utilise le contrôle d'accès basé sur le rôle (RBAC) pour sécuriser l'accès aux données et aux fonctionnalités au sein de votre organisation. Les rôles déterminent le type d'informations auxquelles un utilisateur peut accéder à partir de son compte en fonction de son rôle.

Les utilisateurs disposant des autorisations appropriées peuvent attribuer des autorisations à d'autres utilisateurs en fonction de leur rôle pour effectuer les actions suivantes :

- Lire le contenu et les menus, les configuration du système et des indicateurs d'exposition.
- Modifier le contenu et les menus, les configuration du système et des indicateurs d'exposition.
- Créer des comptes, des profils de sécurité et des rôles.

Voir aussi

- Gérer les rôles
- Définir les autorisations d'un rôle
- Définir des autorisations sur les entités de type Interface utilisateur (exemple)

Gérer les rôles

Pour créer un rôle :

1. Dans Tenable Identity Exposure, accédez à **Comptes** > **Gestion des rôles**.
2. Cliquez sur le bouton **Créer un rôle** dans l'angle supérieur droit.

   Le volet **Créer un rôle** apparaît.
3. Dans la zone Nom, saisissez le nom du rôle.
4. Dans la zone Description, saisissez des informations sur le rôle.
5. Cliquez sur **Ajouter** dans l'angle supérieur droit.

   Un message confirme que Tenable Identity Exposure a créé le rôle. Le volet **Modifier un rôle** apparaît et vous permet de définir des autorisations pour le rôle.

Remarque : vous ne pouvez pas modifier le rôle administrateur Tenable Identity Exposure (appelé Administrateur global). Cliquez sur l'icône pour afficher les paramètres du rôle Tenable Identity Exposure.

Pour supprimer un rôle :

1. Dans Tenable Identity Exposure, accédez à **Comptes** > **Gestion des rôles**.
2. Dans la liste des rôles, survolez celui que vous voulez supprimer et cliquez sur l'icône  à droite.

   Un message demande de confirmer la suppression.
3. Cliquez sur Supprimer.

   Un message confirme la suppression du rôle.

Voir aussi

- Définir les autorisations d'un rôle

Définir les autorisations d'un rôle

> **Rôle utilisateur requis** : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

Tenable Identity Exposure utilise le contrôle d'accès basé sur le rôle (RBAC) pour sécuriser l'accès à ses données. Un rôle détermine le type d'informations auxquelles les utilisateurs peuvent accéder, selon leurs fonctions dans l'organisation. Lorsque vous créez un utilisateur dans Tenable Identity Exposure, vous lui assignez un rôle spécifique avec ses autorisations associées.

Pour définir les autorisations d'un rôle :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des rôles**.
2. Survolez le rôle pour lequel vous souhaitez définir des autorisations et cliquez sur l'icône  à droite.

   Le volet **Modifier un rôle** apparaît.
3. Sous **Gestion des autorisations**, sélectionnez un type d'entité :
   - Entités de type Donnée
   - Entités de type Utilisateur

- Entités de type Configuration système
- Entités de type Interface

4. Dans la liste des noms d'entités, sélectionnez l'entité sur laquelle vous voulez définir des autorisations.
5. Sous les colonnes **Lire**, **Modifier** et **Créer**, cliquez sur le curseur pour activer Autorisé ou Interdit.
6. Vous pouvez procédez de l'une ou l'autre des manières suivantes :
   - Cliquez sur Appliquer pour appliquer l'autorisation et maintenir le volet **Modifier un rôle** ouvert pour d'autres modifications.
   - Cliquez sur Appliquer et fermer pour appliquer l'autorisation et fermer le volet **Modifier un rôle**.

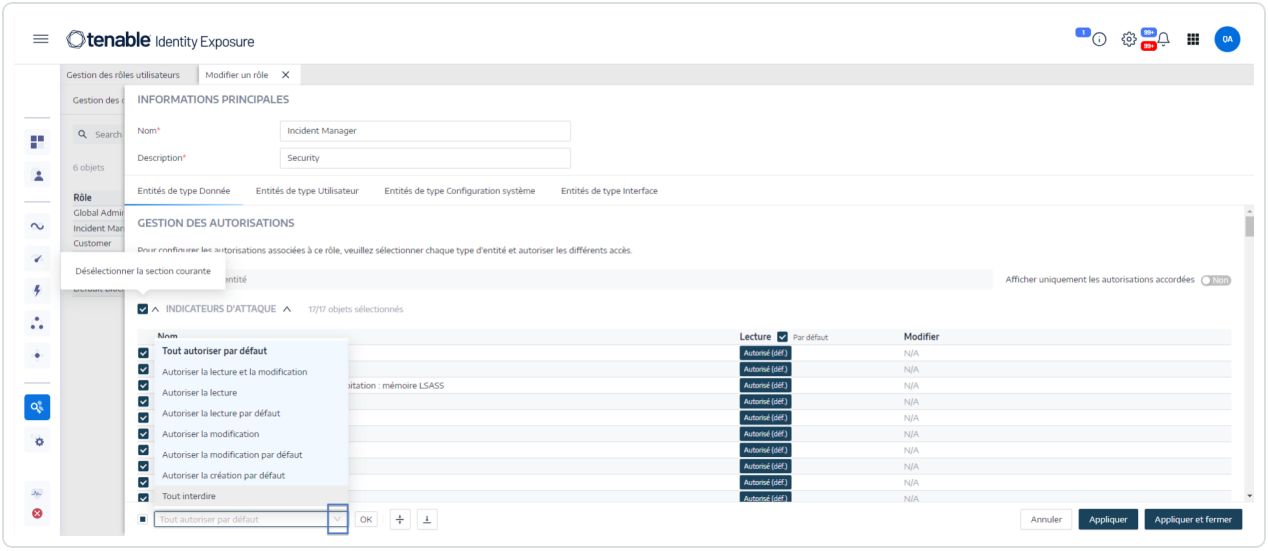
   Un message confirme que Tenable Identity Exposure a mis à jour le rôle.

Pour définir en bloc des autorisations pour un rôle :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des rôles**.
2. Survolez le rôle pour lequel vous souhaitez définir des autorisations et cliquez sur l'icône  à droite.

   Le volet **Modifier un rôle** apparaît.
3. Sous **Gestion des autorisations**, sélectionnez un type d'entité.
4. Sélectionnez les entités ou les sections d'entités (les indicateurs d'exposition, par exemple) sur lesquelles vous voulez définir des autorisations.
5. Au bas de la page, cliquez sur la flèche de la zone déroulante pour afficher une liste d'autorisations.
6. Sélectionnez la ou les autorisations du rôle.
7. Cliquez sur **OK**.

   Un message confirme que Tenable Identity Exposure a défini les autorisations sur les entités.



Type d'autorisations

Autorisation	Description
Lecture	Autorisation d'afficher un objet ou une configuration.
Modifier	Autorisation de modifier un objet ou une configuration. Requiert l'autorisation de lecture pour appliquer des modifications.
Créer	Autorisation de créer un objet ou une configuration. L'autorisation **Créer** nécessite les autorisations **Lire** et **Modifier** pour effectuer les actions autorisées sur les ressources autorisées.

Types d'entités

Il existe quatre types d'entités dans Tenable Identity Exposure ; elles nécessitent des autorisations d'accès que vous pouvez personnaliser pour chaque rôle utilisateur de votre organisation :

Type d'entité	Contient	Autorisations
Entités de type Donnée		
Cette entité contrôle les autorisations permettant de configurer de l'Active Directory surveillé et l'analyse de données	• Indicateurs d'attaque • Indicateurs d'exposition • Forêts	Lire, Modifier, Créer

dans Tenable Identity Exposure.	• Domaines • Profils • Utilisateurs • Alertes par e-mail • Alertes par Syslog • Rôles • Entité Relay • Rapports	
Entités de type Utilisateur		
Cette entité contrôle la possibilité pour un utilisateur de configurer les informations que Tenable Identity Exposure affiche pour l'analyse des données, et de modifier ses informations et préférences personnelles.	• Préférences • Dashboards • Widgets • Clé API • Informations personnelles	Modifier, Créer
Entités de type Configuration système		
Cette entité contrôle l'accès à la plateforme et aux services Tenable Identity Exposure.	• Services de l'application (SMTP, journaux, authentification Tenable Identity Exposure, indicateurs d'attaque, autorités de certification de confiance) • Scores via l'API publique • Licences • Authentification LDAP	Lire, Modifier

	• Authentification SAML **Remarque** : les autorisations pour l'authentification LDAP et SAML ne sont pas disponibles si vous disposez d'une licence Tenable Vulnerability Management. • Topologie • Stratégie de verrouillage des comptes • Réexplorer les domaines • Journaux d'activité • Service Tenable Cloud (Collecte de données via Tenable Cloud) • Prise en charge de Microsoft Entra ID • Vérifications de l'état du système • Afficher uniquement les traces personnelles de l'utilisateur	
Entités de type Interface		
Cette entité définit les autorisations d'accès à des parties spécifiques de l'interface utilisateur et des fonctionnalités de Tenable Identity Exposure.	Chemins d'accès à des fonctionnalités spécifiques Tenable Identity Exposure. Pour plus d'informations, voir Définir des autorisations sur les entités de type Interface utilisateur (exemple).	Autorisé, Interdit

Voir aussi

- Comptes utilisateur
- Rôles utilisateur

Définir des autorisations sur les entités de type Interface utilisateur (exemple)

Tenable Identity Exposure applique des autorisations sur le chemin utilisé pour accéder à une certaine fonctionnalité de l'interface utilisateur. L'exemple suivant montre comment définir des autorisations pour autoriser la configuration de Syslog.

Pour accéder aux paramètres Syslog, les utilisateurs ont besoin d'autorisations sur le chemin **Système** > **Configuration** > **SYSLOG** dans Tenable Identity Exposure :

- Configuration système : **Gestion** > **Système**
- Paramètres de configuration : **Gestion** > **Système** > **Configuration**
- Alertes Syslog : **Gestion** > **Système** > **Configuration** > **Moteur de remontée d'alertes** > **SYSLOG**

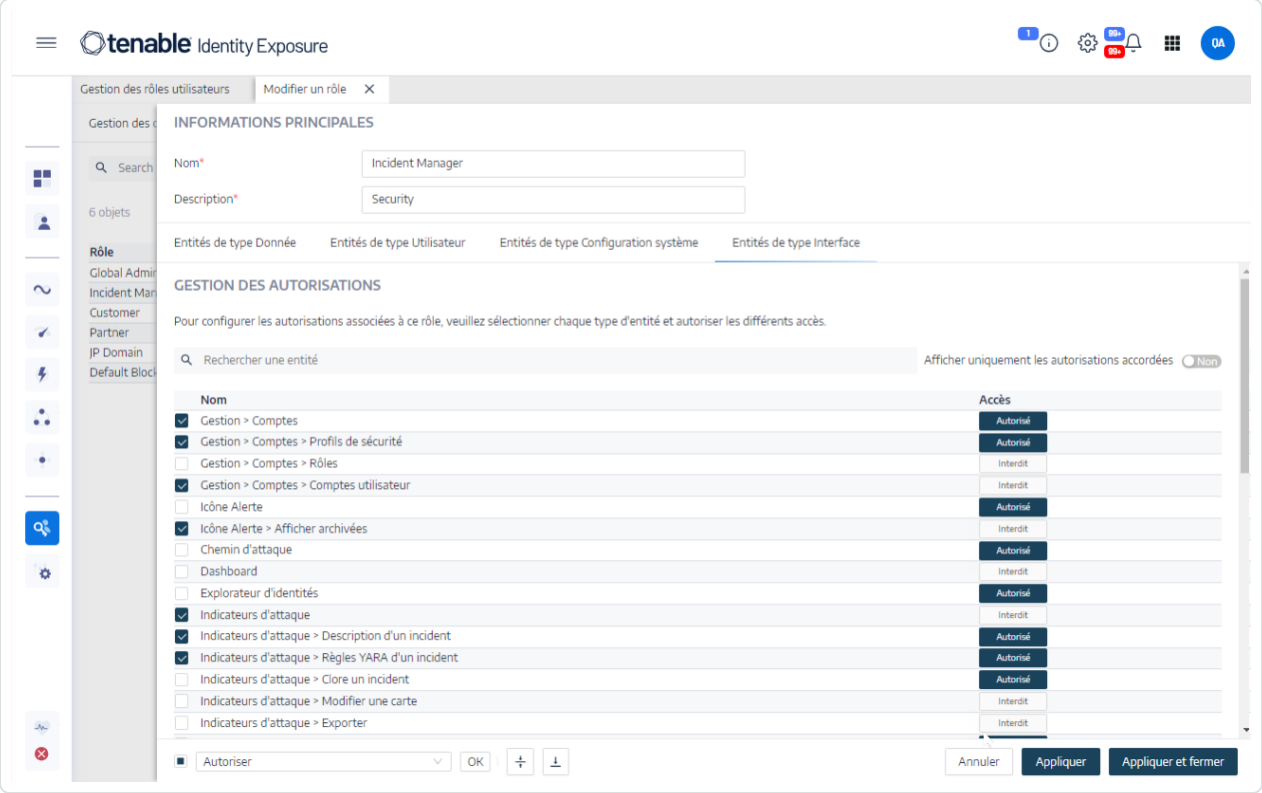
Pour définir des autorisations pour la configuration Syslog :

1. Dans Tenable Identity Exposure, cliquez sur **Comptes** > **Gestion des rôles**.
2. Survolez le rôle pour lequel vous souhaitez définir des autorisations et cliquez sur l'icône à droite.

   Le volet **Modifier un rôle** apparaît.
3. Sous **Gestion des autorisations**, sélectionnez **Entités de type Interface**.
4. Dans la liste des entités, effectuez les opérations suivantes :
   - Sélectionnez **Gestion** > **Système** et cliquez sur le curseur Accès pour activer **Autorisé**.
   - Sélectionnez **Gestion** > **Système** > **Configuration** et cliquez sur le curseur Accès pour activer **Autorisé**.
   - Sélectionnez **Gestion** > **Système** > **Configuration** > **Moteur de remontée d'alertes** > **SYSLOG**et cliquez sur le curseur Accès pour activer **Autorisé**.

5. Cliquez sur **Appliquer**.

   Un message confirme que Tenable Identity Exposure a mis à jour les autorisations sur les entités.

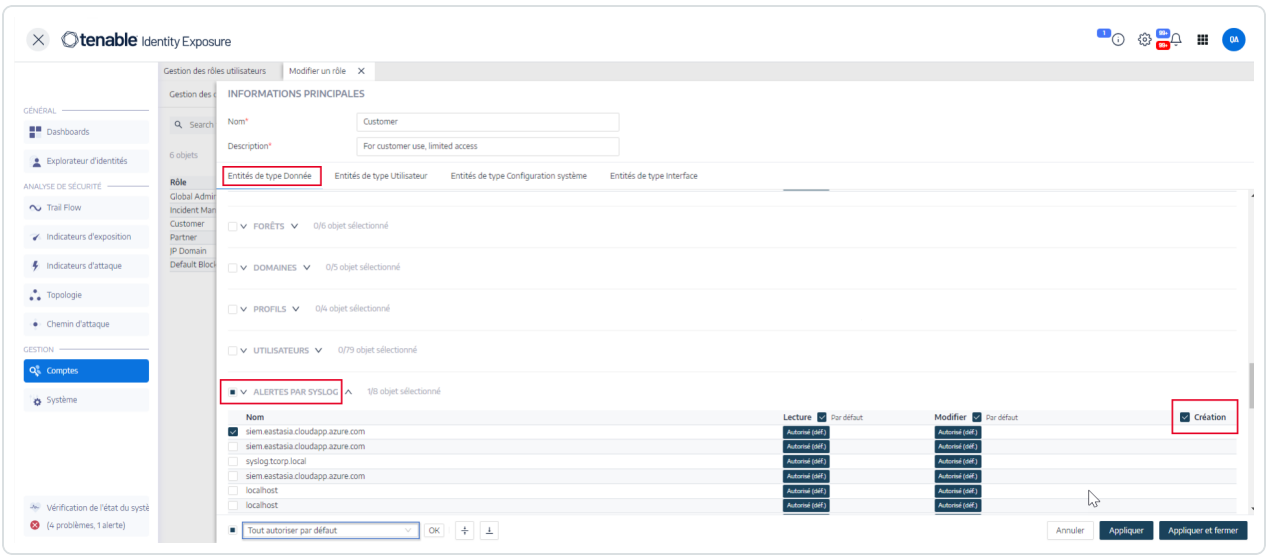


6. Sous **Gestion des autorisations**, sélectionnez **Entités de type Donnée**.
7. Dans la liste des sections des entités, sélectionnez **Alertes par Syslog**.
8. Sélectionnez l'autorisation **Création**.

   Tenable Identity Exposure accorde implicitement les autorisations de lecture et de modification.

9. Cliquez sur **Appliquer et fermer**.

   Un message confirme que Tenable Identity Exposure a mis à jour les autorisations sur les entités.



Forêts

Une forêt Active Directory (AD) est un ensemble de domaines qui partagent un schéma, une configuration et des relations d'approbation communs. Elle fournit une structure hiérarchique pour gérer et organiser les ressources, ce qui permet de centraliser l'administration et de sécuriser l'authentification sur plusieurs domaines dans une organisation.

Gestion des forêts

Pour ajouter une forêt :

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Gestion des forêts**.
2. Cliquez sur **Ajouter une forêt** sur la droite.

   Le volet Ajouter une forêt apparaît.
3. Dans la zone **Nom**, saisissez le nom de la forêt.
4. Dans la section **Compte**, fournissez les éléments suivants pour le compte de service que Tenable Identity Exposure utilise :

   - **Connexion** : saisissez le nom du compte de service.
     Format : nom principal d'utilisateur (UPN), tel que « `tenablead@exemple.domaine.com` » (recommandé pour la compatibilité avec Authentification Kerberos ou NetBios ; par exemple

« `DomainNetBIOSName\SamAccountName` ».

- **Mot de passe** : saisissez le mot de passe du compte de service.

> **Remarque** : si vous devez définir le compte de service AD de Tenable Identity Exposure en tant que membre d'un groupe d'utilisateurs protégés, assurez-vous que votre configuration Tenable Identity Exposure prend en charge Authentification Kerberos, car les utilisateurs protégés ne peuvent pas utiliser l'authentification NTLM.

5. Cliquez sur **Ajouter**.

   Un message confirme l'ajout d'une nouvelle forêt.

Pour modifier une forêt :

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Gestion des forêts**.
2. Dans la liste des forêts, survolez celle que vous souhaitez modifier et cliquez sur l'icône  à droite.

   Le volet **Modifier une forêt** apparaît.
3. Modifiez selon vos besoins.
4. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour la forêt.

Protection des comptes de service

Tenable recommande de protéger les comptes de service pour maintenir la sécurité en définissant correctement les attributs de contrôle de compte d'utilisateur (UAC) pour empêcher la délégation, exiger une pré-authentification, utiliser un chiffrement complexe, imposer l'expiration et les critères de mot de passe et permettre les changements de mot de passe autorisés. Ces mesures atténuent le risque d'accès non autorisé et de violation de sécurité, afin de garantir l'intégrité des systèmes et des données d'une organisation.

Pour modifier les paramètres à l'aide d'un éditeur de stratégie Windows :

Vous pouvez modifier les paramètres de contrôle de compte utilisateur à l'aide de l'éditeur de stratégie de sécurité locale ou de l'éditeur de stratégie de groupe de Windows avec les privilèges

administratifs appropriés.

- Dans l'éditeur, accédez à **Local Policies** (Stratégie locales) > **Security Options** (Options de sécurité) pour localiser et configurer les paramètres suivants : (cela peut varier selon votre version de Windows.)
    - *« Accès réseau : ne pas autoriser le stockage de mots de passe et d'identifiants pour l'authentification du réseau »* : réglez sur **Activé**.
    - *« Comptes : La pré-authentification Kerberos n'est pas nécessaire »* : réglez sur **Désactivé**.
    - *« Sécurité réseau : configurez les types de chiffrements autorisés pour Kerberos »* : vérifiez que l'option *« types de chiffrement DES Kerberos pour cette option »* n'est **pas** sélectionnée.
    - *« Comptes : ancienneté maximale du mot de passe »* : définissez la période d'expiration du mot de passe (par exemple, 30, 60 ou 90 jours de façon à ce que `PasswordNeverExpires = FALSE`).
    - *« Comptes : restreindre l'utilisation de mots de passe vides par le compte local à l'ouverture de session console »* : réglez sur **Désactivé**.
    - *« Ouverture de session interactive : nombre d'ouvertures de sessions précédentes réalisées en utilisant le cache (lorsqu'aucun contrôleur de domaine n'est disponible) »* : définissez la valeur souhaitée, par exemple « 10 » pour permettre aux utilisateurs de modifier leurs mots de passe.

Pour modifier les paramètres à l'aide de Powershell :

- Sur une machine hébergeant AD, ouvrez PowerShell avec les privilèges administratifs appropriés et exécutez la commande suivante :

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly
$false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired
$false -CannotChangePassword $false
```

`<AD_ACCOUNT>` est le nom du compte Active Directory à modifier.

Domaines

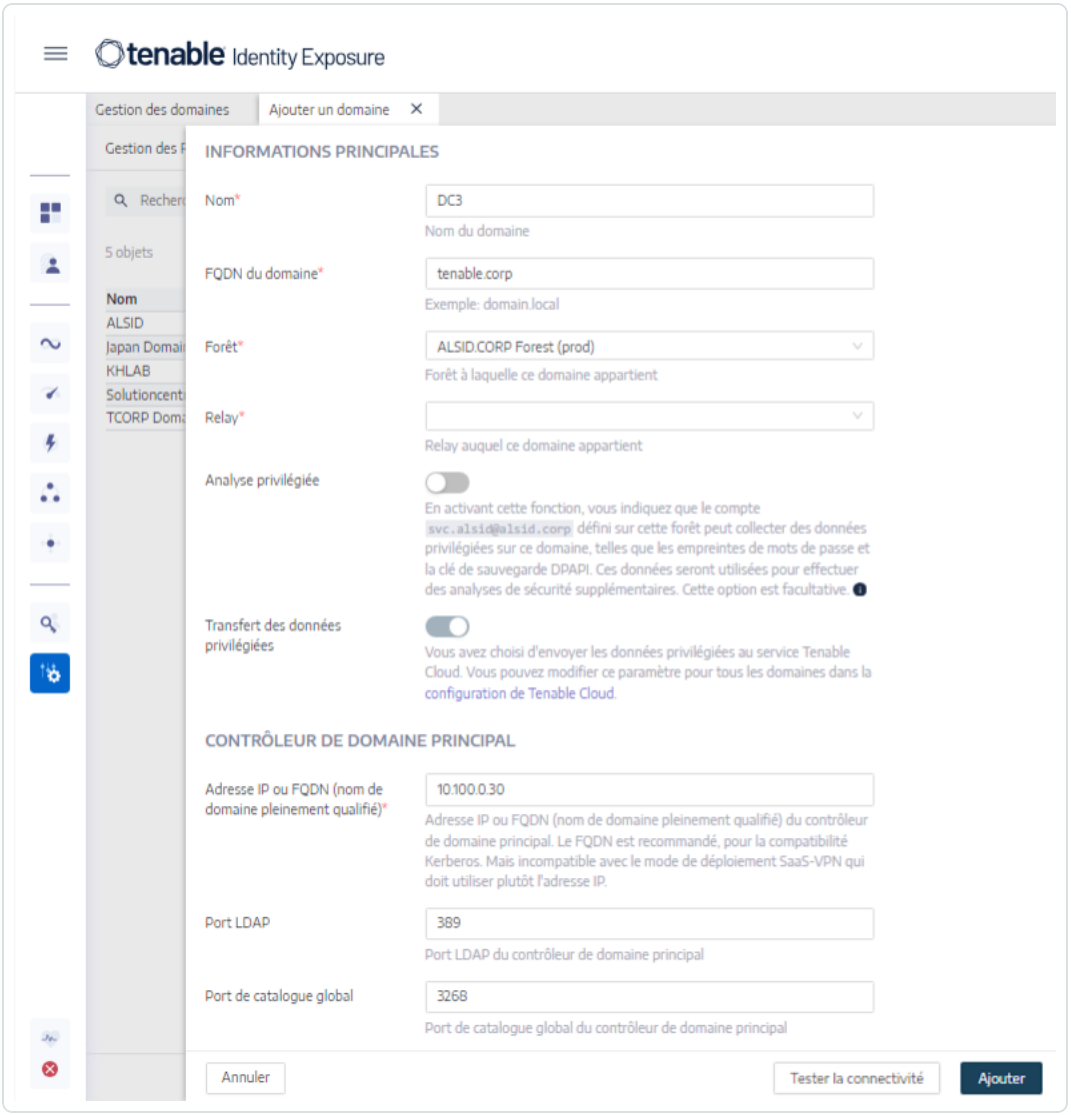
Tenable Identity Exposure surveille les domaines qui regroupent les objets partageant des paramètres communs de manière logique pour une gestion centralisée.

Pour ajouter un domaine :

1. Dans Tenable Identity Exposure, cliquez sur **Système**.
2. Cliquez sur l'onglet **Gestion des domaines**.

   Le volet **Gestion des domaines** apparaît.
3. Cliquez sur **Ajouter un domaine** dans l'angle supérieur droit.

   Le volet **Ajouter un domaine** apparaît.



4. Dans la section **Informations principales**, fournissez les informations suivantes :
    - Dans la zone **Nom**, saisissez le nom du domaine.
    - Dans la zone **FQDN du domaine**, saisissez le nom complet (FQDN) du domaine.
    - Dans la zone déroulante **Forêt**, sélectionnez la forêt à laquelle le domaine appartient.
5. **Analyse privilégiée** (facultatif) : si vous activez la curseur, vous autorisez le compte « dcadmin » de cette forêt à collecter des données privilégiées sur ce domaine pour effectuer une analyse de sécurité avancée.
6. **Transfert des données privilégiées** : pour plus d'informations sur cette option, voir Collecte de données via Tenable Cloud
7. Dans la section **Contrôleur de domaine principal**, fournissez les informations suivantes :
    - Dans la zone **Adresse IP ou nom d'hôte**, saisissez le nom d'hôte du contrôleur de domaine principal (requis pour la compatibilité avec Authentification Kerberos, mais incompatible avec les modes de déploiement SaaS-VPN) ou son adresse IP.

      Tenable Identity Exposure ne prend pas en charge les équilibreurs de charge.
    - Dans la zone **Port LDAP**, saisissez le port LDAP du contrôleur de domaine principal.

      Remarque : si vous utilisez le port TCP/636 (LDAP) pour vous connecter à votre domaine, Tenable Identity Exposure doit avoir accès au certificat Autorité de certification (CA) de votre infrastructure Active Directory pour valider votre certificat AD, afin d'établir la connexion. Dans les environnements Secure Relay, vous pouvez installer le certificat CA sur la machine Relay. Cette configuration n'est pas possible dans les environnements VPN.
    - Dans la zone **Port de catalogue global**, saisissez le contrôleur de domaine principal du port du catalogue global.
    - Dans la zone **Port SMB**, saisissez le port SMB du contrôleur de domaine principal.
8. Cliquez sur **Ajouter**.

    Un message confirme que Tenable Identity Exposure a ajouté le domaine.

Pour modifier un domaine :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes**.
2. Cliquez sur l'onglet **Gestion des domaines**.

   Le volet **Gestion des domaines** apparaît.
3. Survolez le nom du domaine à modifier pour afficher l'icône sur la droite.
4. Cliquez sur l'icône .

   Le volet **Modifier un domaine** apparaît.
5. Modifiez les informations du domaine.
6. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour le domaine.

Pour supprimer un domaine et des données historiques :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes**.
2. Cliquez sur l'onglet **Gestion des domaines**.

   Le volet **Gestion des domaines** apparaît.
3. Survolez le nom du domaine à supprimer pour afficher l'icône .
4. Cliquez sur l'icône .

   Un message demande de confirmer la suppression du domaine « domain_name ».
5. Cliquez sur **Supprimer**.

   Un message confirme que Tenable Identity Exposure a supprimé le domaine.
6. Attendez que le système nettoie toutes les données Active Directory historiques associées au domaine supprimé.

Voir aussi

- Forcer l'actualisation des données sur un domaine
- Honey Accounts
- Authentification Kerberos

Forcer l'actualisation des données sur un domaine

Pour forcer l'actualisation des données sur un domaine :

1. Dans Tenable Identity Exposure, cliquez sur **Système**.
2. Cliquez sur l'onglet **Gestion des domaines**.

   Le volet **Gestion des domaines** apparaît.
3. Survolez le nom du domaine dont vous voulez forcer l'actualisation des données pour afficher l'icône sur la droite.
4. Cliquez sur l'icône .

   Un message apparaît avec des informations sur l'action d'actualisation des données.
5. Cliquez sur **Confirmer**.

Voir aussi

- Honey Accounts

Honey Accounts

Rôle utilisateur requis : administrateur sur l'ordinateur local.

Un Honey Account (Compte leurre) est un compte dont le seul but est de détecter un attaquant qui tenterait de compromettre le réseau via Active Directory.

Il s'agit d'une condition préalable pour que l'indicateur d'attaque de Tenable Identity Exposure détecte les tentatives d'exploitation Kerberoasting qui cherchent à accéder aux comptes de service en demandant et en extrayant des tickets de service, puis en déchiffrant les identifiants du compte

de service hors ligne. L'indicateur d'attaque Kerberoasting envoie des alertes lorsque le Honey Account reçoit des tentatives de connexion ou des demandes de tickets.

Vous associez un Honey Account à chaque domaine. Les Honey Accounts ne sont pas liés aux profils de sécurité.

Pour ajouter un Honey Account :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Gestion des domaines**.

   Le volet **Gestion des domaines** apparaît.

2. Survolez le domaine pour lequel vous souhaitez ajouter un Honey Account.

3. Sous **Statut de configuration du Honey Account**, cliquez sur **+**.

   Le volet **Ajouter un Honey Account** apparaît.

4. Dans la zone **Nom**, saisissez le nom distinctif (DN) du compte utilisateur à utiliser comme Honey Account.

   Conseil : vous pouvez saisir n'importe quelle chaîne. Tenable Identity Exposure recherche et affiche les noms de compte utilisateur correspondants dans la zone déroulante si ce compte utilisateur existe déjà dans Active Directory.

5. Dans la section **Déploiement**, Tenable Identity Exposure génère un script avec les paramètres appropriés à exécuter pour déployer le Honey Account. Cliquez sur pour copier ce script.

6. Cliquez sur **Ajouter**.

   Un message apparaît pour confirmer que Tenable Identity Exposure a ajouté le Honey Account. Dans le volet Gestion des domaines, le **statut de configuration du Honey Account** du domaine sélectionné apparaît en orange ( ) pour signaler que vous devez exécuter le script de déploiement du Honey Account pour l'activer.

   Remarque : si le **statut de configuration du Honey Account** est rouge ( ), cela indique que Tenable Identity Exposure n'a pas trouvé ce compte utilisateur dans Active Directory. Vous devez créer ce compte utilisateur et passer à l'étape suivante.

7. Dans un terminal Windows PowerShell sur une machine pourvue du module Active Directory, exécutez le script de déploiement de Honey Account que vous avez copié.

   Dans le volet **Gestion des domaines**, le **statut de configuration du Honey Account** du domaine sélectionné apparaît est en vert ( ) pour signaler qu'il est actif.

   > **Remarque** : Tenable Identity Exposure peut prendre un certain temps pour traiter et activer le Honey Account.

Pour modifier un Honey Account :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Gestion des domaines**.

   Le volet **Gestion des domaines** apparaît.

2. Survolez le domaine pour lequel vous souhaitez ajouter un Honey Account.

3. Sous **Statut de configuration du Honey Account**, cliquez sur l'icône sur la droite.

   Le volet **Modifier un Honey Account** apparaît.

4. Dans la zone **Nom**, modifiez le compte utilisateur selon vos besoins.

5. Dans la section **Déploiement**, cliquez sur pour copier le script de déploiement de Honey Account.

6. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour le Honey Account. Dans le volet Gestion des domaines, le **statut de configuration du Honey Account** du domaine sélectionné apparaît en orange ( ) pour signaler que vous devez exécuter le script de déploiement du Honey Account pour l'activer.

   > **Remarque** : si le **statut de configuration du Honey Account** est rouge ( ), cela indique que Tenable Identity Exposure n'a pas trouvé ce compte utilisateur dans Active Directory. Vous devez créer ce compte utilisateur et passer à l'étape suivante.

7. Dans un terminal Windows PowerShell sur une machine pourvue du module Active Directory, exécutez le script de déploiement de Honey Account que vous avez copié.

Dans le volet **Gestion des domaines**, le **statut de configuration du Honey Account** du domaine sélectionné apparaît en vert ( ) pour signaler qu'il est configuré.

> **Remarque** : Tenable Identity Exposure peut prendre un certain temps pour traiter et activer le Honey Account.

Pour supprimer un Honey Account :

1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Gestion des domaines**.

   Le volet **Gestion des domaines** apparaît.

2. Survolez le domaine pour lequel vous souhaitez ajouter un Honey Account.

3. Sous **Statut de configuration du Honey Account**, cliquez sur l'icône sur la droite.

   Le volet **Modifier un Honey Account** apparaît.

4. Cliquez sur **Supprimer**.

   Un message confirme que Tenable Identity Exposure a supprimé le Honey Account.

Voir aussi

- Forcer l'actualisation des données sur un domaine

Authentification Kerberos

Tenable Identity Exposure s'authentifie sur le ou les contrôleurs de domaine configurés à l'aide des identifiants que vous avez fournis. Ces DC acceptent l'authentification NTLM ou Kerberos. NTLM est un ancien protocole qui présente des problèmes de sécurité documentés. Microsoft et toutes les normes de cyber-sécurité invitent désormais à ne pas l'utiliser. En revanche, Kerberos est un protocole plus robuste et largement recommandé. Windows tente toujours d'utiliser Kerberos en premier et ne recourt à NTLM que si Kerberos n'est pas disponible.

Tenable Identity Exposure est compatible avec NTLM et Kerberos à quelques exceptions près. Tenable Identity Exposure utilise de préférence le protocole Kerberos lorsque toutes les conditions requises sont remplies. Cette section décrit les exigences et explique comment configurer Tenable Identity Exposure pour utiliser Kerberos.

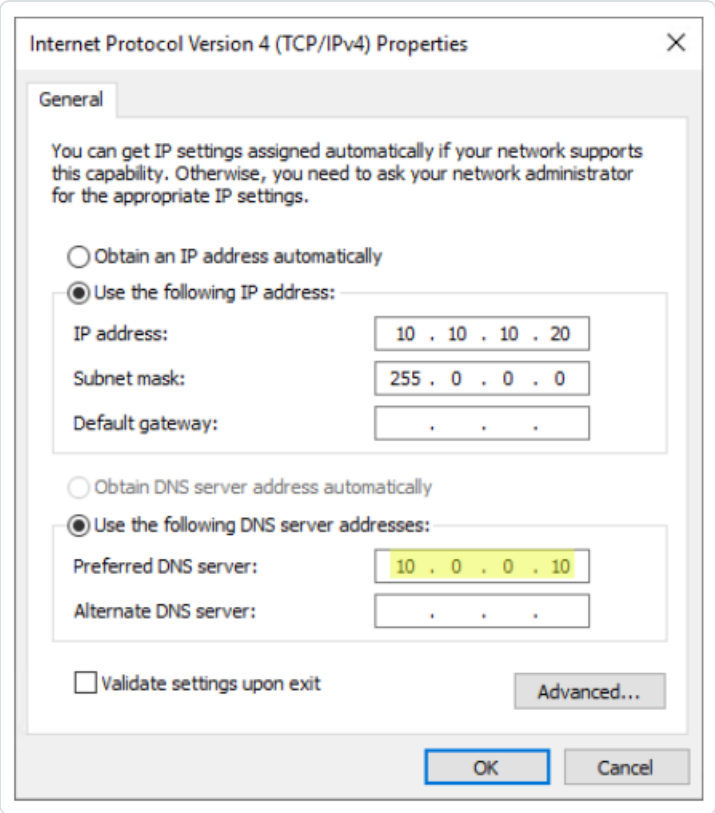
L'utilisation de NTLM au lieu de Kerberos est également la raison pour laquelle le durcissement SYSVOL interfère avec Tenable Identity Exposure. Pour plus d'informations, voir Interférence du durcissement SYSVOL avec Tenable Identity Exposure.

Compatibilité avec les modes de déploiement de Tenable Identity Exposure

Mode de déploiement	Prise en charge de Kerberos
Sur site	Oui
SaaS-TLS (ancien)	Oui
SaaS avec Secure Relay pour Tenable Identity Exposure	Oui
SaaS avec VPN	Non – Vous devez faire passer l'installation en mode de déploiement Secure Relay pour Tenable Identity Exposure.

Exigences techniques

- **Le compte de service AD configuré dans Tenable Identity Exposure doit avoir un nom principal d'utilisateur (UPN)**. Voir Configuration des comptes et des domaines de service pour obtenir des instructions.
- **La configuration DNS et le serveur DNS doivent permettre de résoudre toutes les entrées DNS nécessaires** – Vous devez configurer le Directory Listener ou la machine Relay de manière à utiliser des serveurs DNS qui connaissent les contrôleurs de domaine. Si le Directory Listener ou la machine Relay sont joints à un domaine, ce que Tenable Identity Exposure ne recommande pas, vous devriez déjà respecter cette exigence. Le moyen le plus simple consiste à utiliser le contrôleur de domaine lui-même comme serveur DNS préféré, car il exécute généralement également DNS. Par exemple :



> **Remarque** : si le Directory Listener ou la machine Relay sont connectés à plusieurs domaines, et potentiellement dans plusieurs forêts, vérifiez que les serveurs DNS configurés peuvent résoudre toutes les entrées DNS requises pour tous les domaines. Sinon, vous devez configurer plusieurs Directory Listeners ou machines Relay.

- **Accessibilité du « serveur » Kerberos (KDC)** – Nécessite une connectivité réseau du Directory Listener ou du Relay vers les contrôleurs de domaine sur le port TCP/88. Si le Directory Listener ou le Relay sont joints à un domaine, ce que Tenable ne recommande pas, vous devriez déjà respecter cette exigence. Chaque forêt Tenable Identity Exposure configurée nécessite une connectivité réseau Kerberos avec au moins un contrôleur dans son domaine correspondant contenant le compte de service, ainsi qu'au moins un contrôleur dans chaque domaine connecté.

  Pour plus d'informations sur les exigences, voir Network Flow Matrix.

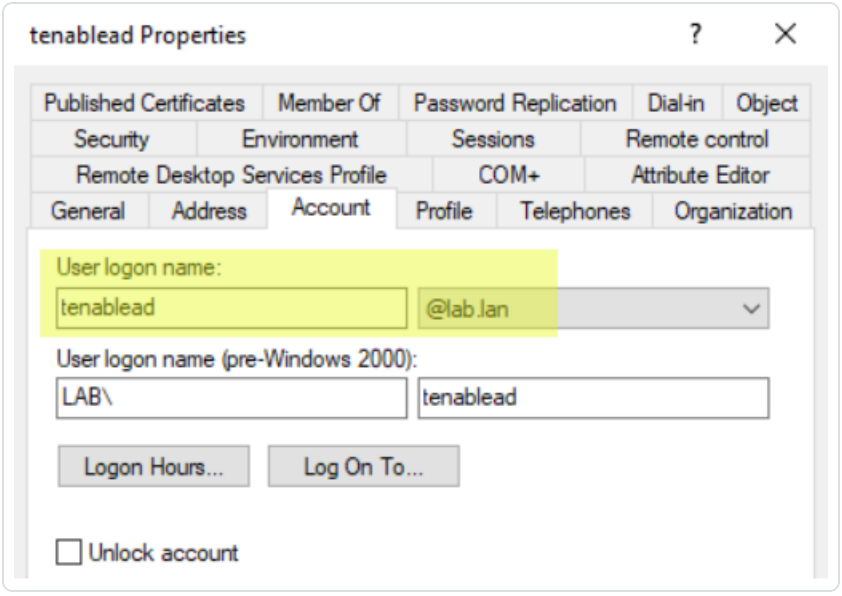
  > **Remarque** : le Directory Listener ou la machine Relay n'a pas besoin d'être joint à un domaine pour utiliser Kerberos.

Configuration des comptes et des domaines de service

Pour configurer le compte de service AD et le domaine AD dans Tenable Identity Exposure pour utiliser Kerberos :

1. Utilisez le format Nom principal d'utilisateur (UPN) pour la connexion. Dans cet exemple, l'attribut UPN est « `tenablead@lab.lan` ».

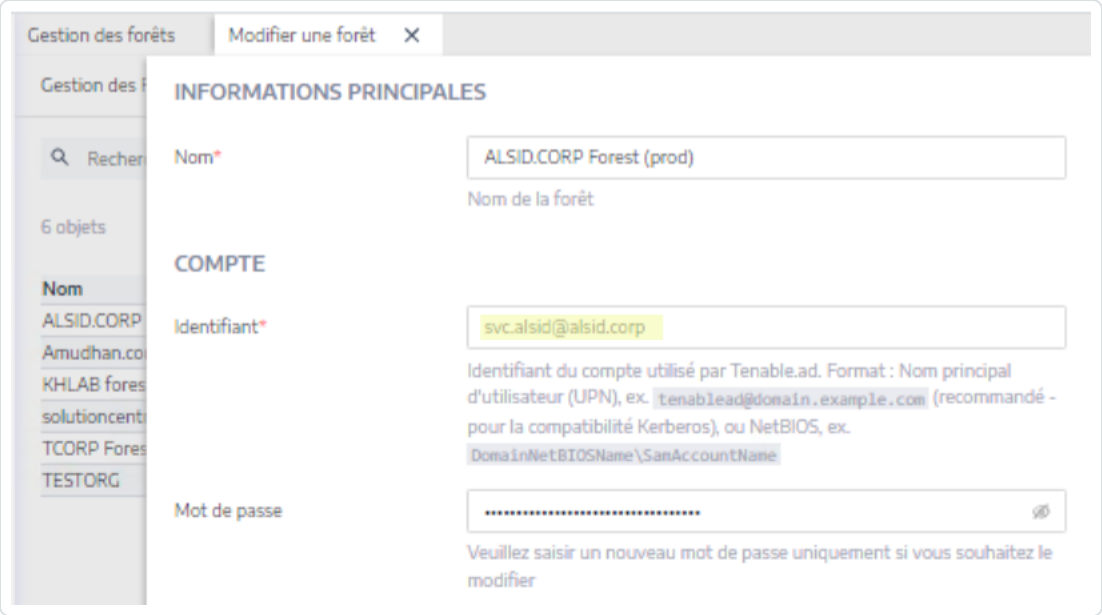
    a. Localisez l'attribut UPN dans le domaine de la forêt qui contient le compte de service comme suit :





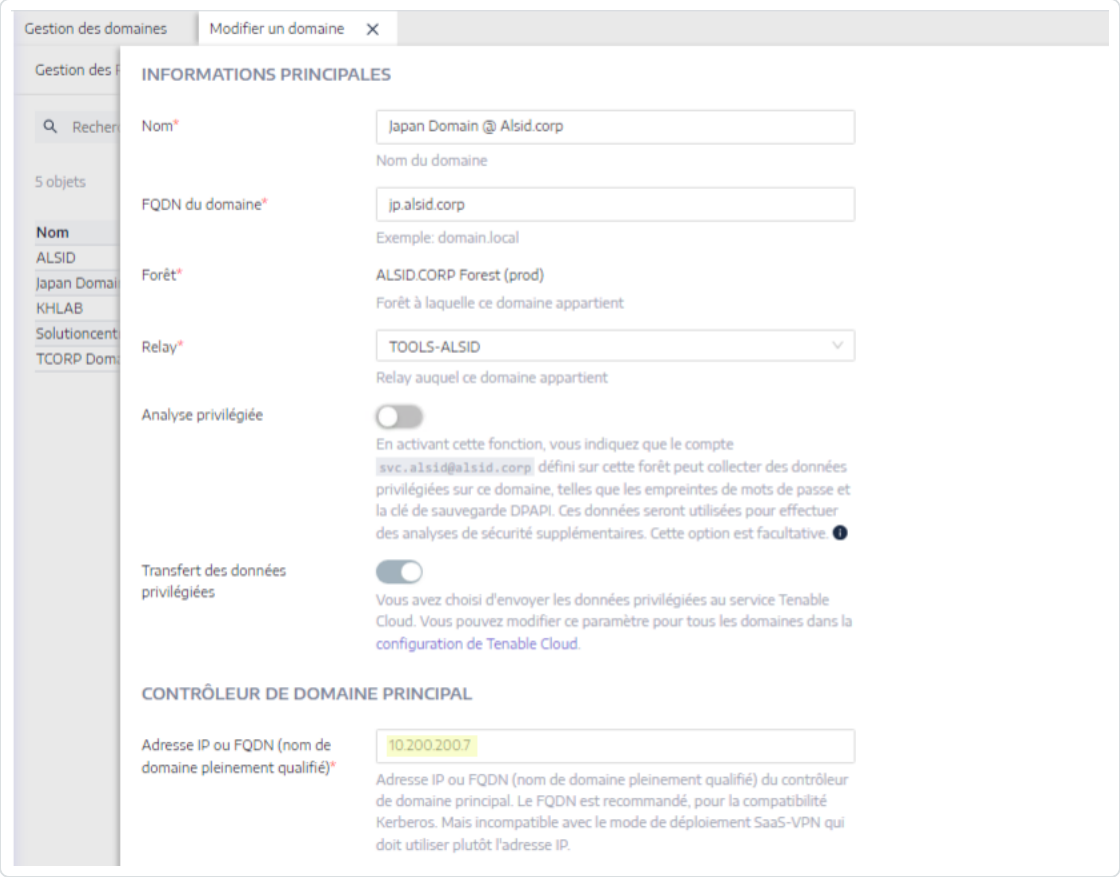
> **Remarque** : l'UPN ressemble à une adresse e-mail et est même souvent, mais pas toujours, identique à l'adresse e-mail de l'utilisateur.

b. Dans la section de configuration de la forêt de Tenable Identity Exposure, définissez cet UPN au lieu du format court « `nom d'utilisateur` » ou du format NetBIOS « `domaine\nom d'utilisateur` », comme suit :



2. Utiliser le nom de domaine complet (FQDN) Dans la configuration du domaine dans Tenable Identity Exposure, définissez le FQDN du contrôleur de domaine principal (PDC) au lieu de

son adresse IP.

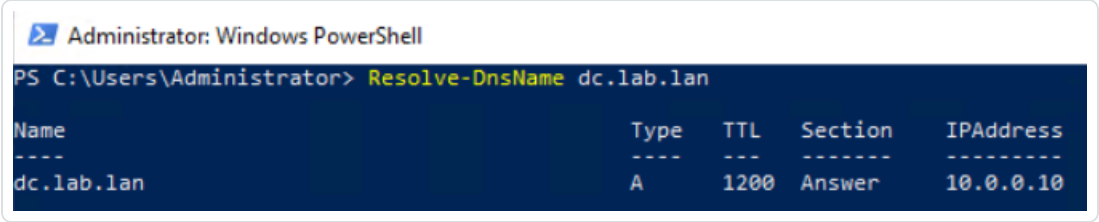


Résolution des problèmes

Il est nécessaire d'exécuter plusieurs étapes de configuration pour que Kerberos fonctionne correctement. Sinon, Windows, et par extension Tenable Identity Exposure, reviennent silencieusement à l'authentification NTLM.

DNS

Vérifiez que le ou les serveurs DNS utilisés sur le Directory Listener ou la machine Relay peuvent résoudre le FQDN de PDC fourni, tels que :



Kerberos

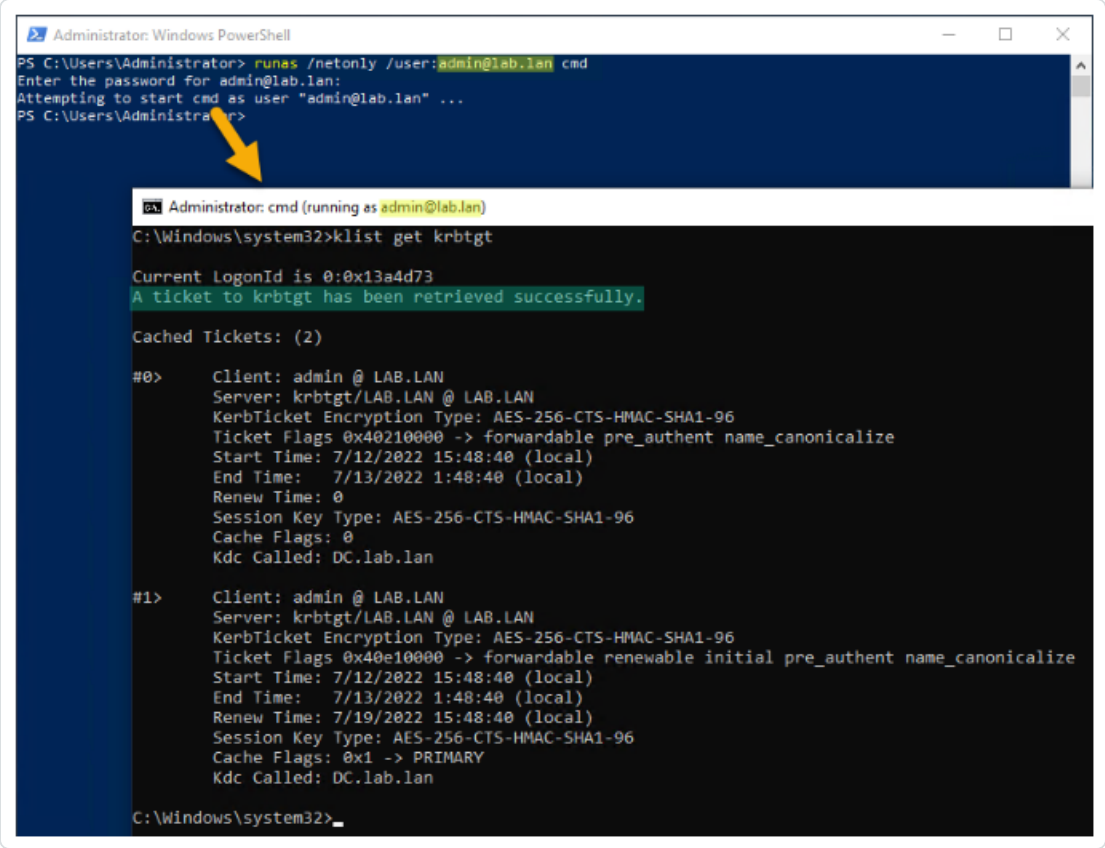
Pour vérifier que Kerberos fonctionne avec les commandes que vous exécutez sur le Directory Listener ou la machine Relay :

1. Vérifiez que le compte de service AD configuré dans Tenable Identity Exposure peut obtenir un TGT :

    a. Dans un terminal de ligne de commande ou PowerShell, exécutez « `runas /netonly /user:<UPN> cmd` » et saisissez le mot de passe. Soyez particulièrement prudent lorsque vous saisissez ou collez le mot de passe, car aucune vérification n'est effectuée du fait de l'indicateur « `/netonly` ».

    b. À la deuxième invite de commande, exécutez « `klist get krbtgt` » pour demander un ticket TGT.

    L'exemple suivant montre un résultat correct :

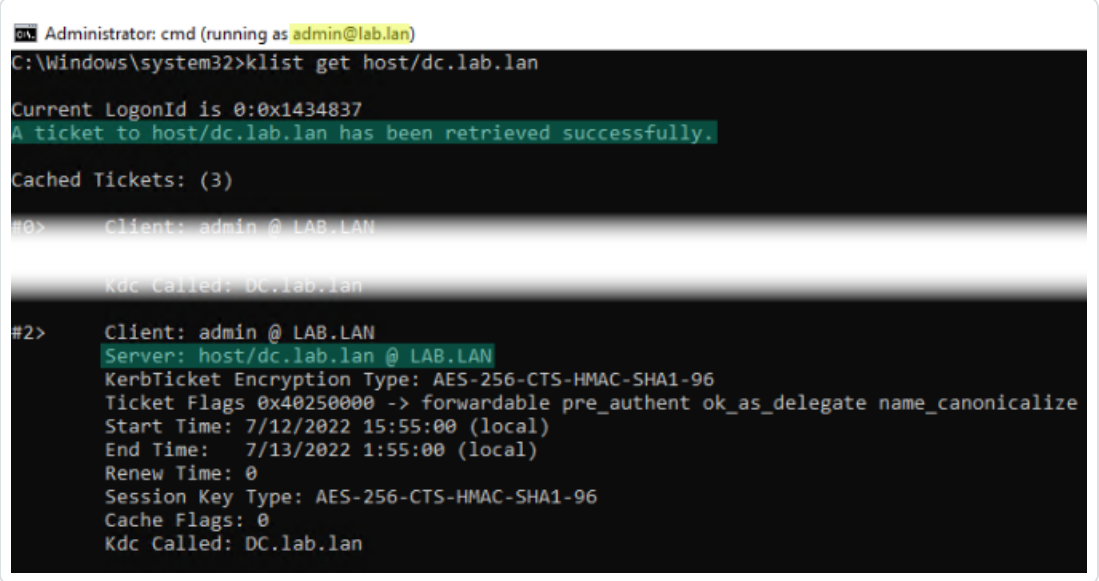


    Voici les codes d'erreur potentiels :

- `0xc0000064` : « User logon with misspelled or bad user account » (Connexion utilisateur avec un compte utilisateur mal orthographié ou incorrect) -> Vérifiez l'identifiant (c'est-à-dire la partie avant « @ » dans l'UPN).
- `0xc000006a` : « User logon with misspelled or bad password » (Connexion utilisateur avec un mot de passe mal orthographié ou incorrect) -> Vérifiez le mot de passe.
- `0xc000005e` : « There are currently no logon servers available to service the logon request. » (Il n'existe actuellement aucun serveur de connexion disponible pour répondre à la demande de connexion.) -> Vérifiez que la résolution DNS fonctionne, que le serveur peut contacter le ou les KDC retournés, etc.
- Autres codes d'erreur : voir la documentation de Microsoft relative aux événements 4625.

2. Vérifiez que le contrôleur de domaine configuré dans Tenable Identity Exposure peut obtenir un ticket de service. Dans la même deuxième invite de commandes, exécutez « `klist get host/<DC_FQDN>` » (remplacez « `<DC_FQDN>` »).

   L'exemple suivant montre un résultat correct :



Alertes

Licence requise : selon le type d'alerte que vous souhaitez envoyer, vous pouvez avoir besoin de licences pour les indicateurs d'attaque ou les indicateurs d'exposition.

Le système d'alerte de Tenable Identity Exposure permet d'identifier les régressions de sécurité et/ou les attaques au sein de votre infrastructure Active Directory supervisée. Il envoie les données d'analyse sur les vulnérabilités et les attaques en temps réel par e-mail ou par notification Syslog.

- Configuration de serveur SMTP
- Alertes par e-mail
- Alertes Syslog
- Détails des alertes Syslog et par e-mail

Configuration de serveur SMTP

Tenable Identity Exposure nécessite de configurer le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des notifications d'alerte.

Différences dans l'architecture de déploiement

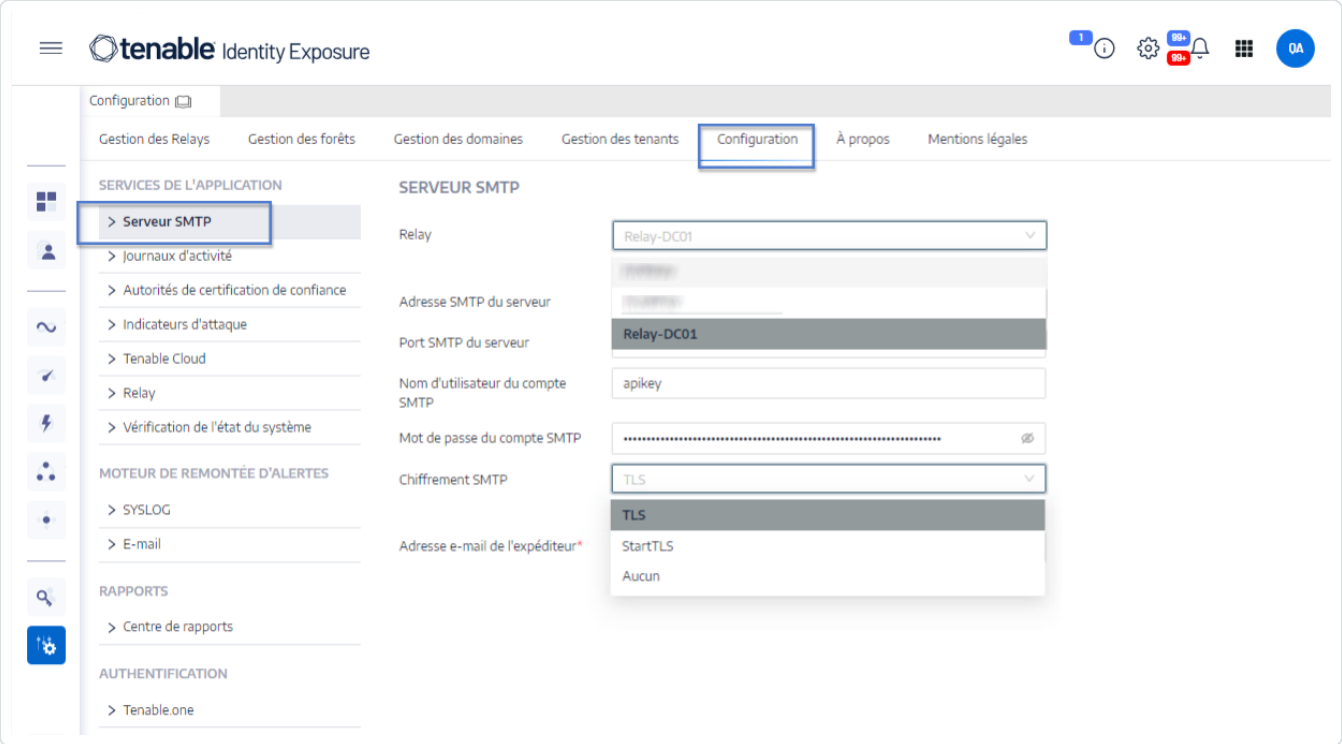
- Architecture **Secure Relay** :
  - Le Secure Relay est **installé dans l'environnement du client**.
  - Vous gérez la communication entre le Secure Relay et le serveur SMTP/SYSLOG.
- Architecture **VPN** :
  - Le service Secure Relay est **hébergé sur le cloud de Tenable**.
  - Vous ouvrez une demande d'assistance avec Tenable pour gérer la communication des alertes.

Configuration du serveur SMTP pour les environnements Secure Relay

Pour configurer le serveur SMTP **pour Secure Relay** :

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Configuration**.
2. Sous **Services de l'application**, sélectionnez **Vérification de l'état du système**.

   Le volet **Serveur SMTP** apparaît.



3. **Si votre réseau utilise Secure Relay :** dans la zone **Relay**, cliquez sur la flèche pour sélectionner un Relay pour communiquer avec votre serveur SMTP dans la liste déroulante.
4. Fournissez les informations suivantes :
   - Adresse du serveur SMTP
   - Port du serveur SMTP
   - Nom d'utilisateur du compte SMTP
   - Mot de passe du compte SMTP
5. Dans la zone Chiffrement SMTP, cliquez sur la flèche pour sélectionner une méthode de chiffrement dans la liste déroulante.
6. Dans la zone **Adresse e-mail de l'expéditeur**, fournissez l'adresse e-mail que Tenable Identity Exposure doit utiliser lors de l'envoi d'e-mails.

7. Cliquez sur **Enregistrer**.

   Un message confirme que Tenable Identity Exposure a mis à jour les paramètres SMTP.

Configuration du serveur SMTP pour les environnements VPN

Pour configurer le serveur SMTP **pour le VPN** :

1. Déterminez si le serveur SMTP est hébergé :
   - **À l'intérieur** du réseau du client (**privé**).
   - **En dehors** du réseau du client (**public**).
2. Selon votre configuration réseau :
   - Pour un serveur SMTP hébergé **à l'intérieur** du réseau du client :
     - Fournissez l'adresse IP privée du serveur SMTP à Tenable en ouvrant une demande d'assistance. Demandez également l'ajout de cette adresse IP à une liste blanche pour assurer la communication au sein du tunnel VPN.
     - Attendez que l'équipe de développement de Tenable ait terminé la configuration.
     - Testez le tunnel VPN pour confirmer la connectivité entre Tenable Cloud et le serveur SMTP interne.
   - Pour un serveur SMTP hébergé **en dehors** du réseau du client :
     - Vérifiez si le serveur SMTP externe filtre les connexions entrantes :
       - Si le trafic entrant **est filtré** en fonction de l'adresse IP source :
         - Ouvrez une demande d'assistance auprès de Tenable pour demander l'adresse IP d'alerte pour le tunnel VPN.
         - Contactez le fournisseur du serveur SMTP externe pour ajouter l'adresse IP d'alerte de Tenable à la liste blanche.

        - Si le trafic entrant **n'est pas filtré** : vérifiez que l'adresse IP publique du serveur SMTP est accessible via le tunnel VPN.

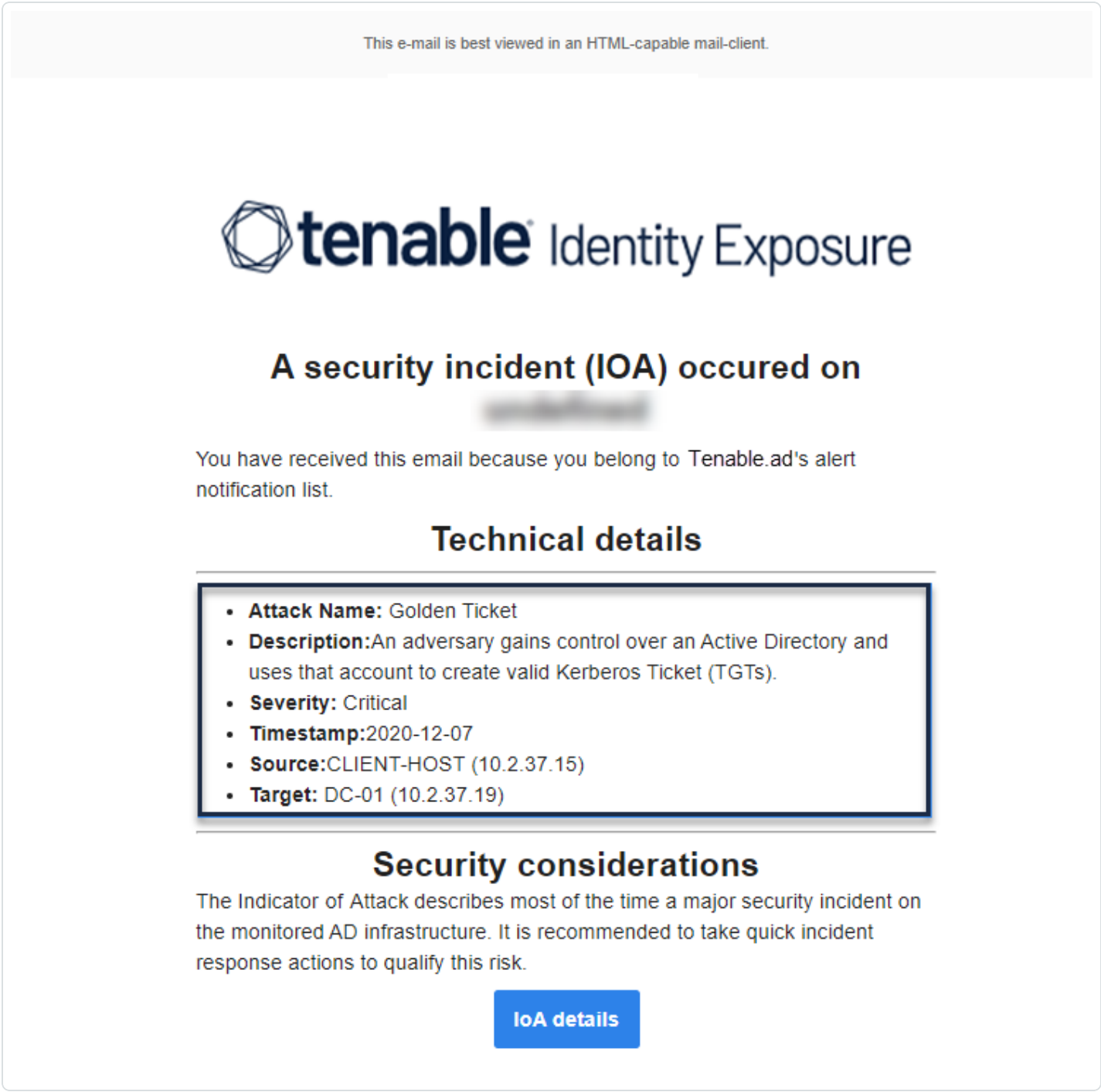
3. **Maintenance en cours** : informez Tenable de toute modification de l'adresse IP privée ou publique du serveur SMTP afin de maintenir la fonctionnalité du tunnel VPN.

Résolution des problèmes courants

- **Impossible d'envoyer des alertes** (SMTP/SYSLOG) :
    - Vérifiez que le serveur SMTP (privé ou public) est accessible via le tunnel VPN.
    - Confirmez que l'adresse IP est sur liste blanche aux deux extrémités (Tenable Cloud et serveur SMTP).
- **Expiration de la connexion** :
    - Vérifiez l'activité du tunnel VPN et la configuration du routage.

Alertes par e-mail

Tenable Identity Exposure envoie des alertes par e-mail pour vous signaler automatiquement que les événements atteignent un certain seuil de sévérité et nécessitent des actions de remédiation. Voici un exemple d'alerte par e-mail :



Pour ajouter une alerte e-mail

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Configuration** > **E-mail**.
2. Cliquez sur le bouton **Ajouter une alerte e-mail** sur la droite.

   Le volet **Ajouter une alerte e-mail** apparaît.

3. Dans la section **Informations principales**, fournissez les éléments suivants :
    - Dans la zone **Adresse e-mail**, saisissez l'adresse e-mail du destinataire des notifications.
    - Dans la zone **Description**, saisissez la description l'adresse du destinataire.
4. Dans la liste déroulante **Déclencher les alertes**, sélectionnez l'une des options suivantes :
    - **À chaque déviance** : Tenable Identity Exposure envoie une notification chaque fois qu'un IoE déviant est détecté.
    - **À chaque attaque** : Tenable Identity Exposure envoie une notification chaque fois qu'un IoA déviant est détecté.
    - **À chaque changement de statut de l'état du système** : Tenable Identity Exposure envoie une notification chaque fois qu'un statut de l'état du système change.
5. Dans la zone **Profils**, cliquez pour sélectionner le ou les profils à utiliser pour l'alerte par e-mail (le cas échéant).
6. **Envoyer des alertes quand des déviances sont détectées pendant la phase d'analyse initiale** : exécutez l'une des actions suivantes (le cas échéant) :
    - Cochez la case : Tenable Identity Exposure envoie un grand volume de notifications par e-mail lorsqu'un redémarrage du système déclenche des alertes.
    - Décochez la case : Tenable Identity Exposure n'envoie pas de notifications par e-mail lorsqu'un redémarrage du système déclenche des alertes.
7. **Seuil de sévérité** : cliquez sur la flèche de la zone déroulante pour sélectionner le seuil auquel Tenable Identity Exposure envoie des alertes (le cas échéant).
8. En fonction du déclencheur d'alerte que vous avez sélectionné précédemment :
    - **Indicateurs d'exposition** : si vous définissez des alertes pour qu'elles se déclenchent **à chaque déviance**, cliquez sur la flèche à côté de chaque niveau de sévérité pour développer la liste des indicateurs d'exposition et sélectionner ceux pour lesquels des alertes doivent être envoyées.

- **Indicateurs d'attaque** : si vous définissez des alertes pour qu'elles se déclenchent **à chaque attaque**, cliquez sur la flèche à côté de chaque niveau de sévérité pour développer la liste des indicateurs d'attaque et sélectionner ceux pour lesquels des alertes doivent être envoyées.
- **Changement du statut de l'état du système** : cliquez sur **Vérifications de l'état du système** pour sélectionner le type de vérification de l'état du système qui doit déclencher une alerte, puis cliquez sur **Filtrer sur la sélection**.

9. Cliquez sur la zone **Domaines** pour sélectionner les domaines pour lesquels Tenable Identity Exposure envoie des alertes.

   Le volet Forêts et domaines apparaît.

   a. Sélectionnez la forêt ou le domaine.

   b. Cliquez sur **Filtrer sur la sélection**.

10. Cliquez sur **Tester la configuration**.

    Un message confirme que Tenable Identity Exposure a envoyé une alerte e-mail au serveur.

11. Cliquez sur **Ajouter**.

    Un message confirme que Tenable Identity Exposure a créé l'alerte e-mail.

Pour modifier une alerte e-mail

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Configuration** > **E-mail**.
2. Dans la liste des alertes e-mail, survolez celle que vous souhaitez modifier et cliquez sur l'icône en fin de ligne.

   Le volet **Modifier une alerte e-mail** apparaît.

3. Apportez les modifications nécessaires comme décrit dans la procédure précédente « Pour ajouter une alerte e-mail ».
4. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour l'alerte.

Pour supprimer une alerte e-mail

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Configuration** > **E-mail**.
2. Dans la liste des alertes e-mail, survolez celle que vous souhaitez supprimer et cliquez sur l'icône  en fin de ligne.

   Un message demande de confirmer la suppression.
3. Cliquez sur **Supprimer**.

   Un message confirme que Tenable Identity Exposure a supprimé l'alerte.

Voir aussi

- Configuration de serveur SMTP
- Détails des alertes Syslog et par e-mail

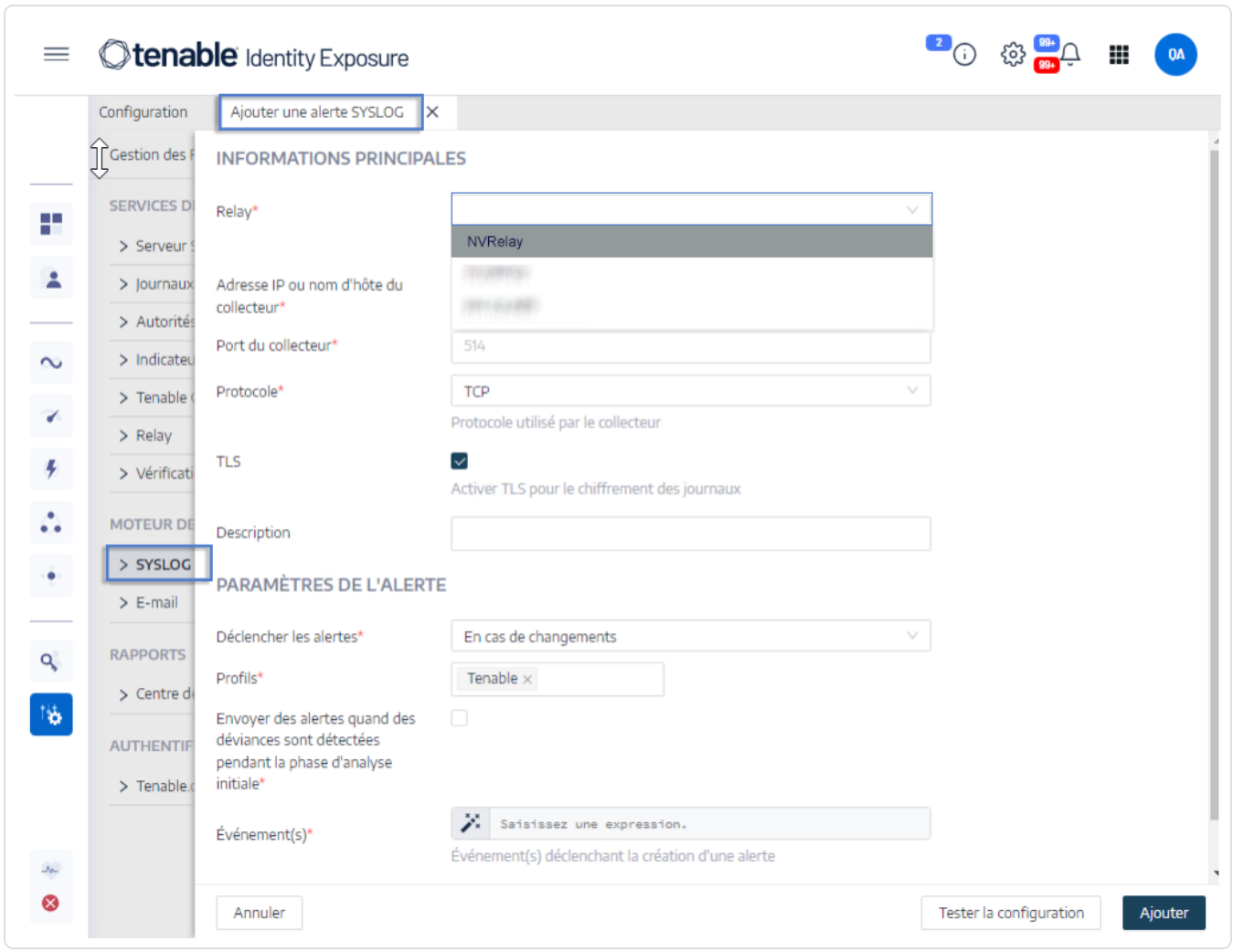
Alertes Syslog

Certaines organisations utilisent un SIEM (outil de gestion des informations et des événements de sécurité) pour collecter des journaux sur les menaces potentielles et les incidents de sécurité. Tenable Identity Exposure peut envoyer les informations de sécurité liées à Active Directory aux serveurs Syslog SIEM pour améliorer leurs mécanismes d'alerte.

Pour ajouter une nouvelle alerte Syslog

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Configuration** > **Syslog**.
2. Cliquez sur le bouton **Ajouter une alerte Syslog** sur la droite.

   Le volet **Ajouter une alerte Syslog** apparaît.



3. Dans la section **Informations principales**, fournissez les éléments suivants :
    - **Si votre réseau utilise Secure Relay :** dans la zone **Relay**, cliquez sur la flèche pour sélectionner un Relay pour communiquer avec votre outil SIEM dans la liste déroulante.
    - Dans la zone **Adresse IP ou nom d'hôte du collecteur**, saisissez l'adresse IP ou le nom d'hôte du serveur qui reçoit des notifications.
    - Dans la zone **Port**, saisissez le numéro de port du collecteur.
    - Dans la zone **Protocole**, cliquez sur la flèche pour sélectionner UDP ou TCP.
        - Si vous choisissez TCP, cochez la case de l'option **TLS** pour activer le protocole de sécurité TLS en vue de chiffrer les journaux.

- Dans la zone **Description**, saisissez une brève description du collecteur.

4. Dans la liste déroulante **Déclencher les alertes**, sélectionnez l'une des options suivantes :
   - **À chaque changement** : Tenable Identity Exposure envoie une notification chaque fois qu'un événement que vous avez spécifié se produit.
   - **À chaque déviance** : Tenable Identity Exposure envoie une notification chaque fois qu'un IoE déviant est détecté.
   - **À chaque attaque** : Tenable Identity Exposure envoie une notification chaque fois qu'un IoA déviant est détecté.
   - **À chaque changement de statut de l'état du système** : Tenable Identity Exposure envoie une notification chaque fois qu'un statut de l'état du système change.
5. Dans la zone **Profils**, cliquez pour sélectionner le profil à utiliser pour l'alerte Syslog (le cas échéant).
6. **Envoyer des alertes quand des déviances sont détectées pendant la phase d'analyse initiale** : exécutez l'une des actions suivantes (le cas échéant) :
   - Cochez la case : Tenable Identity Exposure envoie un grand volume de messages Syslog lorsqu'un redémarrage du système déclenche des alertes.
   - Décochez la case : Tenable Identity Exposure n'envoie pas de messages Syslog lorsqu'un redémarrage du système déclenche des alertes.
7. **Seuil de sévérité** : cliquez sur la flèche de la zone déroulante pour sélectionner le seuil auquel Tenable Identity Exposure envoie des alertes (le cas échéant).
8. En fonction du déclencheur d'alerte que vous avez sélectionné précédemment :
   - **Modifications** : si vous avez configuré des alertes pour qu'elles se déclenchent **en cas de changement**, saisissez une expression pour déclencher la notification d'événement.

     Vous pouvez cliquer sur l'icône pour utiliser l'assistant de recherche ou saisir une expression de requête dans la zone de recherche et cliquer sur **Valider**. Pour plus d'informations, voir Personnaliser les requêtes Trail Flow.

> **Remarque** : Tenable Identity Exposure applique ce filtre dès qu'il reçoit des événements pour les transférer à Syslog avant d'effectuer une analyse de sécurité supplémentaire. Par conséquent, les filtres qui s'appuient sur des données enrichies ou post-traitées ne fonctionneront pas à ce stade.

- **Indicateurs d'exposition** : si vous définissez des alertes pour qu'elles se déclenchent **à chaque déviance**, cliquez sur la flèche à côté de chaque niveau de sévérité pour développer la liste des indicateurs d'exposition et sélectionner ceux pour lesquels des alertes doivent être envoyées.
- **Indicateurs d'attaque** : si vous définissez des alertes pour qu'elles se déclenchent **à chaque attaque**, cliquez sur la flèche à côté de chaque niveau de sévérité pour développer la liste des indicateurs d'attaque et sélectionner ceux pour lesquels des alertes doivent être envoyées.
- **Changement du statut de l'état du système** : cliquez sur **Vérifications de l'état du système** pour sélectionner le type de vérification de l'état du système qui doit déclencher une alerte, puis cliquez sur **Filtrer sur la sélection**.

9. Cliquez sur la zone **Domaines** pour sélectionner les domaines pour lesquels Tenable Identity Exposure envoie des alertes.

   Le volet **Forêts et domaines** apparaît.

   a. Sélectionnez la forêt ou le domaine.

   b. Cliquez sur **Filtrer sur la sélection**.

10. Cliquez sur **Tester la configuration**.

    Un message confirme que Tenable Identity Exposure a envoyé une alerte Syslog au serveur.

11. Cliquez sur **Ajouter**.

    Un message confirme que Tenable Identity Exposure a créé l'alerte Syslog.

Pour modifier une alerte Syslog

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Configuration** > **Syslog**.
2. Dans la liste des alertes Syslog, survolez avec la souris celle que vous souhaitez modifier et cliquez sur l'icône en fin de ligne.

   Le volet **Modifier une alerte Syslog** apparaît.
3. Apportez les modifications nécessaires comme décrit dans la procédure précédente « Pour ajouter une nouvelle alerte Syslog ».
4. Cliquez sur **Modifier**.

   Un message confirme que Tenable Identity Exposure a mis à jour l'alerte.

Pour supprimer une alerte Syslog

1. Dans Tenable Identity Exposure, cliquez sur **Système** > **Configuration** > **Syslog**.
2. Dans la liste des alertes Syslog, survolez celle que vous souhaitez supprimer et cliquez sur l'icône en fin de ligne.

   Un message demande de confirmer la suppression.
3. Cliquez sur **Supprimer**.

   Un message confirme que Tenable Identity Exposure a supprimé l'alerte.

Voir aussi

- Détails des alertes Syslog et par e-mail

Détails des alertes Syslog et par e-mail

Lorsque vous activez Syslog ou les alertes par e-mail, Tenable Identity Exposure envoie des notifications lorsqu'il détecte une déviance, une attaque ou un changement.

Remarque : un certain temps d'intégration doit être respecté avant de pouvoir recevoir des alertes IoA. Ce délai est différent de celui observé pendant la phase de « test de la configuration » lorsque vous configurez Syslog et les alertes par e-mail. Par conséquent, la durée du test de la configuration ne doit pas servir de référence ; elle ne doit pas être comparée au moment où les alertes sont déclenchées par une attaque réelle.

En-tête d'alerte

Les en-têtes d'alerte Syslog (RFC-3164) utilisent le format d'événement commun (CEF), un format couramment employé par les solutions de gestion des informations et des événements de sécurité (SIEM).

Exemple d'alerte pour un indicateur d'exposition (IoE)

En-tête d'alerte IoE

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "0" "1" "Alsid Forest" "emea.corp" "C-PASSWORD-DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-DONT-EXPIRE-SET" "2434" "TrusteeCn"="Gustavo Fring"
```

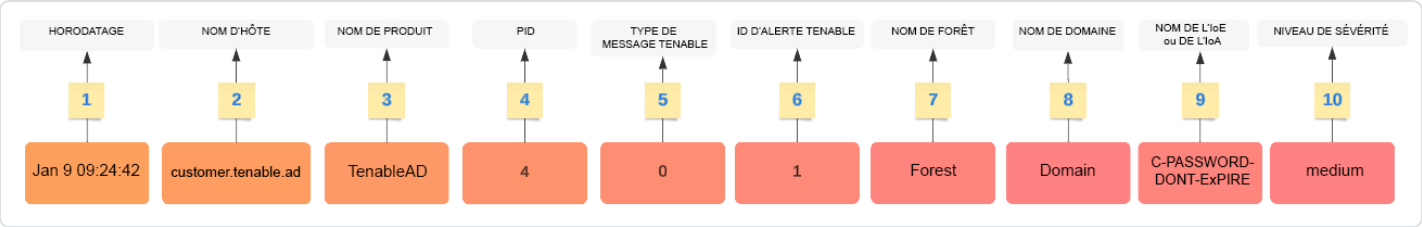
Exemple d'alerte pour un indicateur d'attaque (IoA)

En-tête d'alerte IoA

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "2" "1337" "Alsid Forest" "emea.corp" "DC Sync" "medium" "yoda.alsid.corp" "10.0.0.1" "antoinex1x.alsid.corp" "10.1.0.1" "user"="Gustavo Fring" "dc_name"="MyDC"
```

Informations sur les alertes

Éléments génériques

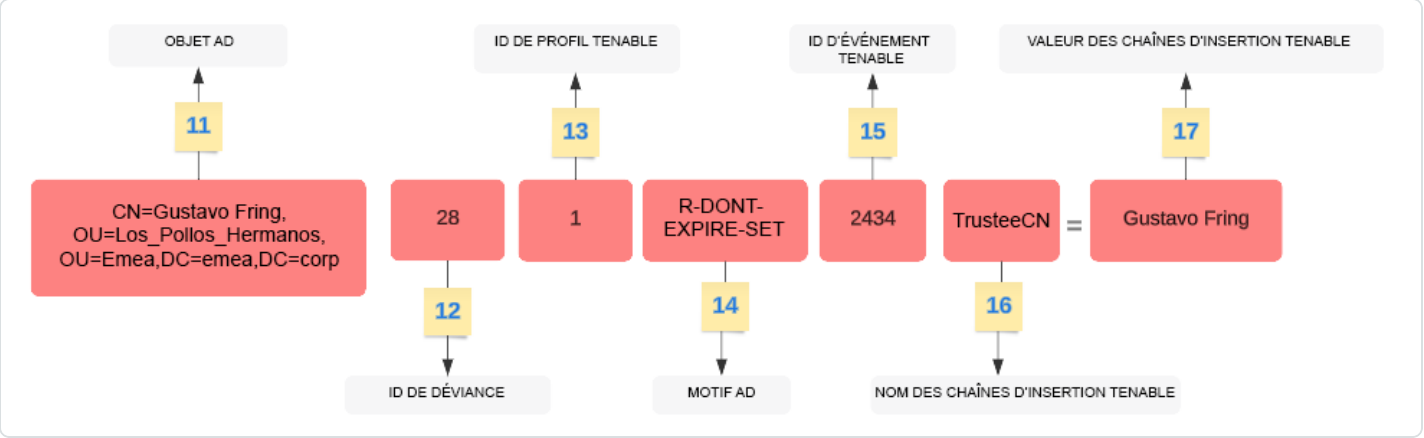


La structure d'en-tête comprend les éléments suivants, comme décrit dans le tableau.

Élément	Description
1	**Horodatage** – Date de la détection. Exemple : « 7 juin 05:37:03 »
2	**Nom d'hôte** – Nom d'hôte de votre application. Exemple : « customer.tenable.ad »

3	**Nom du produit** – Nom du produit qui a déclenché la déviance. Exemple : « TenableAD », « AutreProduitTenableAD »
4	**PID** – ID (Tenable Identity Exposure) du produit. Exemple : [4]
5	**Type de message Tenable** – Identifiant des sources d'événements. Exemple : « 0 » (= À chaque déviance), « 1 » (= En cas de changement), « 2 » (= À chaque attaque), « 3 » (= À chaque changement de l'état du système)
6	**ID de l'alerte Tenable** – Identifiant unique de l'alerte. Exemple : « 0 », « 132 »
7	**Nom de la forêt** – Nom de la forêt de l'événement connexe. Exemple : « Forêt Corp »
8	**Nom de domaine** – Nom de domaine lié à l'événement. Exemple : « tenable.corp », « zwx.com »
9	**Nom de code deTenable** – Nom de code de l'indicateur d'exposition (IoE) ou de l'indicateur d'attaque (IoA). Exemples : « C-PASSWORD-DONT-EXPIRE », « DC Sync ».
10	**Niveau de sévérité Tenable** – Niveau de sévérité de la déviance associée. Exemple : « critique », « élevé », « moyen »

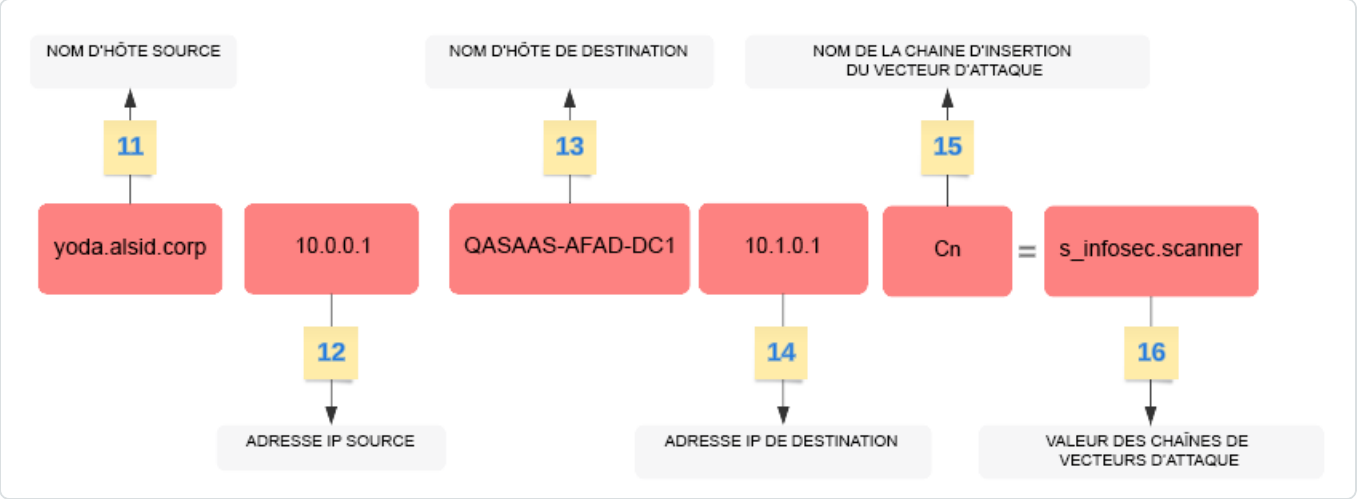
Éléments spécifiques aux IoE



Élément	Description
11	**Objet AD** – Nom distinctif de l'objet déviant. Exemple : « CN=s_

	infosec.scanner,OU=ADManagers,DC=domaine,DC=local »
12	**ID de déviance Tenable** – Identifiant de la déviance. Exemple : « 24980 », « 132 », « 28 »
13	**ID de profil Tenable** – Identifiant du profil sur lequel Tenable Identity Exposure a déclenché la déviance. Exemple : « 1 » (Tenable), « 2 » (sec_team)
14	**Nom du code de motif AD**– Nom de code du motif de la déviance. Exemple : « R-DONT-EXPIRE-SET », « R-UNCONST-DELEG »
15	**ID d'événement Tenable** – Identifiant de l'événement déclenché par la déviance. Exemple : « 40667 », « 28 »
16	**Nom des chaînes d'insertion Tenable** – Nom de l'attribut que l'objet déviant a déclenché. Exemple : « Cn », « useraccountcontrol », « member », « pwdlastset »
17	**Valeur des chaînes d'insertion Tenable** – Valeur de l'attribut que l'objet déviant a déclenché. Exemple : « s_infosec.scanner », « CN=Backup Operators,CN=Builtin,DC=domain,DC=local »

Éléments spécifiques IoA



Élément	Description
11	**Nom d'hôte source** – Nom de l'hôte attaquant. La valeur peut également être « Inconnue ».

12	**Adresse IP source** – Adresse IP de l'hôte attaquant. Les valeurs peuvent être IPv4 ou IPv6.
13	**Nom d'hôte de destination** – Nom de l'hôte attaqué.
14	**Adresse IP de destination** – Adresse IP de l'hôte attaqué. Les valeurs peuvent être IPv4 ou IPv6.
15	**Nom des chaînes d'insertion de vecteur d'attaque** – Nom de l'attribut que l'objet déviant a déclenché.
16	**Valeur des chaînes d'insertion de vecteur d'attaque** – Valeur de l'attribut que l'objet déviant a déclenché.

Encadrement des messages Syslog

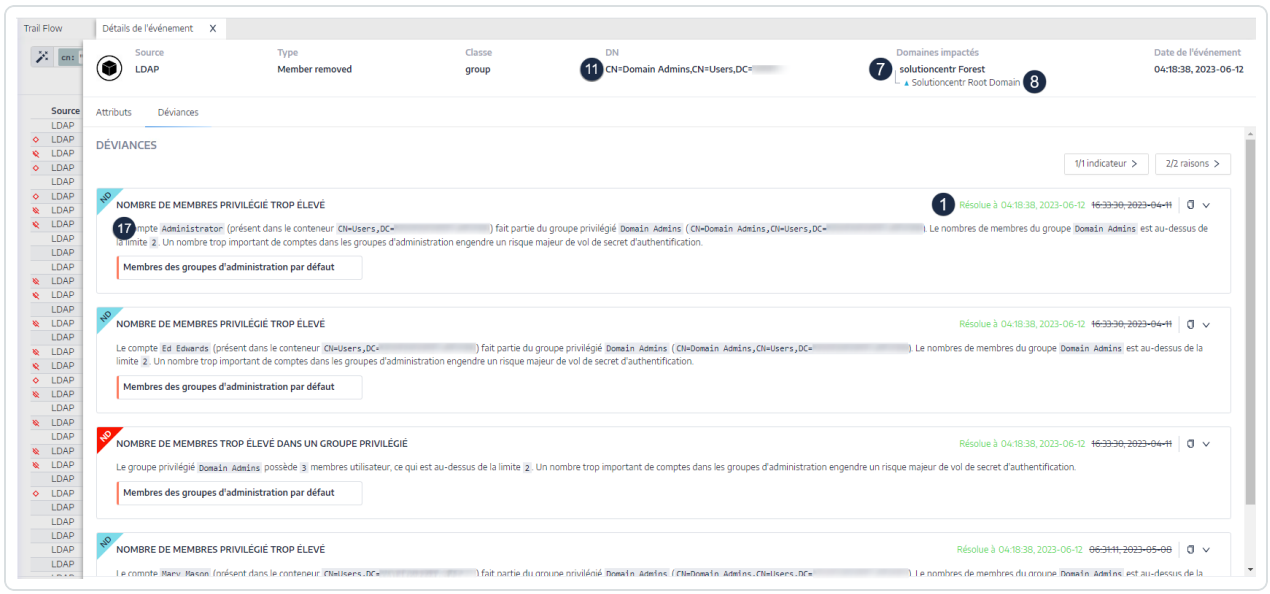
- Pour la configuration syslog UDP et TCP, Tenable Identity Exposure utilise la méthode d'encadrement non transparent selon la norme RFC-6587#3.4.2 pour délimiter les messages. Le caractère d'encadrement est LF (\n).
- Pour TCP avec TLS, Tenable Identity Exposure utilise la méthode de comptage d'octets décrite dans la norme RFC-6587#3.4.1.

Exemples

Détails de l'événement Trail Flow

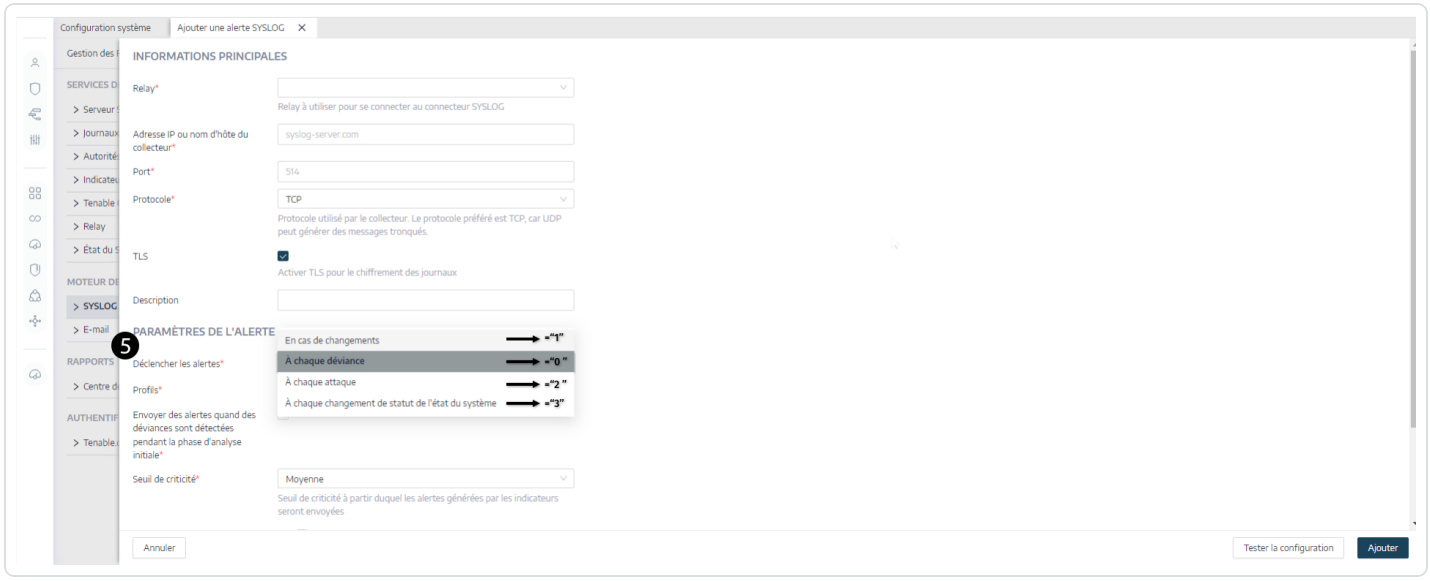
L'exemple suivant montre les détails d'un événement dans le Trail Flow contenant les éléments suivants :

- L'horodatage (1)
- Le nom d'objet déviant (11)
- Les noms de forêt (7) et de domaine (8)
- Valeur de l'attribut que l'objet déviant a déclenché (17)



Source de l'événement

Cet exemple affiche la source de l'événement (5). Vous définissez ce paramètre dans la page de configuration Syslog. Pour plus d'informations, voir Alertes Syslog.



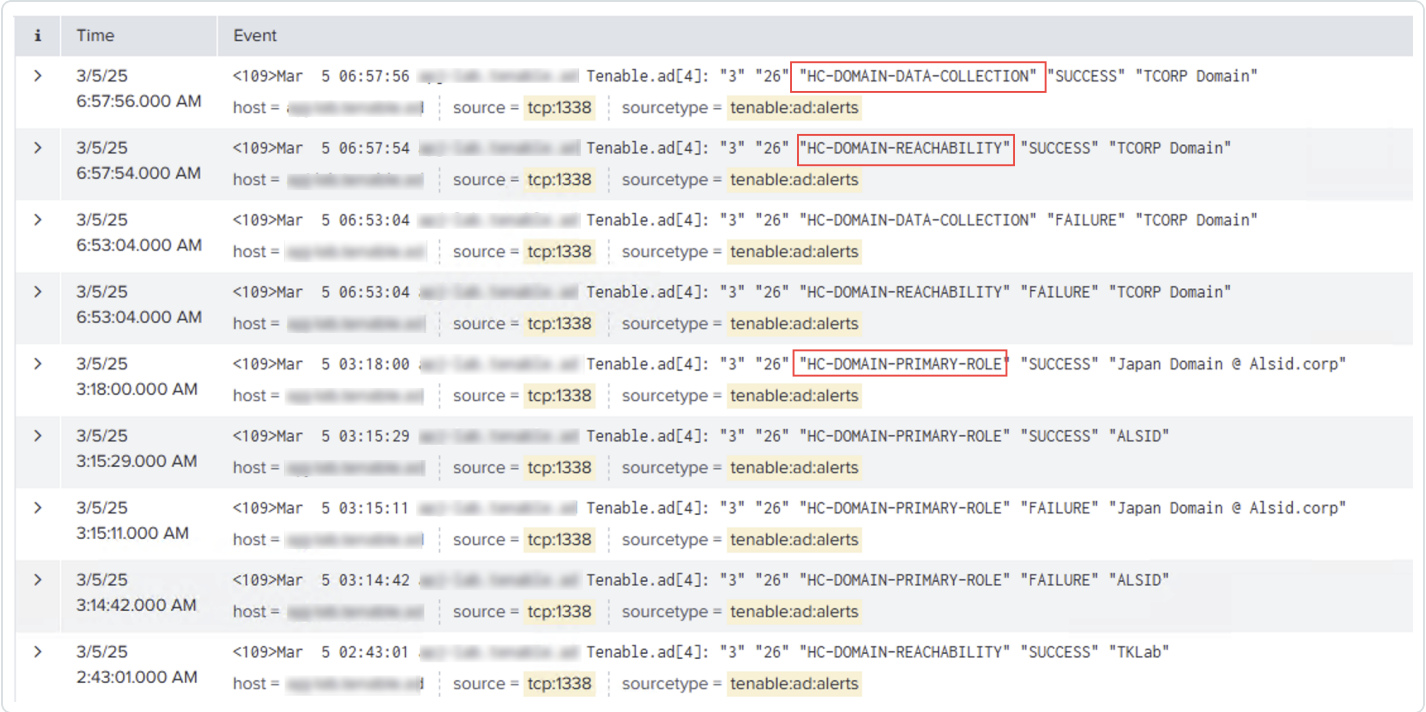
ID de l'alerte

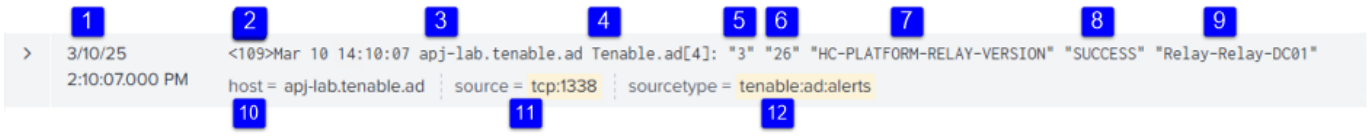
Cet exemple montre l'identifiant unique de l'alerte (6), que vous pouvez voir dans la liste des adresses e-mail configurées dans Tenable Identity Exposure sous **Système** > **Configuration** > **E-mail**.



Vérifications de l'état du système

Cet exemple affiche les résultats des vérifications de l'état du système effectuées par Tenable Identity Exposure dans votre environnement. Pour plus d'informations, voir [Vérifications de l'état du système](#).





La structure d'en-tête comprend les éléments suivants, comme décrit dans le tableau.

Élément	Description

1	**Horodatage** – Indique la date et l'heure auxquelles l'événement a été détecté.
2	**Priorité Syslog** – Il s'agit de la valeur de priorité syslog, combinant les niveaux d'installation et de sévérité (RFC-3164)
3	**Nom d'hôte** – Le nom d'hôte de l'application ou de l'appareil qui a généré l'alerte.
4	**Nom du produit et PID** – Spécifie le nom du produit et son ID de processus.
5	**Type de message Tenable** – Identifiant des sources d'événements. Exemple : « 0 » (= À chaque déviance), « 1 » (= En cas de changement), « 2 » (= À chaque attaque), « 3 » (= À chaque changement de l'état du système)
6	**ID de l'alerte Tenable** – Identifiant unique de l'alerte. Exemple : « 0 », « 132 »
7	**Nom de code de la vérification de l'état du système** – Indique la vérification de l'état du système spécifique effectuée. Pour plus d'informations, voir Vérifications de l'état du système.
8	**Statut de la vérification de l'état du système** – Indique le résultat de la vérification de l'état du système.
9	**Nom du Relay ou Nom de domaine** – Identifie le Relay ou le contrôleur de domaine associé à cette vérification de l'état du système.
10-12	**Champs de métadonnées** : • Hôte (10) : répète le nom d'hôte à des fins d'indexation et de recherche. • Source (11) : spécifie la source du journal. • Type de source (12) : catégorise le format du journal pour l'analyse.

Vérifications de l'état du système

La fonctionnalité **Vérification de l'état du système** dans Tenable Identity Exposure vous offre une visibilité en temps réel sur la configuration de vos domaines et comptes de service dans une vue consolidée unique, à partir de laquelle vous pouvez lancer une exploration détaillée pour rechercher toute anomalie de configuration entraînant des problèmes de connectivité ou autres dans vos infrastructures. Elle vérifie que tout est correctement configuré pour assurer le bon fonctionnement

de Tenable Identity Exposure et vous donne la possibilité de prendre des mesures rapidement et précisément pour remédier aux problèmes. Elle vous donne également l'assurance que vos paramètres de configuration sont optimaux pour permettre à Tenable Identity Exposure de fonctionner efficacement.

Les vérifications de l'état du système sont visibles par défaut pour les rôles d'administrateur et en fonction des autorisations pour certains rôles d'utilisateur. Vous pouvez également créer des alertes Syslog ou par e-mail à chaque modification du statut de vérification de l'état du système.

Vérifications de l'état du système et détection d'attaque DCSync

Les vérifications de l'état du système fournissent des informations précieuses sur le statut et l'utilisation des services Tenable Identity Exposure. Elles vérifient la capacité du compte de service à collecter des informations sensibles telles que les empreintes de mot de passe et les clés de sauvegarde DPAPI utilisées pour l'analyse privilégiée. Dans le rapport de vérification de l'état du système, Tenable tente de collecter des données sensibles pour déterminer si la fonctionnalité Analyse privilégiée est correctement configurée pour le compte de service. Rien n'est collecté si elle n'est pas utilisée. Pour empêcher la détection d'une attaque DCSync pendant ce processus, Tenable ajoute automatiquement le compte de service fourni à la liste d'autorisation pour l'indicateur d'attaque DCSync.

Statut des domaines

Tenable Identity Exposure effectue les vérifications suivantes pour chaque domaine :

- Authentification au domaine AD — Paramètres et statut LDAP, identifiants, et accès SMB
- Accessibilité du domaine — Connexion au port RPC dynamique fonctionnelle, à un serveur SMB accessible, à une adresse IP ou au FQDN d'un contrôleur de domaine accessible, connexion fonctionnelle au port RPC, à un serveur LDAP accessible et à un serveur LDAP de catalogue global accessible.
- Autorisations — Possibilité d'accéder aux données du domaine AD et de collecter des données privilégiées.
- Domaine lié à un Relay — Le domaine est correctement associé à un service Relay.
- Indicateurs d'attaque : activité des contrôleurs de domaine — Tenable Identity Exposure Reçoit les journaux d'événements Windows de tous les contrôleurs de domaine.

- Indicateurs d'attaque : installation du domaine – Vérifie que la configuration de la GPO de l'IoA Tenable est correcte.

Statut de la plateforme

Tenable Identity Exposure effectue les vérifications suivantes sur la configuration de votre plateforme :

- Fonctionnement du service Relay – Vérifie si la configuration du Relay est correcte ou non en fournissant des conseils de dépannage.
- Cohérence de la version du Relay – Vérifie si la version du Relay est compatible ou non avec la version de Tenable Identity Exposure.
- Fonctionnement du service Collecteur de données AD – Vérifie si le service Collecteur de données, le Broker et le pont du collecteur sont opérationnels et capables de relayer les données vers d'autres services.

Pour accéder aux vérifications de l'état du système :

1. Dans l'angle inférieur gauche de la page Tenable Identity Exposure, survolez l'icône  pour identifier l'état global de votre infrastructure.
2. Cliquez sur l'icône pour ouvrir la page **Vérification de l'état du système**. Sous l'onglet **Statut du domaine** ou **Statut de la plateforme**, figure l'un ou l'autre des éléments suivants :
    - Message indiquant que les vérifications de l'état du système ont réussi
    - Liste d'avertissements ou de problèmes avec des statuts spécifiques :

	La vérification a réussi et affiche un résultat normal.
	La vérification a échoué et identifie un problème.
	La vérification a échoué, mais le problème n'empêche pas Tenable Identity Exposure de fonctionner correctement. Par exemple, la vérification de la collecte de données

	entraînera un échec en raison d'une mauvaise configuration d'Active Directory côté client si le compte de service ne peut pas collecter de données privilégiées. Cependant, il ne s'agit pas d'un problème grave, car vous n'avez pas activé la fonctionnalité Analyse privilégiée sur ce domaine dans Tenable Identity Exposure, d'où l'avertissement. Mais si vous l'activez, la vérification échoue immédiatement.
	La vérification affiche un résultat inconnu, car une vérification dépendante a échoué. Par exemple, la vérification de l'accessibilité du réseau ne peut pas continuer si la vérification de l'authentification a échoué.

Pour voir toutes les vérifications de l'état du système :

- Au-dessus de la liste des vérifications de l'état du système sur la droite, cliquez sur le curseur **Afficher les vérifications réussies** pour afficher la liste de toutes les vérifications que Tenable Identity Exposure a effectuées avec les informations suivantes :
    - Nom de la vérification de l'état du système
    - Statut (succès, échec, échec mais non bloquant ou inconnu)
    - Domaine impacté et sa forêt associée (uniquement pour les vérifications de statut de domaine)
    - Date/heure de la dernière vérification effectuée
    - Durée du statut de la vérification

Pour actualiser la page Vérification de l'état du système :

- Bien qu'il vérifie régulièrement l'état du système, Tenable Identity Exposure n'actualise pas la page des résultats en temps réel. Cliquez sur  pour actualiser la liste des résultats.

Pour filtrer les résultats par type de vérification d'état du système ou par domaine :

1. Au-dessus de la liste des vérifications de l'état du système sur la droite, cliquez sur **n/n vérifications** ou **n/n domaines** (uniquement pour le statut de domaine).

   Le volet **Vérifications de l'état du système** ou **Forêts et domaines** apparaît.

2. Sélectionnez les types de vérifications de l'état du système ou les forêts/domaines (le cas échéant) et cliquez sur **Filtrer sur la sélection**.

Pour obtenir plus d'informations sur chaque vérification d'état du système :

1. Dans la liste des vérifications de l'état du système, cliquez sur un nom de vérification du système ou sur la flèche bleue (→) à la fin de la ligne.

   Le volet **Détails** apparaît et affiche la description de la vérification et la liste des détails pertinents. Pour plus d'informations, voir Liste des vérifications de l'état du système ci-dessous.

2. Cliquez sur la flèche à la fin de la ligne de détail pour la développer et afficher plus d'informations sur le résultat.

Pour masquer l'icône de statut de vérification de l'état du système :

Par défaut, Tenable Identity Exposure affiche cette icône dans l'angle inférieur gauche de l'écran.

1. Dans Tenable Identity Exposure, accédez à **Système** dans la barre de navigation de gauche et sélectionnez l'onglet **Configuration**.

   Vous pouvez également cliquer sur ··· dans l'angle supérieur droit de la page Vérification de l'état du système et sélectionner **Configuration**.

2. Sous **Services de l'application**, sélectionnez **Vérification de l'état du système**.

3. Cliquez sur le curseur **Afficher le statut global de l'état du système** pour désactiver la fonctionnalité.

   Tenable Identity Exposure masque l'icône de vérification de l'état du système dans l'angle inférieur gauche de l'écran.

Pour attribuer des autorisations de vérification de l'état du système à des rôles utilisateur :

1. Dans Tenable Identity Exposure, accédez à **Comptes** dans la barre de navigation de gauche et sélectionnez l'onglet **Gestion des rôles**.
2. Dans la liste des rôles, sélectionnez le rôle utilisateur et cliquez sur  à la fin de la ligne.

   Le volet **Modifier un rôle** apparaît.
3. Sélectionnez l'onglet **Entités de type Configuration système**.
4. Sélectionnez l'entité **Vérification de l'état du système** et cliquez sur le curseur d'autorisation pour passer de **Non autorisé** à **Autorisé**.
5. Cliquez sur **Appliquer et fermer**.

Pour plus d'informations sur les autorisations, voir Définir les autorisations d'un rôle.

Pour configurer des alertes en cas de changement du statut des vérifications de l'état du système :

1. Dans Tenable Identity Exposure, accédez à **Système** dans la barre de navigation de gauche et sélectionnez l'onglet **Configuration**.

   Vous pouvez également cliquer sur dans l'angle supérieur droit de la page Vérification de l'état du système et sélectionner **Alertes**.
2. Sous **Moteur de remontée d'alertes**, sélectionnez **Syslog** ou **E-mail**.
3. Cliquez sur **Ajouter une alerte Syslog** ou **Ajouter une alerte par e-mail**.

   Un nouveau volet apparaît. Pour la procédure complète, voir Alertes.
4. Sous **Paramètres d'alerte**, dans la zone **Déclencher l'alerte**, sélectionnez **À chaque changement de statut de l'état du système** dans le menu déroulant.
5. Cliquez sur la flèche dans la zone **Vérifications de l'état du système** pour sélectionner le type de vérification de l'état du système qui déclenchera une alerte, puis cliquez sur **Filtrer sur la sélection**.
6. Cliquez sur **Ajouter**.

Liste des vérifications de l'état du système

Nom de la vérification de l'état du système	Type	Description de la vérification	Détails
Accessibilité du domaine (HC-DOMAIN-REACHABILITY)	Domaine	Possibilité d'établir une connexion avec le domaine AD.	• Adresse IP ou FQDN du contrôleur de domaine joignable • Serveur LDAP catalogue global joignable • Serveur LDAP joignable • Serveur SMB joignable • Connexion au port dynamique RPC fonctionnelle • Connexion au port RPC fonctionnelle
Authentification au domaine AD (HC-DOMAIN-AUTHENTICATION)	Domaine	Possibilité de s'authentifier au domaine AD.	• Identifiants valides • Serveur LDAP non occupé • Serveur LDAP disponible • Accès LDAP autorisé • Accès SMB autorisé
Autorisations de	Domaine	Possibilité de	• Autorisations

collecter les données du domaine (HC-DOMAIN-DATA-COLLECTION)		collecter les données du domaine AD.	accordées pour collecter les données privilégiées
Autorisations d'accéder aux conteneurs AD (HC-DOMAIN-CONTAINER-ACCESS)	Domaine	Possibilité d'accéder aux conteneurs AD.	• Autorisations accordées pour accéder au conteneur des objets supprimés • Autorisations accordées pour accéder au conteneur des paramètres de mot de passe
Domaine AD lié à un Relay (HC-DOMAIN-LINKED-TO-RELAY)	Domaine	Le domaine est lié à un Relay.	• Liaison du domaine AD à un Relay
IoA – Activité des contrôleurs de domaine (HC-DOMAIN-EVENT-LOGS-COLLECTION-DOMAIN-CONTROLLER-ACTIVITY)	Domaine	Tenable Identity Exposure reçoit les journaux d'événements Windows de tous les contrôleurs de domaine.	• Contrôleurs de domaine inactifs
Le contrôleur de domaine supervisé possède le rôle PDCe (HC-DOMAIN-	Domaine	Le contrôleur de domaine surveillé détient le rôle d'émulateur de PDC	• Assure le fonctionnement optimal des indicateurs

PRIMARY-ROLE)		(PDCe), qui est essentiel pour certaines fonctionnalités de sécurité.	d'exposition (IoE) et des indicateurs d'attaque (IoA)
IoA - Installation du domaine (HC-DOMAIN-IOA-CONFIGURATION)	Domaine	Vérifie que la configuration de la GPO de l'IoA Tenable est correcte.	• La GPO de l'IoA Tenable existe dans LDAP • Le dossier de la GPO de l'IoA Tenable existe dans le SYSVOL • Le dossier de l'IoA de la GPO de l'IOA Tenable existe dans le SYSVOL • Le fichier de l'écouteur Tenable IoA GPO EVT Subscribe existe dans le SYSVOL • Le fichier de configuration de la GPO de l'IoA Tenable existe dans le SYSVOL • Le fichier `audit.csv` de la GPO de l'IoA Tenable existe

			dans le SYSVOL
Fonctionnement du Service Relay (HC-PLATFORM-RELAY-UP)	Plateforme	Le Relay fonctionne comme prévu.	• Le Service Relay fonctionne
Version du Service Relay (HC-PLATFORM-RELAY-VERSION)	Plateforme	La version du Relay est conforme à celle du produit.	• Cohérence de la version du Relay
Fonctionnement du collecteur de données AD (HC-PLATFORM-AD-DATA-COLLECTOR-UP)	Plateforme	Le collecteur de données AD fonctionne comme prévu.	• Le pont du collecteur de données AD fonctionne • Le service Collecteur de données AD fonctionne • Le Broker fonctionne
Synchronisation entre les services Tenable Cloud et Tenable Identity Exposure (HC-PLATFORM-TENABLE-CLOUD-SYNC)	Plateforme	Le groupe, les autorisations et les utilisateurs Tenable Cloud créés sont synchronisés avec la base de données Tenable Identity Exposure.	• Disponibilité de Tenable Cloud

Centre de rapports

Le **Centre de rapports** de Tenable Identity Exposure fournit une fonctionnalité très utile qui vous permet d'exporter des données importantes dans des rapports destinés aux principaux acteurs au sein d'une organisation. Le Centre de rapports permet de créer des rapports à partir d'une liste prédéfinie pour garantir un processus efficace et rationnel.

Il offre les fonctions suivantes :

- **Filtrage granulaire** : affinez les rapports à l'aide de filtres granulaires basés sur la plage de dates, le domaine, l'indicateur d'attaque (IoA), l'indicateur d'exposition (IoE) et d'autres paramètres, qui vous garantiront des informations extrêmement détaillées.
- **Livraison automatisée** : planifiez des rapports de façon à automatiser leur création et leur livraison aux intervalles souhaités, et simplifiez ainsi les processus de surveillance de la sécurité et de reporting.
- **Exportation flexible** : exportez des rapports dans différents formats, dont CSV, pour procéder à une analyse plus approfondie, les partager à l'aide d'une clé d'accès aux rapports ou les intégrer à vos workflows de création de rapports.

Les administrateurs peuvent créer différents types de rapports pour un éventail d'utilisateurs, portant sur des périodes flexibles pouvant aller jusqu'à un trimestre. La possibilité de partager des données d'identité critiques à partir de Tenable Identity Exposure permet à l'organisation d'atténuer les risques de manière proactive et d'identifier les attaques potentielles basées sur l'identité.

Pour télécharger un rapport, les utilisateurs reçoivent un e-mail contenant une URL d'accès à une page dans laquelle ils saisissent une clé d'accès au rapport, qu'ils ont reçue de leur administrateur. Les rapports peuvent être téléchargés pendant 30 jours. Passé ce délai, ils expirent et Tenable Identity Exposure les supprime. Les utilisateurs doivent télécharger leurs rapports avant que Tenable Identity Exposure n'en génère un nouveau pour la période spécifiée, qui va remplacer le précédent.

Pour accéder au Centre de rapports :

1. Dans Tenable Identity Exposure, sélectionnez **Systèmes** > **Configuration**.
2. Sous **Rapports**, cliquez sur **Centre de rapports**.

   Un volet apparaît avec une liste des rapports configurés et leurs informations associées, telles que le nom du rapport, le type, le domaine, le profil, la période, la récurrence et les adresses e-mails des destinataires.

Prise en charge de Microsoft Entra ID

Outre Active Directory, Tenable Identity Exposure prend en charge Microsoft Entra ID (anciennement Azure AD ou AAD) pour étendre la portée des identités dans une organisation. Cette fonctionnalité utilise de nouveaux indicateurs d'exposition qui se concentrent sur les risques spécifiques à Microsoft Entra ID.

Pour intégrer Microsoft Entra ID à Tenable Identity Exposure, suivez scrupuleusement ce processus d'intégration :

1. Respecter les Conditions préalables
2. Vérifier les Autorisations
3. Configurer les paramètres Microsoft Entra ID
4. Activer la prise en charge de Microsoft Entra ID
5. Activer les scans de tenant

Conditions préalables

Vous avez besoin d'un compte Tenable Cloud pour vous connecter à « cloud.tenable.com » et utiliser la fonction de prise en charge de Microsoft Entra ID. Ce compte Tenable Cloud utilise la même adresse e-mail que celle de votre e-mail de bienvenue. Si vous ne connaissez pas l'adresse e-mail à utiliser pour « cloud.tenable.com », veuillez contacter le service d'assistance. Tous les clients disposant d'une licence valide (sur site ou SaaS) peuvent accéder à Tenable Cloud sur « cloud.tenable.com ». Ce compte vous permet de configurer des scans Tenable pour Microsoft Entra ID et de collecter les résultats de ces scans.

Remarque : vous n'avez pas besoin d'une licence **Tenable Vulnerability Management** valide pour accéder à Tenable Cloud. Une licence autonome Tenable Identity Exposure en cours de validité (sur site ou SaaS) est suffisante.

Remarque : Tenable Identity Exposure **ne prend pas en charge Microsoft Entra ID dans les clouds nationaux**, y compris les zones dédiées aux gouvernements chinois et américain. Microsoft Entra ID propose des clouds nationaux. Il s'agit d'instances d'Azure physiquement isolées, conçues pour des besoins spécifiques en matière de réglementation et de conformité. Tenable Identity Exposure ne prend en

charge que l'environnement Microsoft Entra ID global, à l'exception du cloud national chinois et du cloud national du gouvernement américain. Pour plus d'informations sur les clouds nationaux Microsoft Entra ID, voir Authentification de Microsoft Entra et clouds nationaux - Plateforme d'identités Microsoft.

Autorisations

La prise en charge de Microsoft Entra ID nécessite de collecter des données auprès de Microsoft Entra ID : utilisateurs, groupes, applications, principaux de service, rôles, autorisations, politiques, journaux, etc. Ces données sont collectées à l'aide de l'API Microsoft Graph et des identifiants des principaux de service conformément aux recommandations de Microsoft.

- Vous devez vous connecter à Microsoft Entra ID en tant qu'**utilisateur disposant des autorisations nécessaires pour accorder le consentement d'administrateur à l'échelle du tenant** sur Microsoft Graph, qui doit avoir le rôle administrateur global ou d'administrateur de rôle privilégié (ou tout autre rôle personnalisé avec les autorisations appropriées), selon Microsoft.
- Pour accéder à la configuration et à la visualisation des données pour Microsoft Entra ID, votre **rôle utilisateur Tenable Identity Exposure** doit disposer des autorisations appropriées. Pour plus d'informations, voir Définir les autorisations d'un rôle.

Nombre de licences

Tenable ne compte pas les identités dupliquées dans la licence **uniquement lorsque la fonction Synchronisation de Tenable Cloud est activée**. Sans cette fonctionnalité, Tenable ne peut pas rapprocher les comptes de Microsoft Entra ID et d'Active Directory. Tenable compte donc chacun d'eux séparément.

- **Sans la synchronisation de Tenable Cloud**, un utilisateur unique possédant à la fois un compte AD et un compte Entra ID compte comme deux utilisateurs distincts du point de vue de la licence.
- **Lorsque la synchronisation de Tenable Cloud est activée**, le système regroupe plusieurs comptes en une seule identité, ainsi un utilisateur ayant plusieurs comptes n'est compté qu'une seule fois.

Configurer les paramètres Microsoft Entra ID

Utilisez les procédures suivantes (adaptées de la documentation Microsoft Démarrage rapide : Inscrire une application avec la plateforme d'identités Microsoft) pour configurer tous les paramètres requis dans Microsoft Entra ID.

1. **Créer une application :**

   a. Dans le portail d'administration Azure, ouvrez la page **Inscriptions d'application**.

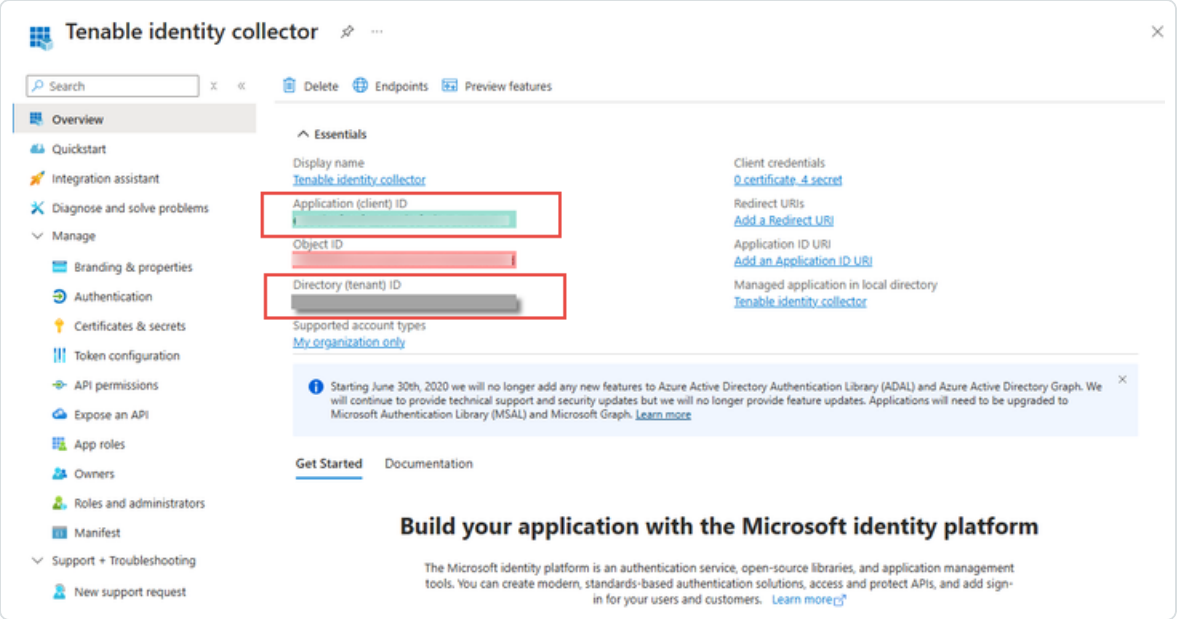
   b. Cliquez sur **Nouvelle inscription**.

   c. Donnez un nom à l'application (par exemple, « Tenable Identity Collector »). Pour les autres options, vous pouvez laisser les valeurs par défaut telles qu'elles.

   d. Cliquez sur **Inscrire**.

   e. Sur la page Présentation de cette application nouvellement créée, notez l'« ID de l'application (client) » et l'« ID de l'annuaire (tenant) », qui vous serviront plus tard au cours de l'étape Pour ajouter un nouveau tenant Microsoft Entra ID :.

   Attention : sélectionnez l'**ID de l'application** et **non** l'**ID d'objet** pour que la configuration fonctionne.



2. **Ajouter des informations d'identification à l'application :**

   a. Dans le portail d'administration Azure, ouvrez la page **Inscriptions d'application**.

   b. Cliquez sur l'application que vous avez créée.

   c. Dans le menu de gauche, cliquez sur **Certificats et secrets**.

   d. Cliquez sur **Nouveau secret de client**.

   e. Dans la zone **Description**, donnez un nom pratique à ce secret et une valeur d'**expiration** conforme à vos politiques. N'oubliez pas de renouveler ce secret quand sa date d'expiration approche.

   f. Enregistrez la valeur secrète dans un emplacement sécurisé, car Azure ne l'affiche qu'une seule fois et vous devez la recréer si vous la perdez.

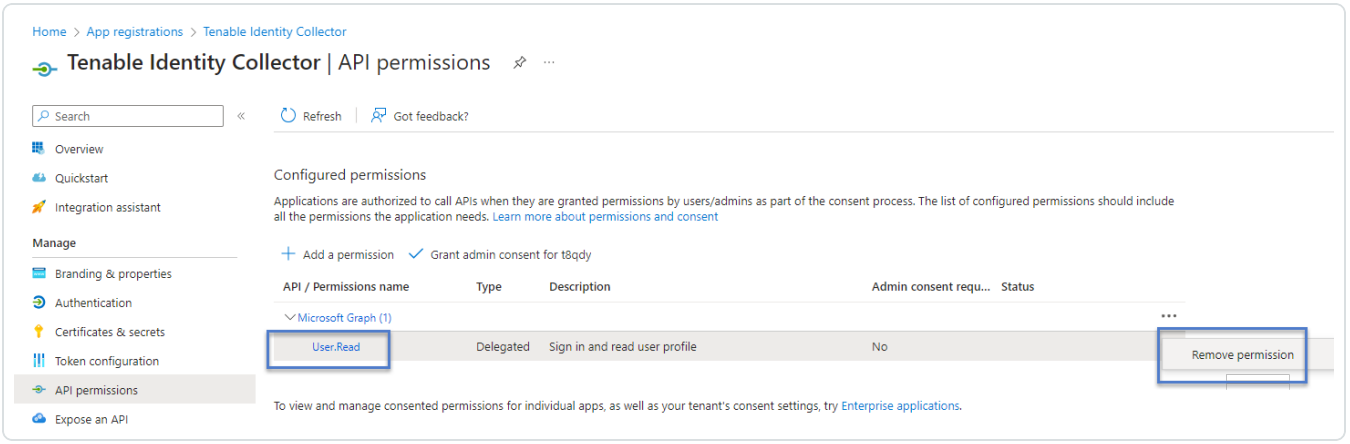
3. **Attribuer des autorisations à l'application :**

   a. Dans le portail d'administration Azure, ouvrez la page **Inscriptions d'application**.

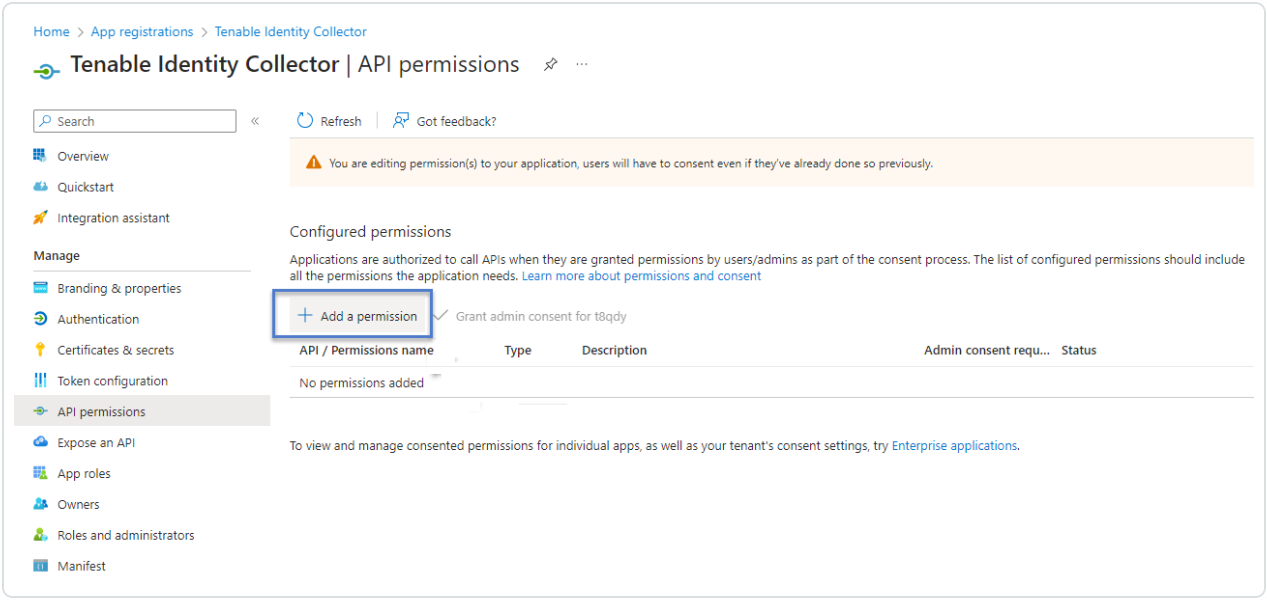
   b. Cliquez sur l'application que vous avez créée.

   c. Dans le menu de gauche, cliquez sur **Autorisations des API**

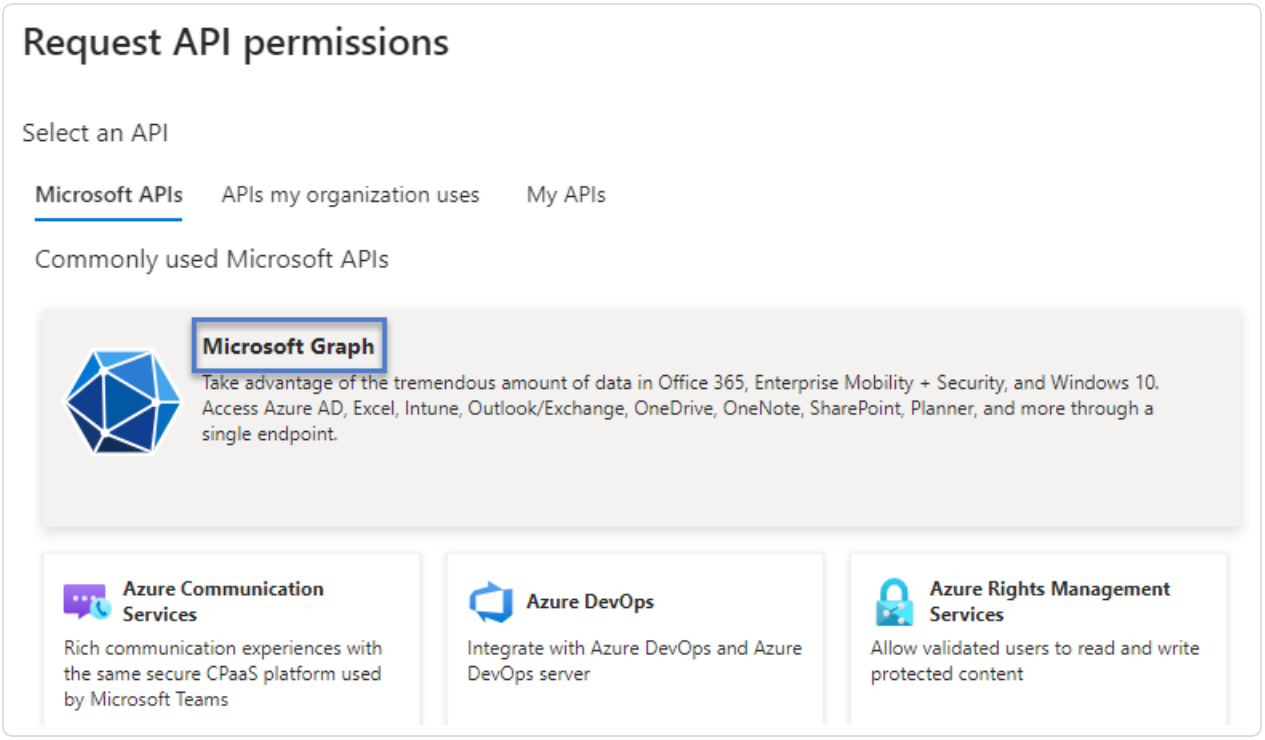
   d. Supprimer l'autorisation existante `User.Read` :



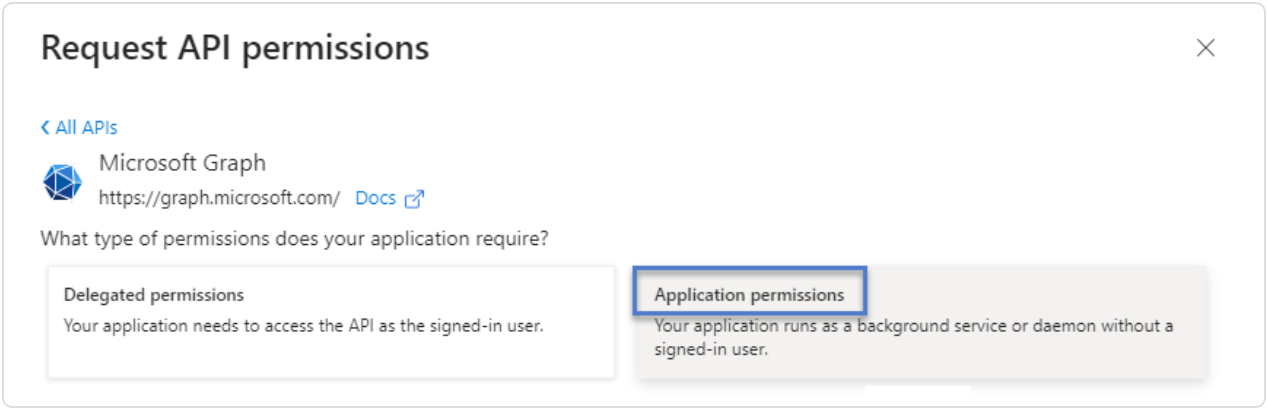
   e. Cliquez sur **Ajouter une autorisation** :



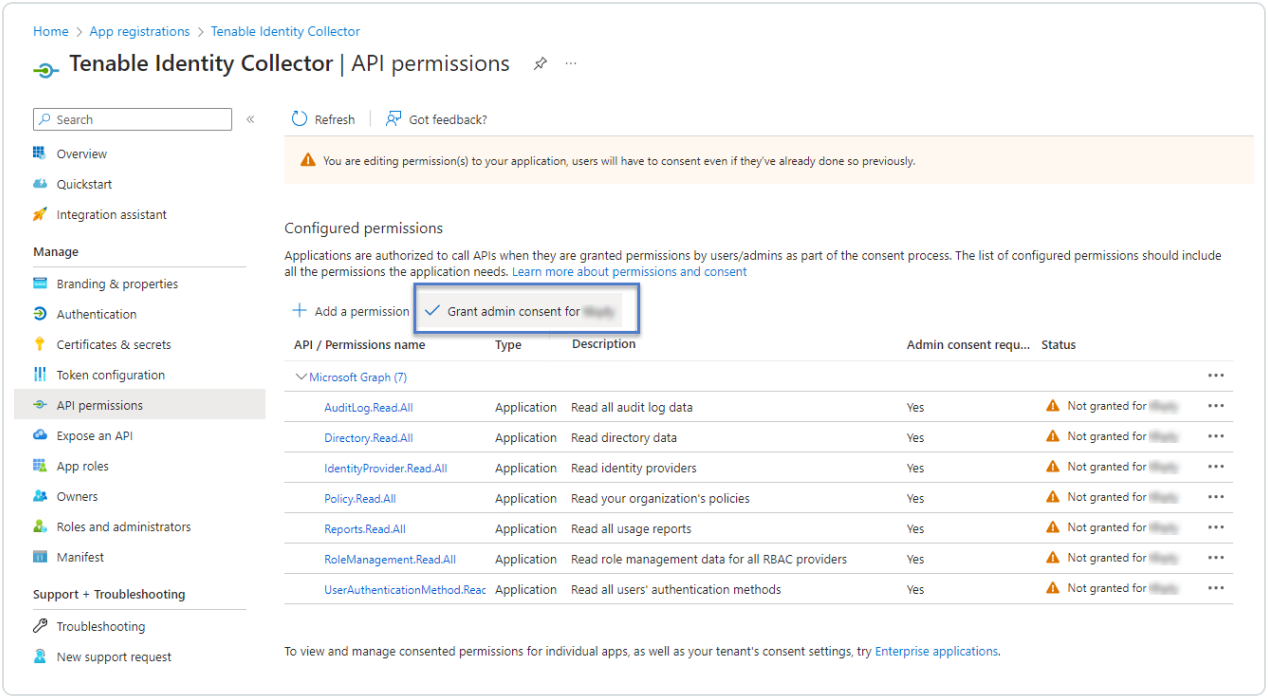
f. Sélectionnez **Microsoft Graph** :

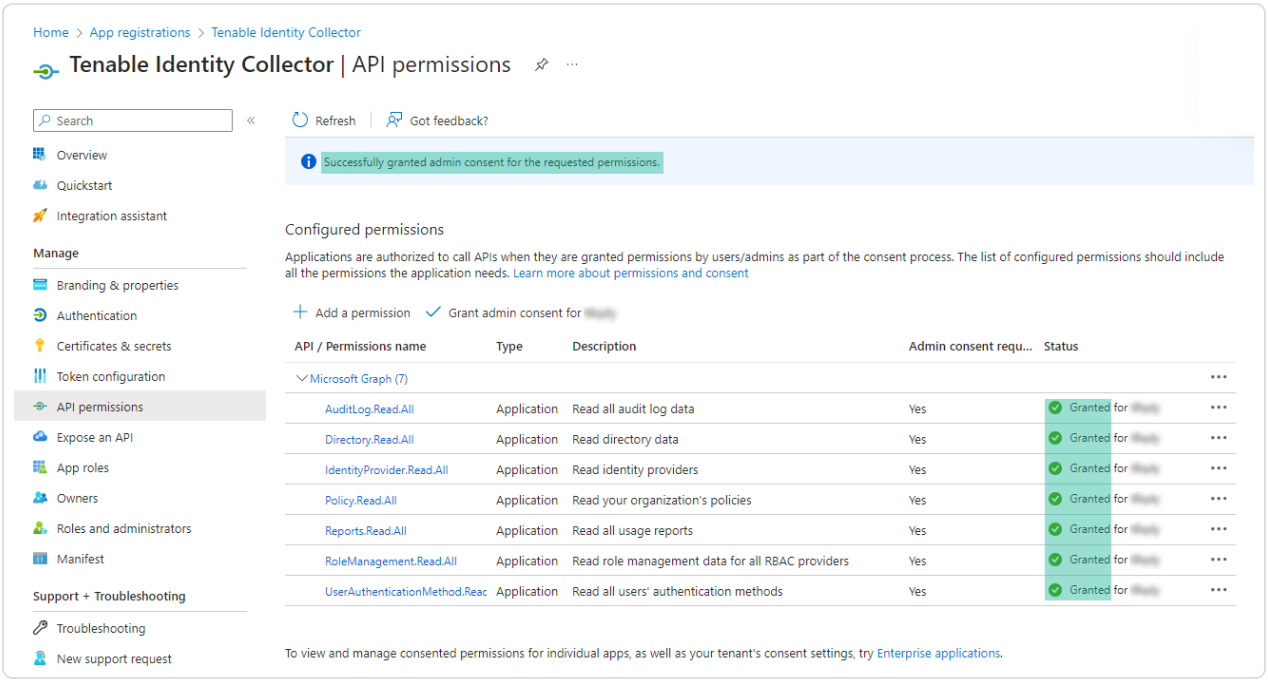


g. Sélectionnez **Autorisations de l'application** et non pas « Autorisations déléguées ».



h. Utilisez la liste ou la barre de recherche pour rechercher et sélectionner toutes les autorisations suivantes :
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `IdentityProvider.Read.All`
   - `Policy.Read.All`
   - `Reports.Read.All`
   - `RoleManagement.Read.All`
   - `UserAuthenticationMethod.Read.All`
i. Cliquez sur **Ajouter des autorisations**.
j. Cliquez sur **Accorder le consentement administrateur <nom du tenant>** et cliquez sur **Oui** pour confirmer :





4. Après avoir configuré tous les paramètres requis dans Microsoft Entra ID :

   a. Dans Tenable Vulnerability Management, créez un nouvel identifiant de type « Microsoft Azure ».

b. Sélectionnez la méthode d'authentification « Clé » et saisissez les valeurs que vous avez récupérées dans la procédure précédente : ID de tenant, ID d'application et Secret de client.

Activer la prise en charge de Microsoft Entra ID

- Pour utiliser **Microsoft Entra ID**, vous devez activer la fonctionnalité dans les paramètres Tenable Identity Exposure.
- Voir Activation de la prise en charge de « Identités 360 », « Centre d'exposition » et « Microsoft Entra ID » pour obtenir des instructions.

Activer les scans de tenant

Pour ajouter un nouveau tenant Microsoft Entra ID :

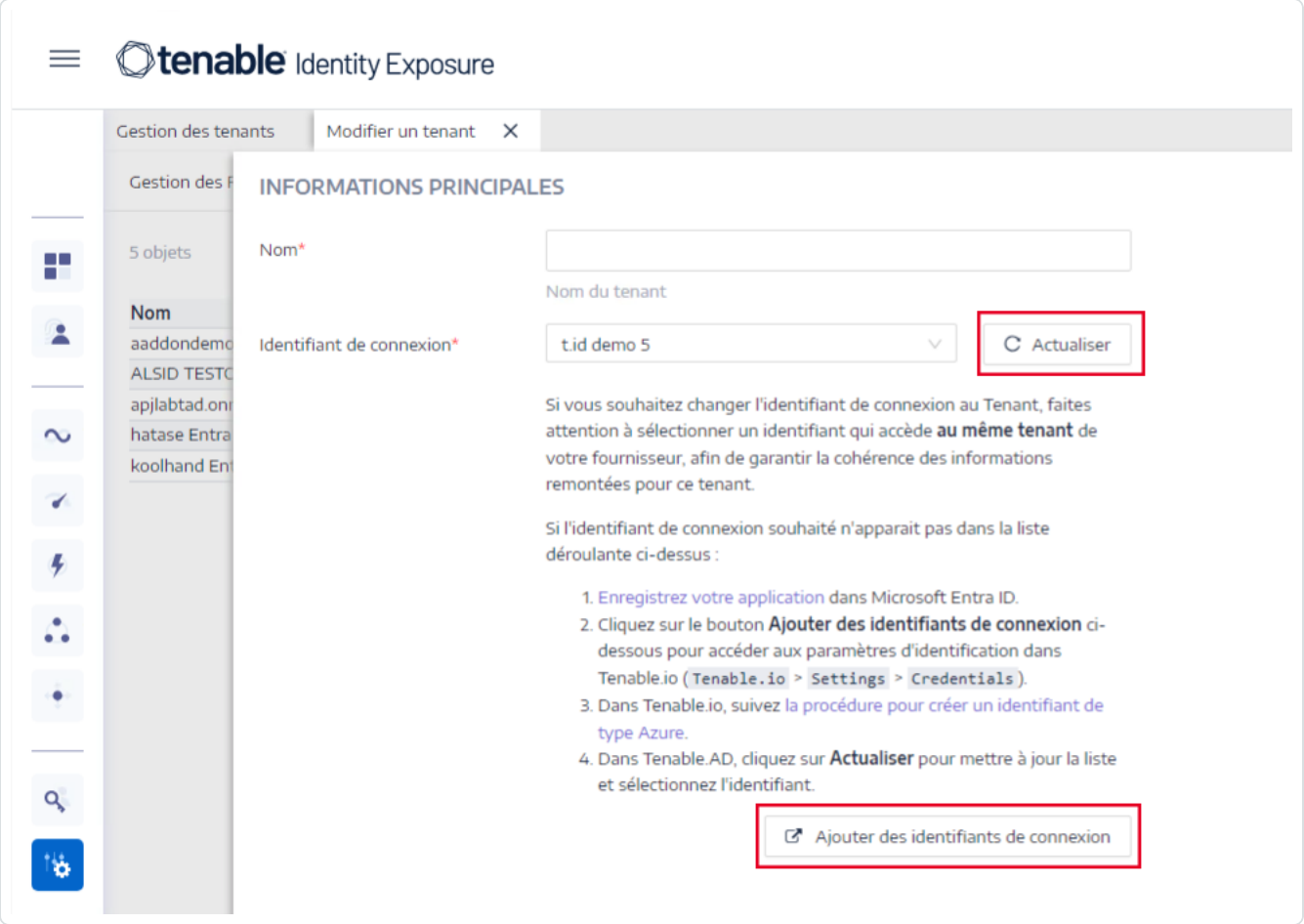
L'ajout d'un tenant lie Tenable Identity Exposure au tenant Microsoft Entra ID pour effectuer des scans sur le tenant.

1. Sur la page de configuration, cliquez sur l'onglet **Gestion des tenants**.

   La page **Gestion des tenants** apparaît.

2. Cliquez sur **Ajouter un tenant**.

   La page **Ajouter un tenant** apparaît.



3. Dans la zone **Nom du tenant**, saisissez un nom.
4. Dans la zone **Identifiants**, cliquez sur la liste déroulante pour sélectionner un identifiant.
5. Si votre identifiant ne figure pas dans la liste, vous pouvez effectuer l'une ou l'autre des opérations suivantes :
    - Créez un identifiant dans Tenable Vulnerability Management (Tenable Vulnerability Management > **Paramètres** > **Identifiants**). Pour plus d'informations, voir la procédure de création d'un identifiant de type Azure dans Tenable Vulnerability Management.
    - Vérifiez que vous disposez de l'autorisation « Peut utiliser » ou « Peut modifier » pour l'identifiant dans Tenable Vulnerability Management. Si vous ne disposez pas de ces

autorisations, Tenable Identity Exposure n'affiche pas l'identifiant dans la liste déroulante.

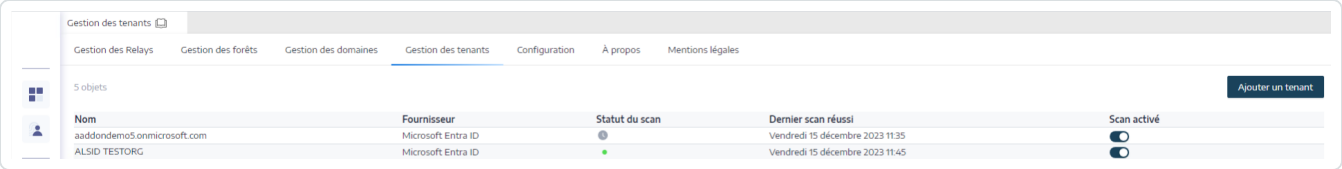
6. Cliquez sur **Actualiser** pour mettre à jour la liste déroulante des identifiants.
7. Sélectionnez l'identifiant que vous avez créé.
8. Cliquez sur **Ajouter**.

   Un message confirme que Tenable Identity Exposure a ajouté le tenant qui apparaît désormais dans la liste de la page Gestion des tenants.

Pour activer les scans pour le tenant :

Remarque : les scans de tenant ne sont pas exécutés en temps réel et il faut compter au moins 45 minutes avant que les données Microsoft Entra ID soient visibles dans l'Explorateur d'identités.

- Sélectionnez un tenant dans la liste et cliquez sur le curseur pour activer l'option **Scan activé**.



  Tenable Identity Exposure demande un scan sur le tenant ; les résultats apparaissent sur la page Indicateur d'exposition.

  Remarque : le délai minimum obligatoire entre deux scans est de **30 minutes**.

Actualiser les identifiants Entra ID

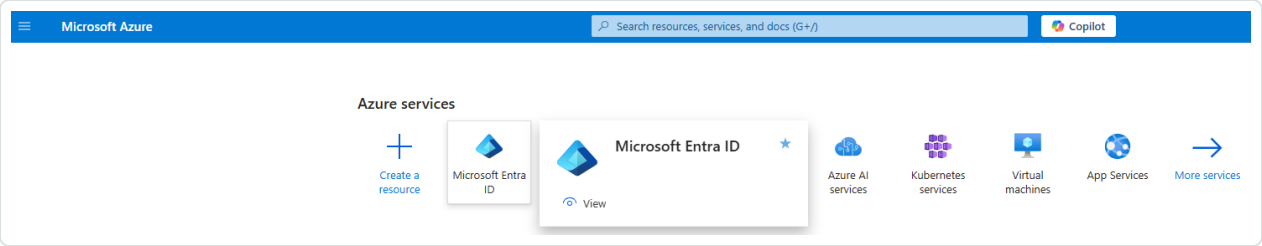
Dans Microsoft Entra ID (anciennement Azure Active Directory), l'expiration des identifiants varie en fonction du type d'identifiant et de la configuration de votre organisation.

Lorsque vos identifiants Entra ID expirent, Tenable Cloud arrête de synchroniser des assets et des vulnérabilités à partir d'Entra ID. Un message d'avertissement s'affiche, indiquant que le connecteur ne fonctionne plus.

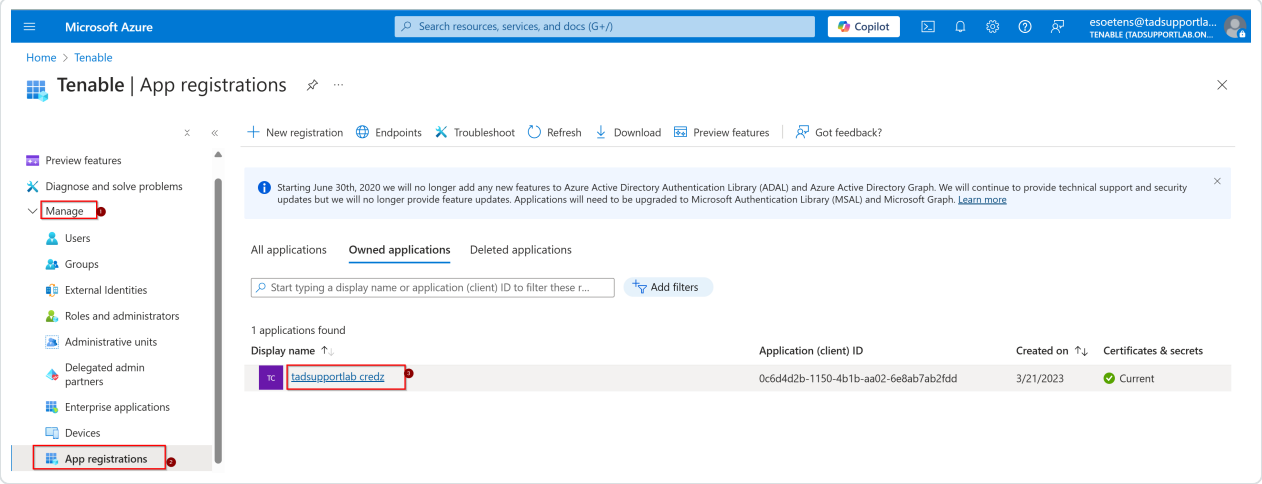
Pour actualiser vos identifiants et restaurer la synchronisation :

1. Accédez à **Microsoft Entra ID**:

   a. Connectez-vous à votre tenant Microsoft Entra ID.

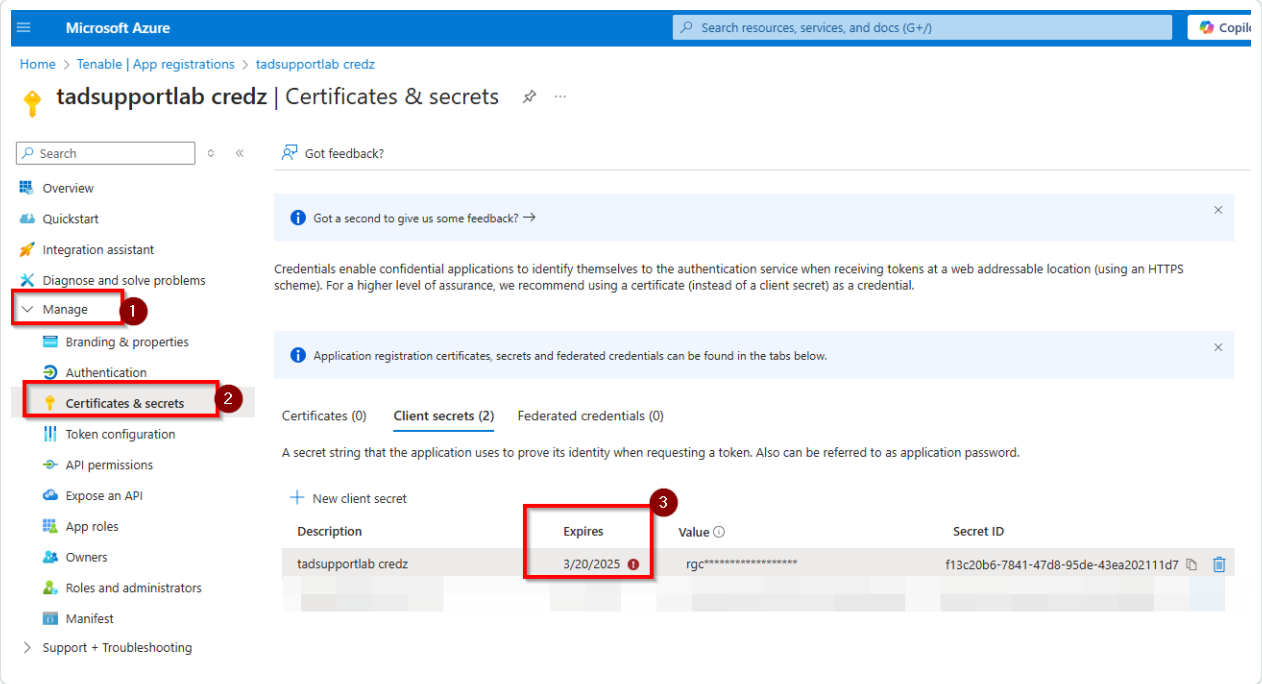


   b. Accédez à **Gérer → Inscriptions d'application.**



   c. Sélectionnez l'application que vous avez créée précédemment pour Tenable

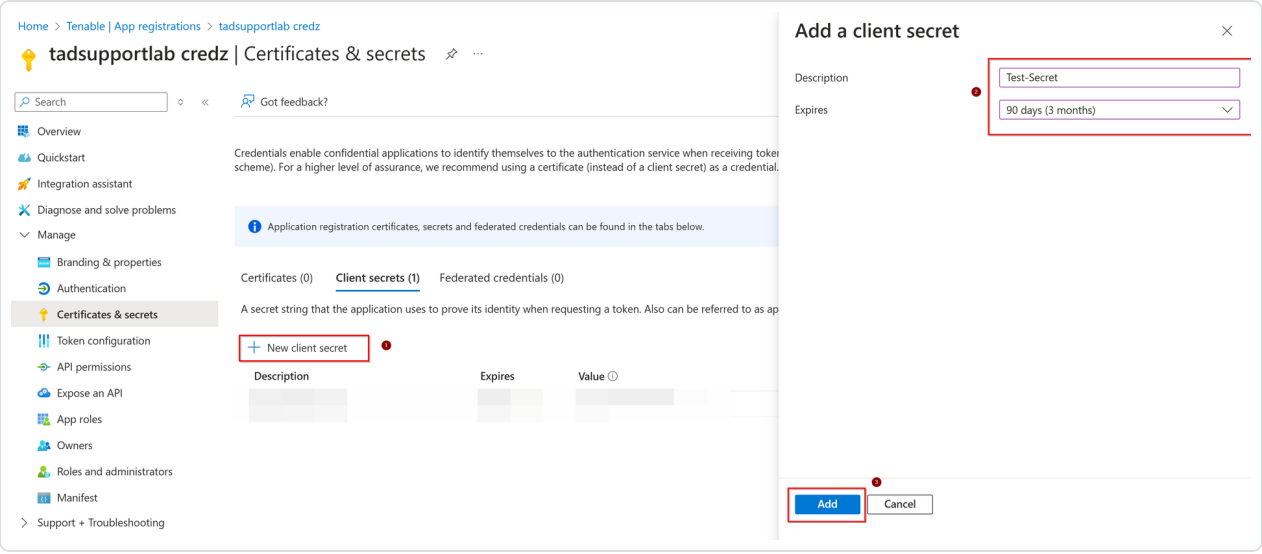
Identity Exposure.



2. Créez une nouvelle clé secrète client :

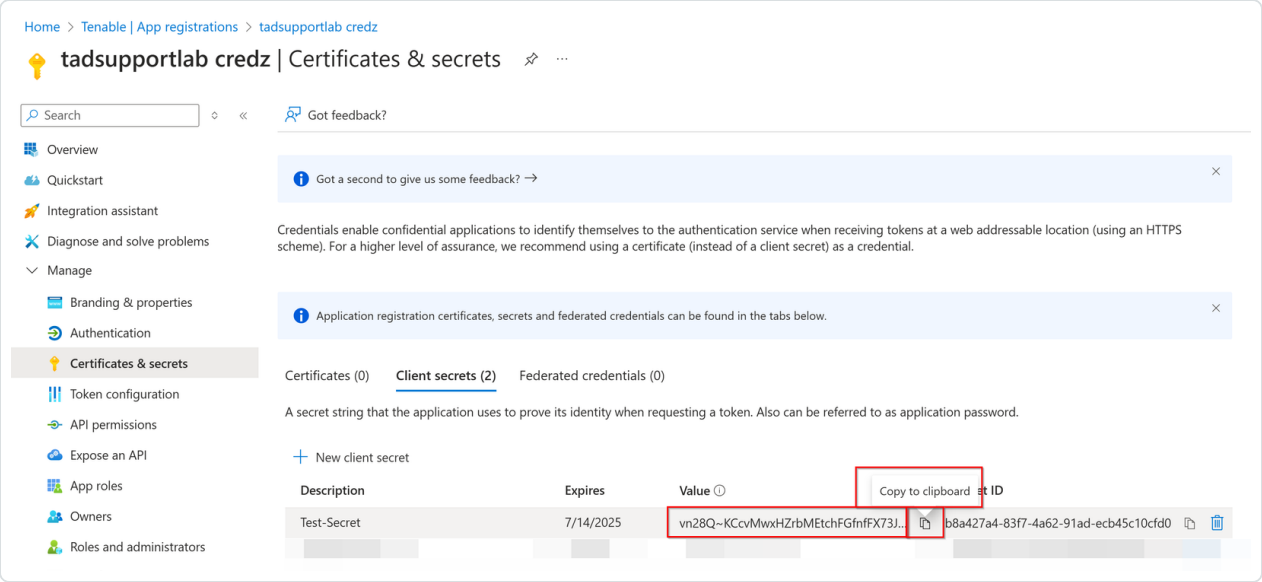
   a. Dans **Gérer**, cliquez sur **Certificats et clés secrètes**.

   b. Cliquez sur **Nouveau secret de client**.



c. Saisissez une description, définissez une période d'expiration (par exemple, 6 ou 12 mois) et cliquez sur **Ajouter**.

d. **Important** : copiez immédiatement la **valeur de la clé secrète client** (et non pas l'ID de la clé secrète) et stockez-la de façon sécurisée dans un gestionnaire de mots de passe sécurisé.



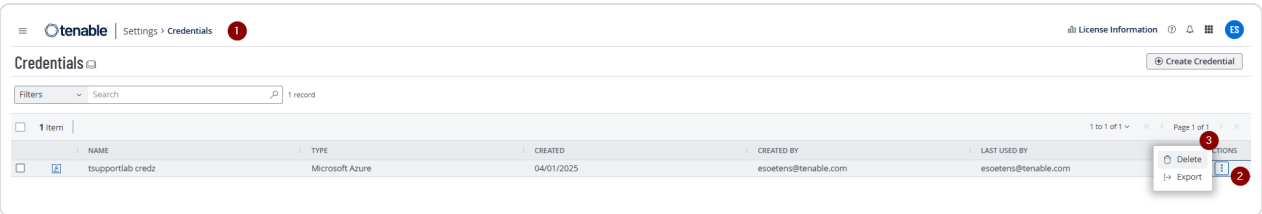
> **Remarque** : cette étape est cruciale, car la valeur de la clé secrète client n'est affichée **qu'une seule fois**, au moment de la création. L'erreur courante à éviter est de copier l'ID de la clé secrète (qui reste visible) au lieu de sa valeur réelle.

3. Mettez à jour les identifiants dans Tenable Cloud :

   a. Connectez-vous à **Tenable Cloud**.

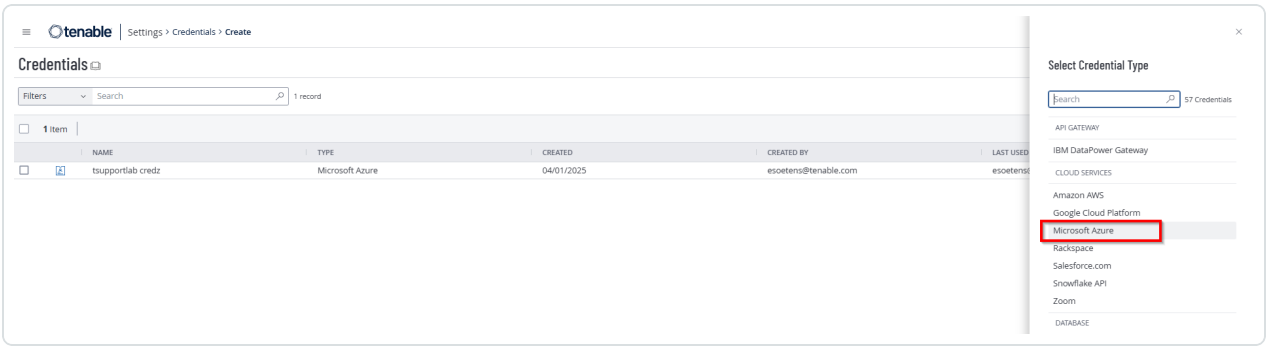
   b. Accédez à **Settings** (Paramètres) → **Credentials** (Informations d'authentification).

   c. Localisez les identifiants expirés et supprimez-les.



d. Cliquez sur **Create credentials** (Créer des informations d'authentification) (en haut à droite).

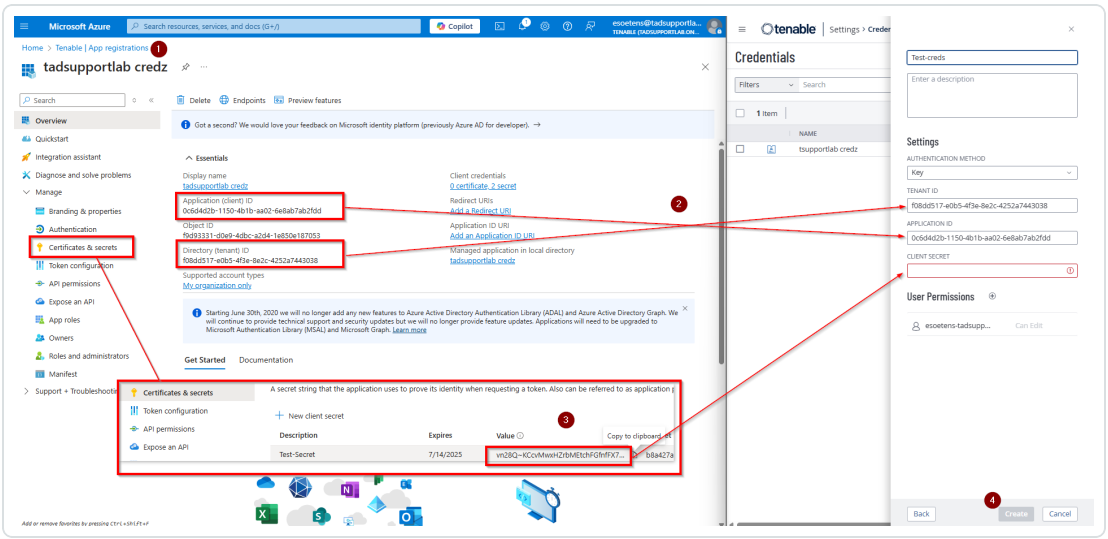
e. Sélectionnez le type **Microsoft Azure**.



f. Saisissez les éléments suivants :

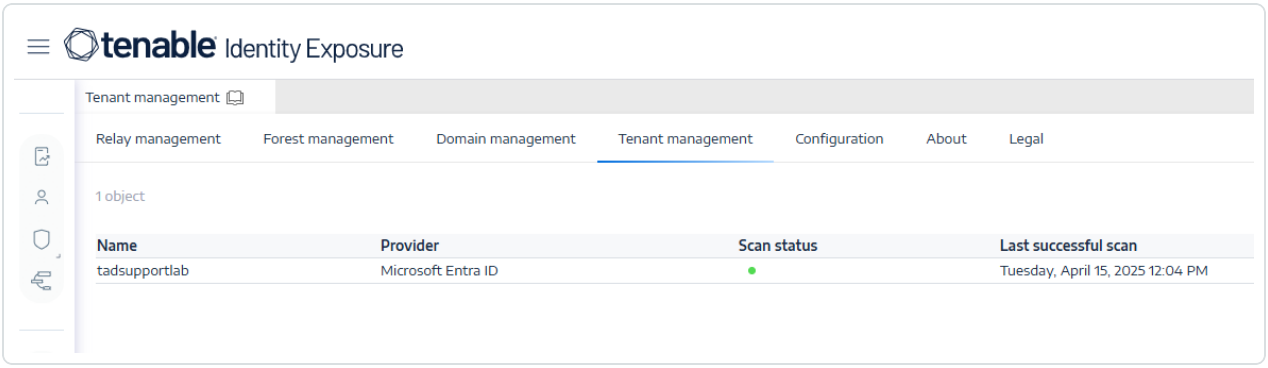
- **App ID** (ID d'application) et **Tenant ID** (ID de tenant) provenant de l'inscription de l'application Entra ID.
- **Client Secret** (clé secrète client que vous avez copiée précédemment).

g. Cliquez sur **Create** (Créer).



4. Confirmez le statut :

    - Après avoir enregistré les nouveaux identifiants, vérifiez le statut de votre scan.



        - Un statut vert indique que le scan a réussi.
        - Si le statut est orange, vérifiez que vous n'avez pas confondu la valeur de la clé secrète avec son ID. Si nécessaire, répétez la procédure à partir de l'étape 2.

Collecte de données via Tenable Cloud

Tenable Cloud, la fonctionnalité de collecte de données de Tenable Identity Exposure, transfère vos informations vers son cloud privé pour fournir des analyses et des services de sécurité. Pour plus d'informations sur la collecte de données, voir la déclaration Confiance et garantie de Tenable.

Pour utiliser Tenable Cloud :

1. Dans Tenable Identity Exposure, cliquez sur **Système** dans la barre de navigation latérale, puis cliquez sur **Système**.

    Le volet **Configuration** apparaît.

2. Sélectionnez l'onglet **Configurations**.
3. Sous **Services de l'application**, cliquez sur **Tenable Cloud**.

    Le volet **Tenable Cloud** apparaît.

4. Cliquez sur le curseur « Utiliser le service Tenable Cloud » pour le passer sur **activé**.

    Un message confirme que Tenable Identity Exposure a mis à jour la configuration de transfert

d'informations.



Analyse privilégiée

L'analyse privilégiée est une fonctionnalité facultative de Tenable Identity Exposure qui nécessite davantage de privilèges (contrairement à ses autres fonctionnalités) pour récupérer des données protégées et fournir une analyse de sécurité plus approfondie.

Conditions préalables

Pour utiliser la fonctionnalité « Analyse privilégiée », vous devez ouvrir les ports RPC dynamiques **TCP/49152-65535** et **UDP/49152-65535**. Pour plus d'informations, voir Network Flow Matrix.

Récupération de données

> Remarque : la fonctionnalité Analyse privilégiée nécessite des privilèges élevés. Voir Accès pour l'analyse privilégiée.

Lorsque l'analyse privilégiée est activée, elle récupère les données supplémentaires suivantes :

- **Empreintes de mot de passe** – Tenable Identity Exposure récupère les empreintes LM et NT pour l'analyse des mots de passe. Tenable Identity Exposure récupère les empreintes LM uniquement pour signaler leur présence parce qu'elles utilisent un algorithme ancien et faible, mais ne les stocke pas. La collecte des empreintes couvre :
    - Tous les comptes utilisateur activés
    - Tous les comptes d'ordinateur de contrôleur de domaine activés

Protection des données

Active Directory (AD) lui-même ne stocke pas directement les mots de passe des utilisateurs. Il ne stocke que leurs empreintes en utilisant les algorithmes de hachage LM ou NT qui ne permettent pas de récupérer le mot de passe d'origine. Tenable Identity Exposure ne stocke pas les empreintes LM.

À l'exception des clients hébergeant leur Relay dans une plateforme SaaS-VPN, les empreintes de mot de passe ne quittent jamais l'infrastructure du client, car seul le Relay les gère. Le Relay ne stocke pas les mots de passe ni les empreintes de mot de passe, mais récupère l'empreinte du mot de passe de l'utilisateur chaque fois qu'elle est nécessaire à des fins d'analyse ; il ne la conserve dans son cache que temporairement, généralement pendant quelques millisecondes.

Cependant, Tenable Identity Exposure maintient un nombre minimal de bits de données d'empreinte de mot de passe, stockés en toute sécurité dans la RAM du Relay, uniquement pour effectuer une analyse du k-anonymat afin de vérifier si des utilisateurs ont des mots de passe identiques.

> **Remarque** : pour les clients de la plateforme SaaS-VPN, le comportement est le même, mais c'est Tenable qui héberge votre Relay.

Journaux d'activité

Les journaux d'activité de Tenable Identity Exposure permettent de visualiser les traces de toutes les activités qui se sont produites sur la plateforme Tenable Identity Exposure, liées à des adresses IP, des utilisateurs ou des actions spécifiques.

Pour configurer les journaux d'activités :

1. Sous **Gestion** dans le volet de navigation latéral de Tenable Identity Exposure, cliquez sur **Système**.

   Le volet **Configuration** apparaît.

2. Sous la section **Services de l'application**, cliquez sur **Journaux d'activité**.

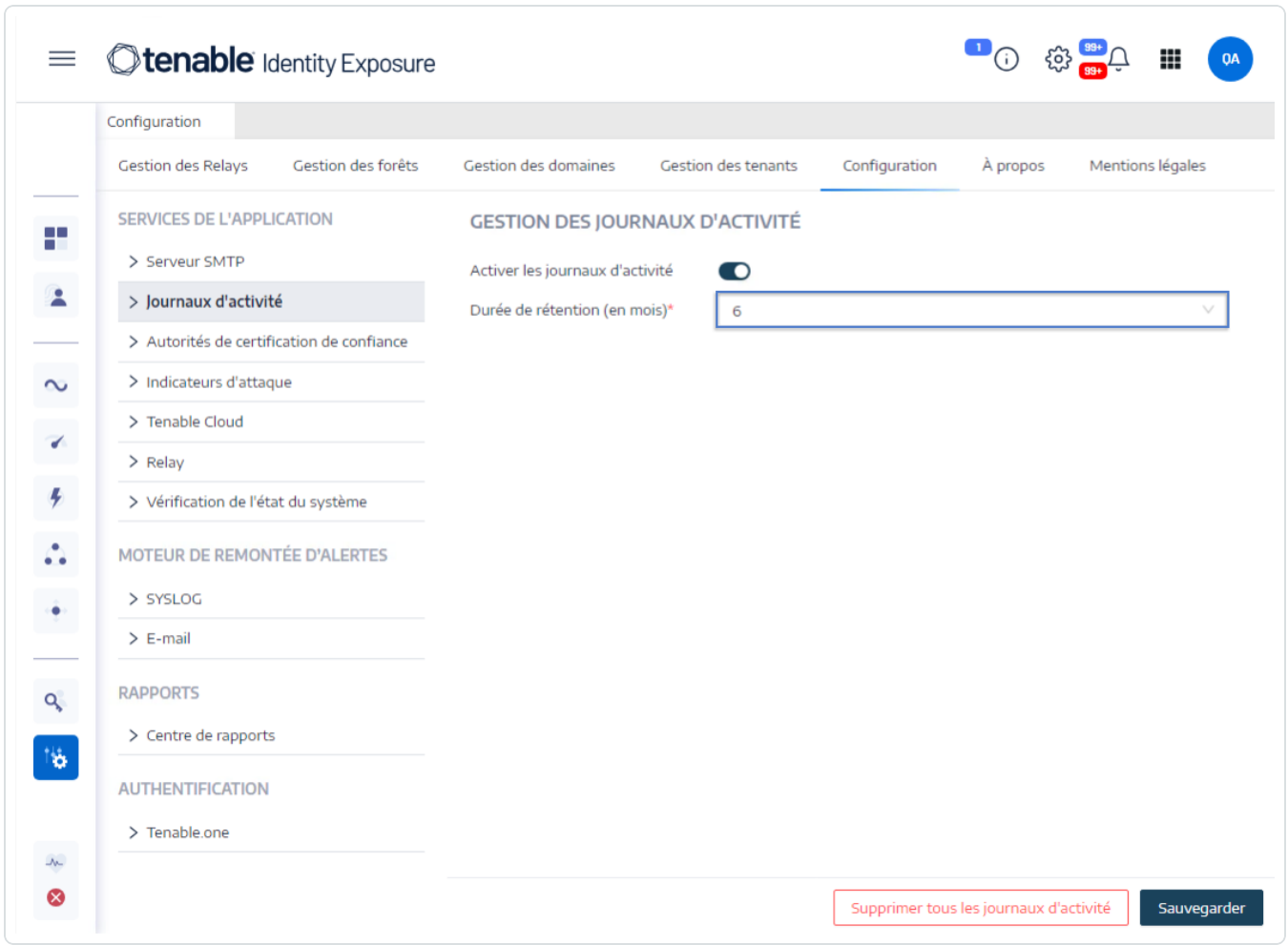
   Le volet **Gestion des journaux d'activité** apparaît.

3. Pour activer la fonctionnalité Journaux d'activité, cliquez sur le curseur **activé**.

4. Dans la zone Durée de rétention (en mois), cliquez sur **>** pour sélectionner le nombre de mois de consignation des activités.

5. Cliquez sur **Enregistrer**.

   Un message confirme que Tenable Identity Exposure a mis à jour les paramètres.



Pour effacer les données des journaux d'activité :

1. Sous **Gestion** dans le volet de navigation latéral de Tenable Identity Exposure, cliquez sur **Système**.

   Le volet **Configuration** apparaît.

2. Sous la section **Services de l'application**, cliquez sur **Journaux d'activité**.

   Le volet **Gestion des journaux d'activité** apparaît.

3. Sous **Supprimer toutes les données des journaux d'activité**, cliquez sur **Effacer**.

   Un message demande de confirmer l'opération.

4. Cliquez sur **Confirmer**.

   Un message confirme que Tenable Identity Exposure a mis à jour les paramètres.

Pour définir des autorisations pour les journaux d'activité d'un utilisateur :

1. Sous **Gestion** dans le volet de navigation latéral Tenable Identity Exposure, cliquez sur **Comptes**.

   Le volet **Gestion des comptes utilisateur** apparaît.

2. Cliquez sur l'onglet **Gestion des rôles**.

3. Dans la liste des rôles, survolez celui qui nécessite cette autorisation et cliquez sur l'icône en fin de ligne.

   Le volet **Modifier un rôle** apparaît.

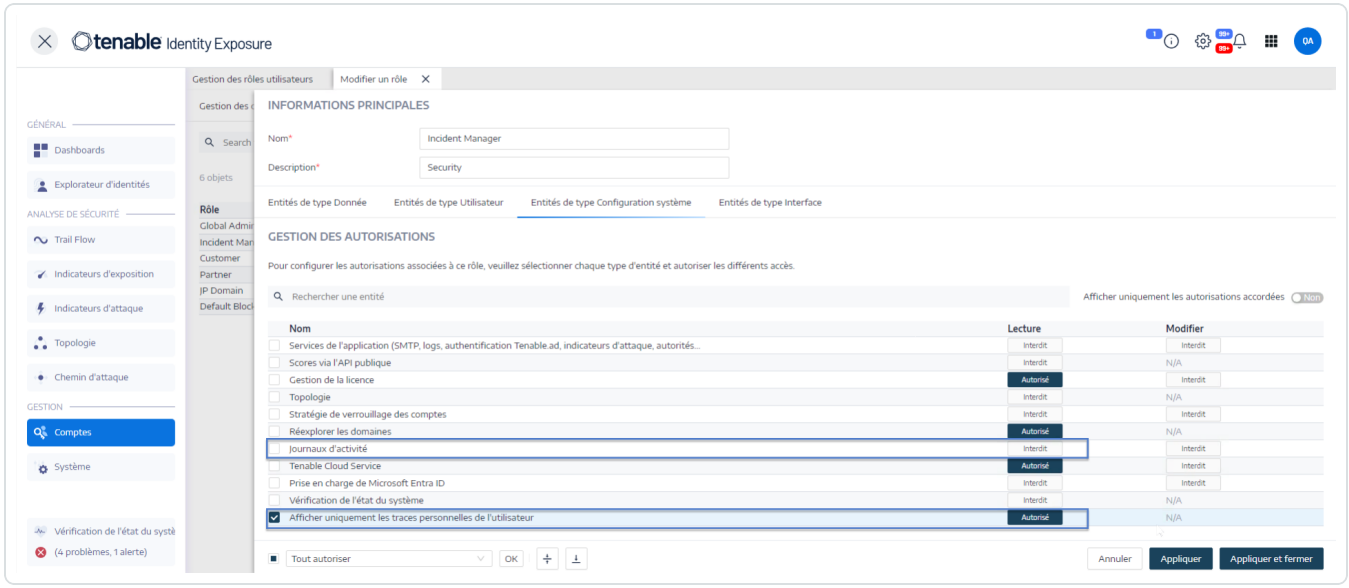
4. Sous la section **Informations principales**, sélectionnez l'onglet **Entités de type Configuration système**.

5. Sous la section **Gestion des autorisations**, procédez comme suit :

   - Désactivez l'autorisation **Journaux d'activité** pour qu'elle passe à l'état *Interdit*.
   - Activez l'autorisation **Afficher uniquement les traces personnelles de l'utilisateur** pour qu'elle passe à l'état *Autorisé*.

6. Cliquez sur **Appliquer et fermer**.

   Un message confirme que Tenable Identity Exposure a mis à jour le rôle utilisateur.



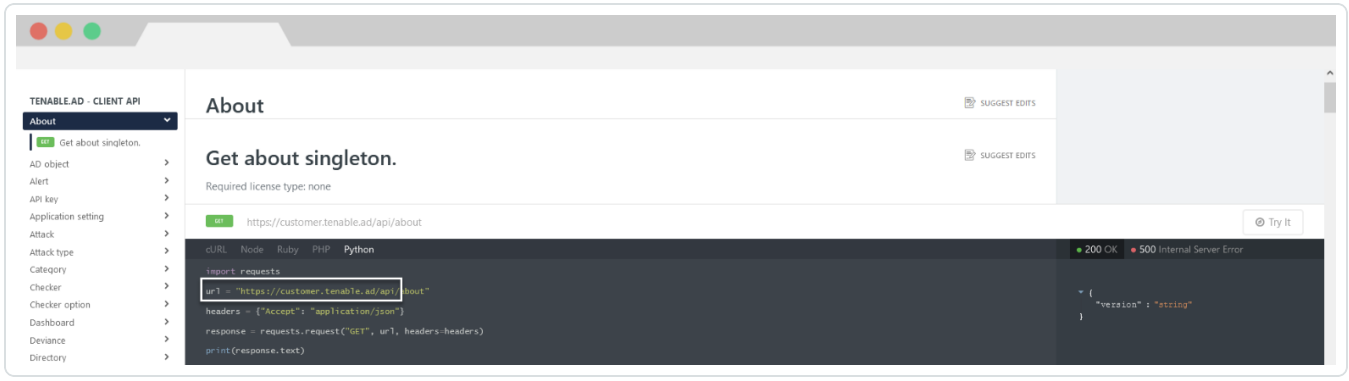
API publique Tenable Identity Exposure

L'API de Tenable Identity Exposure permet de communiquer avec ses services de base de données.

Le fichier OpenAPI contenant la structure et les ressources de l'API de Tenable Identity Exposure est disponible ici.

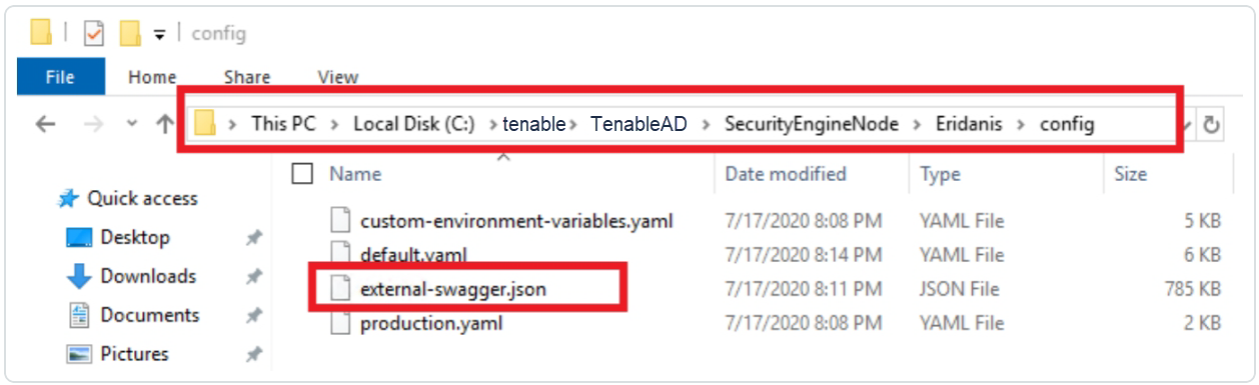
Pour accéder à l'API de votre instance Tenable Identity Exposure :

- Dans votre navigateur, ouvrez cette URL :



Pour télécharger le fichier OpenAPI :

- Pour les installations sur site, suivez ce chemin vers le SN (Security Engine Node) :



- Pour les installations SaaS, accédez à l'Explorateur d'API Tenable Identity Exposure.

Pour récupérer une clé API :

1. Dans Tenable Identity Exposure, cliquez sur l'icône de votre profil utilisateur et sélectionnez **Préférences**.

   Le volet Préférences apparaît.

2. Dans le menu, sélectionnez **Clé API**.

   Tenable Identity Exposure affiche votre clé API actuelle.

3. Cliquez sur pour copier la clé API vers le presse-papiers.

Pour actualiser une clé API :

Les jetons d'accès expirent si vous cliquez sur **Actualiser la clé API** ou que vous perdez le droit de générer une clé API ou un jeton d'accès. L'expiration n'est pas liée au temps ni au nombre de demandes API. La génération ou l'actualisation d'une clé API est spécifique à l'utilisateur actuel et n'interfère pas avec les clés API d'autres comptes. Lorsque vous obtenez une clé API, vous recevez également un jeton d'actualisation. Vous pouvez utiliser ce jeton d'actualisation pour récupérer une nouvelle clé API.

Attention : lorsque vous actualisez votre clé API, Tenable Identity Exposure désactive la clé API actuelle. Vous recevez également un jeton d'actualisation.

1. Cliquez sur **Actualiser la clé API**.

   Un message vous demande confirmation.

2. Cliquez sur **Confirmer**.

Gestion des données

Tenable Identity Exposure conserve les données de Microsoft Entra ID et d'Active Directory jusqu'à 15 mois.

Capacité	Période de rétention
Chemin d'attaque	6 mois
Topologie	
Trail Flow	
Dashboards et rapports	12 mois
Centre d'exposition	Jusqu'à 15 mois
Identités 360	
Indicateurs d'exposition (Entra ID)	
Indicateurs d'exposition (Active Directory)	• Problèmes actifs : conservés indéfiniment • Problèmes traités : conservés pendant six mois
Indicateurs d'attaque (Active Directory)	

Pour plus d'informations, voir Données de la plateforme Tenable Cloud.

Régions de déploiement

Tenable Identity Exposure SaaS est actuellement déployé dans les régions Azure suivantes :

Pays	Région Azure
Amériques	
Brésil – Sao Paulo	Sud du Brésil
Canada – Québec (ville)	Est du Canada
Canada – Toronto	Centre du Canada
États-Unis – Californie	Ouest des États-Unis
États-Unis – Iowa	Centre des États-Unis
États-Unis – Virginie	Est des États-Unis 2
Europe, Moyen-Orient, Afrique	
France – Paris	Centre de la France
Irlande	Europe du Nord
Pays-Bas	Europe de l'Ouest
Afrique du Sud – Johannesburg	Nord de l'Afrique du Sud
Suisse – Zürich	Nord de la Suisse
Émirats arabes unis – Dubaï	Nord des EAU
Royaume-Uni – Londres	Sud du Royaume-Uni
Asie-Pacifique	
Australie – Nouvelle-Galles du Sud	Est de l'Australie
Australie – Victoria	Sud-est de l'Australie
Hong Kong	Asie de l'Est
Inde – Pune	Centre de l'Inde

Japon – Osaka	Ouest du Japon
Singapour	Asie du Sud-Est

Licences Tenable Identity Exposure

Cette rubrique décompose le processus de gestion des licences pour Tenable Identity Exposure en tant que produit autonome. Elle explique également comment les assets sont comptabilisés et décrit ce qui se passe en cas de dépassement ou d'expiration de licence.

Licences Tenable Identity Exposure

Il existe deux versions de Tenable Identity Exposure : une version cloud et une version sur site. Tenable propose également une tarification par abonnement dans certains cas.

Pour utiliser Tenable Identity Exposure, vous achetez des licences en fonction de vos besoins organisationnels et des spécificités de votre environnement. Tenable Identity Exposure attribue ensuite ces licences à vos *assets*, à savoir les utilisateurs activés dans vos services d'annuaire.

Lorsque votre environnement s'agrandit, le nombre de vos assets augmente lui aussi ; vous allez donc acheter davantage de licences pour tenir compte de cette évolution. Les licences Tenable sont soumises à des tarifs dégressifs. Autrement dit, plus vous en achetez, plus le prix unitaire est bas. Pour connaître les prix, contactez votre représentant Tenable.

Conseil : pour afficher le nombre actuel de vos licences et les assets disponibles, cliquez sur , puis sur **Informations de licence** dans la barre de navigation supérieure de Tenable. Pour en savoir plus, voir la page Informations de licence.

Remarque : Tenable propose une tarification simplifiée aux fournisseurs de services de sécurité gérés (MSSP). Pour en savoir plus, contactez votre représentant Tenable.

Méthode de comptage des assets

Chaque licence Tenable Identity Exposure que vous achetez vous permet de scanner une identité unique ou la représentation numérique d'un utilisateur. Tenable ne compte pas deux fois les identités. Par exemple, les comptes utilisateur activés pour la même identité à la fois dans Microsoft Active Directory et Microsoft Entra ID comptent pour une seule licence Tenable.

Utilisez ce script PowerShell pour tracer les comptes utilisateur activés dans AD :

```
(Get-ADuser -Filter 'enabled -eq $true').count
```

Utilisez ce script PowerShell pour tracer les comptes utilisateur activés dans Entra ID :

```
(Get-MgUser -All -Filter "accountEnabled eq true" -Property onPremisesSyncEnabled | where {
$_.onPremisesSyncEnabled -ne $true }).Count
```

Composants Tenable Identity Exposure

Les deux versions de Tenable Identity Exposure sont livrées avec les composants suivants :

- Trail Flow
- Topologie
- Indicateurs d'exposition
- Indicateurs d'attaque
- Chemins d'attaque
- Centre d'exposition
- Prise en charge de Microsoft Entra ID

Récupération de licences

Lorsque vous achetez des licences, le nombre total de vos licences reste le même pendant toute la durée de votre contrat, sauf si vous achetez des licences supplémentaires. Cependant, Tenable Identity Exposure récupère des licences en temps réel lorsque vous supprimez des utilisateurs activés du service d'annuaire de votre environnement.

Dépassement de la limite d'utilisation d'une licence

Pour amortir les pics d'utilisation dus aux renouvellements du matériel, à une croissance rapide de l'environnement ou à des menaces imprévues, les licences Tenable sont flexibles. Vous pouvez temporairement dépasser votre nombre d'identités sous licence. Cependant, lorsque vous scannez plus d'identités que ne le permet votre licence, Tenable communique clairement le dépassement et réduit ensuite les fonctionnalités en trois étapes.

Remarque : dans les environnements sur site utilisant Tenable Identity Exposure 3.77 ou une version ultérieure, l'application de la licence est immédiate.

Scénario	Résultat
Vous avez plus d'identités activées que de licences pendant trois jours consécutifs.	Un message apparaît dans Tenable Identity Exposure.
Vous avez plus d'identités activées que de licences pendant plus de 15 jours.	Un message et un avertissement concernant une réduction des fonctionnalités apparaissent dans Tenable Identity Exposure.
Vous avez plus d'identités activées que de licences depuis plus de 30 jours.	Un message apparaît dans Tenable Identity Exposure et vous ne pouvez pas utiliser la fonction Indicateur d'exposition dans l'interface utilisateur ou l'API.

Licences expirées

Les licences Tenable Identity Exposure que vous achetez sont valables pendant toute la durée de votre contrat. Trente jours avant l'expiration de votre licence, un avertissement apparaît dans l'interface utilisateur. Pendant cette période de renouvellement, échangez avec votre représentant Tenable pour ajouter ou supprimer des produits ou bien pour modifier le nombre de vos licences.

Une fois votre licence expirée, vous ne pouvez plus vous connecter à la plateforme Tenable.

Gérer votre licence

Tenable Identity Exposure nécessite un fichier de licence provenant de Tenable ou de partenaires d'entreprise autorisés. Le nombre d'utilisateurs de la licence couvre tous les utilisateurs et comptes de service activés.

Vous devez charger le fichier de licence pour configurer et utiliser Tenable Identity Exposure.

Conseil : le fichier de licence se trouve sur le portail Tenable Community sous « Mes produits » (vous devez être administrateur dans Tenable Community pour afficher le fichier de licence.)

Attention : si vous n'appliquez pas de licence valide à votre plateforme SaaS, Tenable la met hors service après un certain délai.

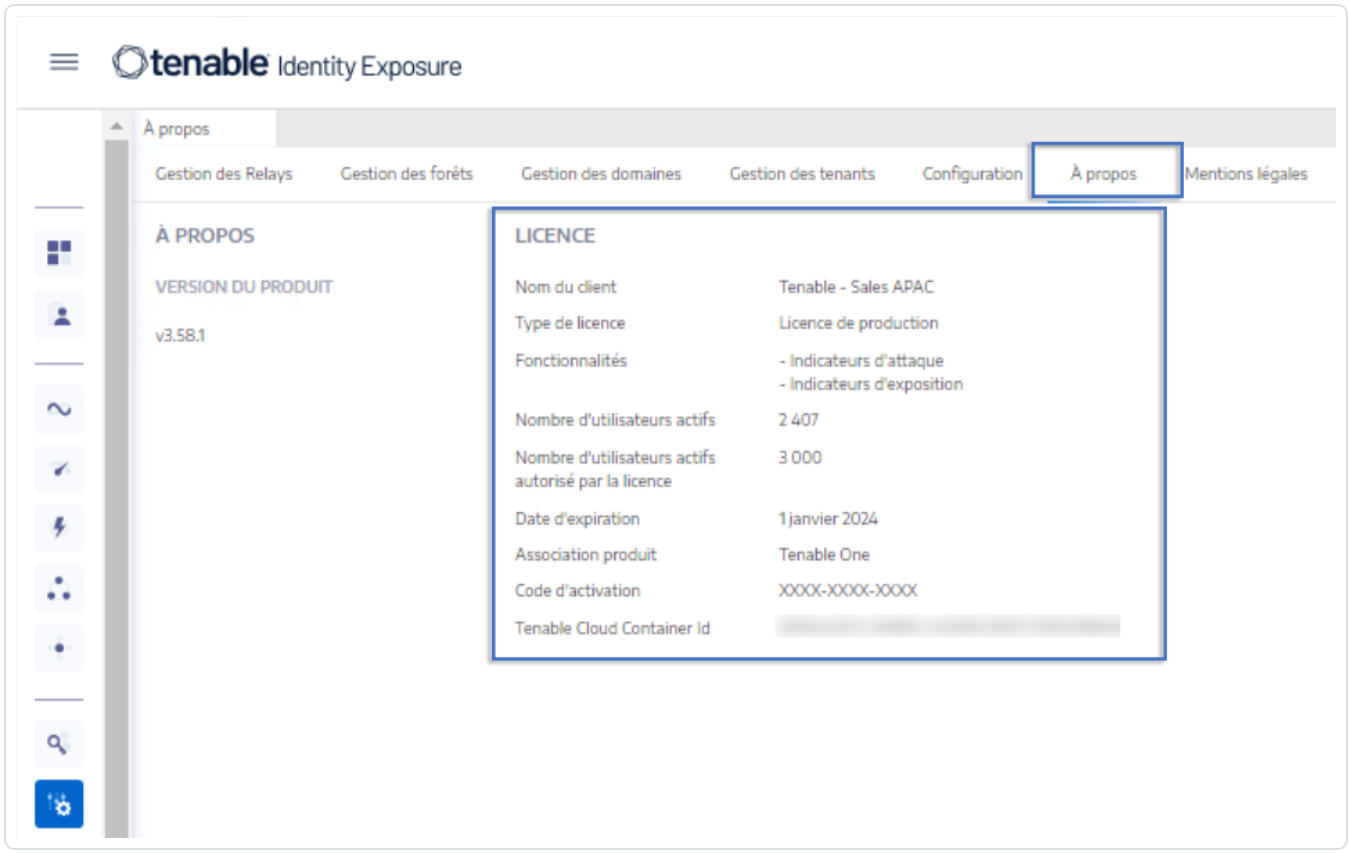
Les licences Tenable Identity Exposure peuvent inclure :

- Indicateurs d'attaque
- Indicateurs d'exposition
- Les deux

Pour afficher votre licence :

- Dans Tenable Identity Exposure, cliquez sur l'icône **Systèmes** > onglet **À propos de**.

  La licence apparaît.



Consommation de licence

Pour les installations sur site, Tenable Identity Exposure effectue un suivi de l'utilisation de la licence si une connexion Internet est disponible.

Prévention des incohérences de l'UUID de conteneur

Dans Tenable Identity Exposure, chaque licence inclut un UUID de conteneur unique, liant l'application à un conteneur Tenable Cloud spécifique. Cet UUID de conteneur doit rester cohérent pour assurer une intégration transparente et éviter tout problème opérationnel.

Afin d'éviter toute incohérence de l'UUID de conteneur (par exemple lors du chargement d'une nouvelle licence après un renouvellement), Tenable Identity Exposure peut détecter les « déviations » par rapport à l'UUID de conteneur.

Si vous essayez d'importer une licence avec un UUID de conteneur différent, le message « Impossible de modifier le conteneur Tenable Cloud » apparaît. Vous pouvez être dans l'un des scénarios suivants :

- Passage d'une licence Tenable Identity Exposure autonome vers une licence Tenable One.
- Migration de votre conteneur d'un site Tenable AWS vers un autre.
- Expiration de l'ancien conteneur et création d'un nouveau.

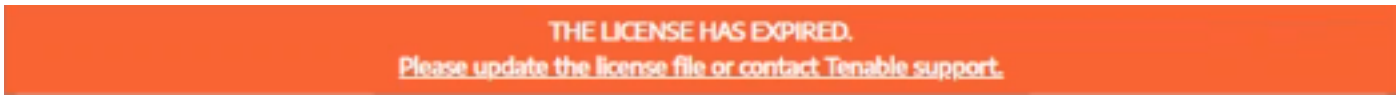
Si vous vous trouvez dans l'une de ces situations, veuillez contacter Tenable pour discuter de la modification de votre conteneur Tenable Cloud pour cette plateforme Tenable Identity Exposure.

Validité de la licence

La licence Tenable Identity Exposure reste valide tant que vous répondez aux critères suivants :

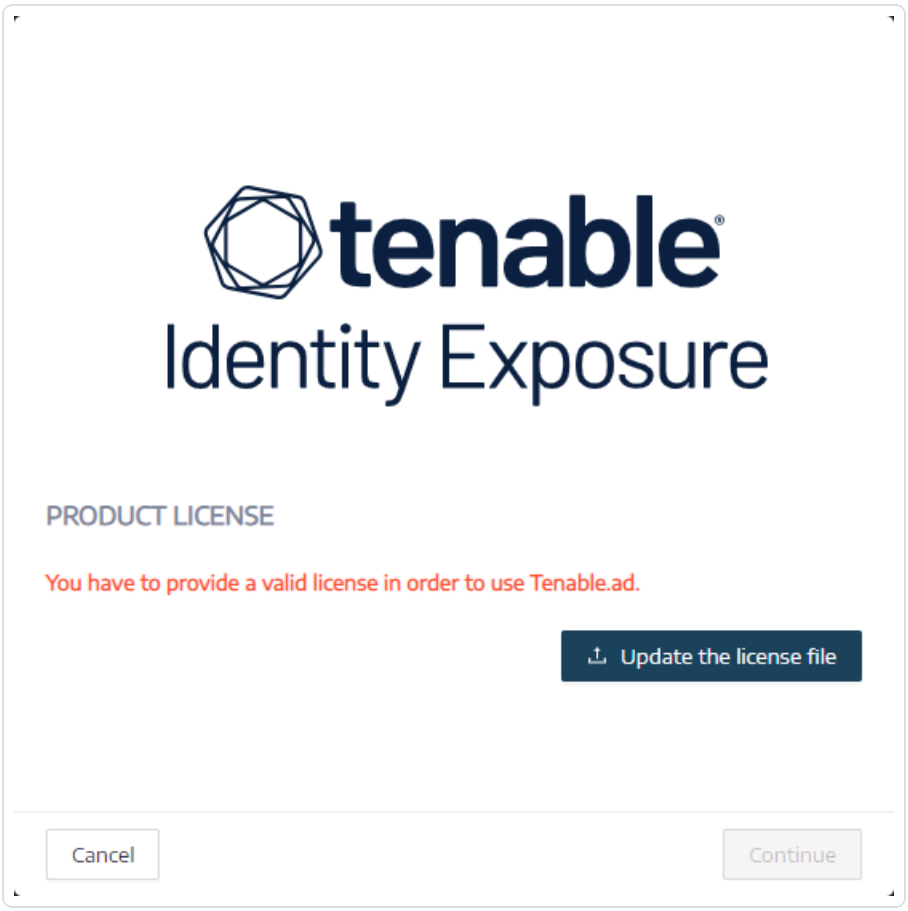
- Le nombre d'utilisateurs actifs ne dépasse pas le nombre accordé dans la licence. Tenable Identity Exposure affiche trois types de messages d'avertissement selon votre cas.
    - Le nombre d'utilisateurs actifs **est proche de la limite** des conditions de licence : vous devez mettre à jour votre licence.
    - Le nombre d'utilisateurs actifs **dépasse** les conditions de licence : vous devez mettre à jour votre licence.
    - Le nombre d'utilisateurs actifs **dépasse les conditions de licence (de 10 %)** : vous n'avez plus accès à la page Indicateur d'exposition et devez mettre à jour votre licence.
- La date d'expiration n'est pas passée.

Si vous ne respectez aucun des critères ci-dessus, Tenable Identity Exposure affiche un avertissement pour vous inviter à mettre à jour votre licence :



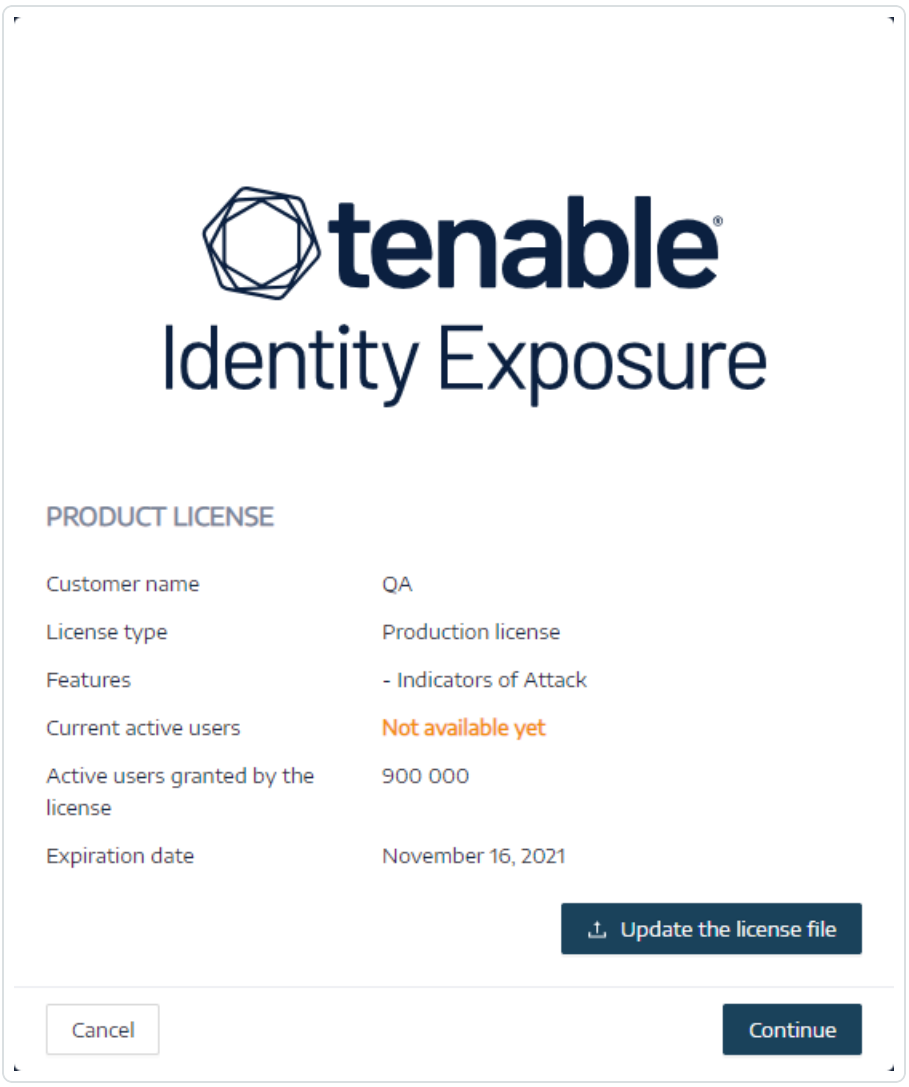
Pour charger un fichier de licence :

1. Dans la fenêtre de connexion, cliquez sur **Mettre à jour le fichier de licence**.



2. Accédez à l'emplacement de votre fichier de licence et cliquez sur **Ouvrir**.

   L'exemple suivant montre un fichier de licence appliqué correctement :



3. Cliquez sur **Continuer** pour ouvrir Tenable Identity Exposure.

Pour mettre à jour un fichier de licence :

1. Dans Tenable Identity Exposure, cliquez sur l'icône **Système** > onglet **À propos de**.
2. Cliquez sur **Mettre à jour le fichier de licence**.
3. Accédez à l'emplacement de votre fichier de licence et cliquez sur **Ouvrir**.

   Tenable Identity Exposure met à jour votre fichier de licence. Dans le cas d'un fichier de licence non valide, contactez le service client.

Versions LTS (Long-Term Support) et normales : avantages et différences clés

Que sont les versions LTS ?

Les versions LTS (Long-Term Support) sont des versions logicielles que nous maintenons pendant une période prolongée : 18 mois. Pendant cette période, nous fournissons des mises à jour régulières, telles que des correctifs de sécurité et des correctifs critiques, sans introduire de nouvelles fonctionnalités qui pourraient perturber les fonctionnalités existantes.

Les versions LTS sont conçues pour les clients qui privilégient la stabilité, la fiabilité et la maintenance à long terme aux dernières fonctionnalités. Ces versions sont idéales pour les environnements où les mises à jour ou les changements fréquents pourraient entraîner des temps d'arrêt ou des coûts de test et de déploiement supplémentaires.

Que sont les versions normales ?

Les versions normales sont nos versions logicielles standard qui incluent de nouvelles fonctionnalités, des améliorations et des mises à jour. Ces versions sont plus dynamiques et mises à jour fréquemment (tous les 6 mois), mais bénéficient d'une prise en charge pendant une période plus courte que les versions LTS.

Les versions normales sont idéales pour les clients qui souhaitent rester à la pointe de la technologie et adopter régulièrement de nouvelles fonctionnalités et mises à jour, même si cela nécessite des mises à niveau plus fréquentes.

Différences clés entre les versions LTS et normales :

- **Durée du support** : les versions LTS bénéficient d'un support pendant 18 mois, tandis que pour les versions normales, le support n'est assuré que pendant 6 mois.
- **Stabilité ou innovation** – Les versions LTS se concentrent sur la stabilité et la sécurité et ne reçoivent que des modifications minimales des fonctionnalités, tandis que les versions normales mettent l'accent sur l'innovation en introduisant de nouvelles fonctionnalités plus fréquemment.
- **Fréquence de mise à niveau** – Les clients qui utilisent des versions LTS procèdent à des mises à niveau moins souvent, tandis que ceux qui utilisent des versions normales devront peut-être effectuer des mises à niveau plus fréquemment pour rester à jour.

Pourquoi choisir les versions LTS ?

Les versions LTS sont parfaites pour les systèmes et les environnements critiques où les temps d'arrêt sont coûteux. Elles offrent la tranquillité d'esprit d'une version stable et prise en charge à long terme.

Pourquoi choisir les versions normales ?

S'il est important pour vous de disposer des dernières fonctionnalités et améliorations, les versions normales vous conviendront mieux. Bien qu'elles puissent nécessiter des mises à jour plus fréquentes, elles permettent d'accéder aux fonctionnalités les plus récentes.

Résolution des problèmes touchant Tenable Identity Exposure

Les rubriques suivantes vous aident à résoudre les problèmes éventuels d'installation de Tenable Identity Exposure (anciennement Tenable.ad) :

- Interférence du durcissement SYSVOL avec Tenable Identity Exposure
- Utilitaire système (handle.exe)

Interférence du durcissement SYSVOL avec Tenable Identity Exposure

SYSVOL est un dossier partagé situé sur chaque contrôleur de domaine (DC) dans un domaine Active Directory. Il contient les dossiers et les fichiers des stratégies de groupe (GPO). Le contenu de SYSVOL se réplique sur tous les DC et est accessible via des chemins UNC (Universal Naming Convention) tels que `\\<exemple.com>\SYSVOL` ou `\\<DC_IP_or_FQDN>\SYSVOL`.

Le durcissement SYSVOL désigne l'utilisation du paramètre « Chemins d'accès UNC renforcés », également dénommé « chemins UNC renforcés », « Durcissement de chemin UNC », « Chemins renforcés », etc. Cette fonctionnalité répond à la vulnérabilité MS15-011 (KB 3000483) dans la stratégie de groupe. De nombreuses normes de cyber-sécurité, les critères CIS par exemple, imposent de mettre en œuvre cette fonctionnalité.

Lorsque vous appliquez ce paramètre de durcissement aux clients SMB (Server Message Block), il augmente la sécurité des machines jointes au domaine pour veiller à ce que le contenu de GPO obtenu de SYSVOL n'a pas été falsifié par un attaquant sur le réseau. Cependant, dans certains cas, ce paramètre peut également interférer avec le fonctionnement de Tenable Identity Exposure.

Suivez les conseils de cette section de dépannage si vous constatez que des chemins UNC renforcés perturbent la connectivité entre Tenable Identity Exposure et le partage SYSVOL.

Environnements affectés

Les options de déploiement Tenable Identity Exposure suivantes peuvent rencontrer ce problème :

- Sur site
- SaaS avec Secure Relay

L'option de déploiement suivante n'est pas affectée :

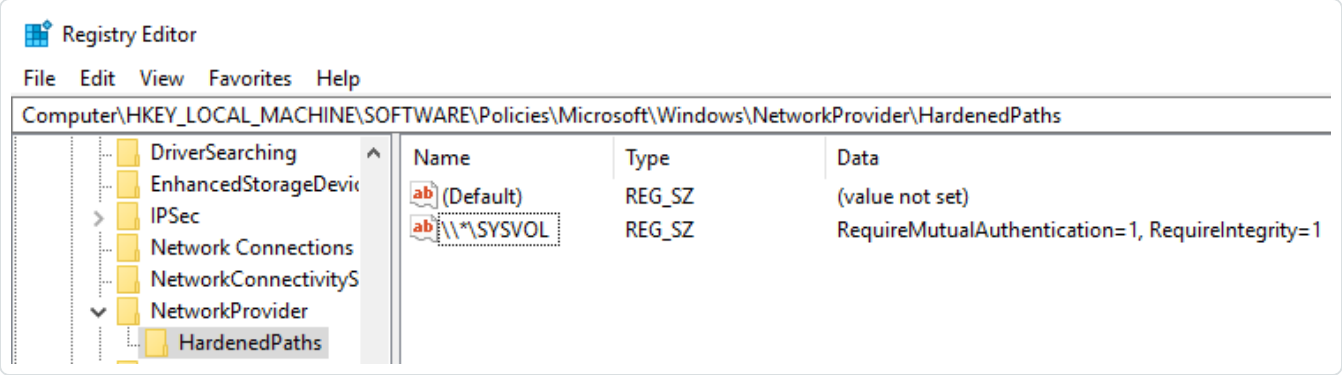
- SaaS avec VPN

Le durcissement SYSVOL étant un paramètre côté client, il fonctionne sur les machines qui se connectent au partage SYSVOL et non pas aux contrôleurs de domaine.

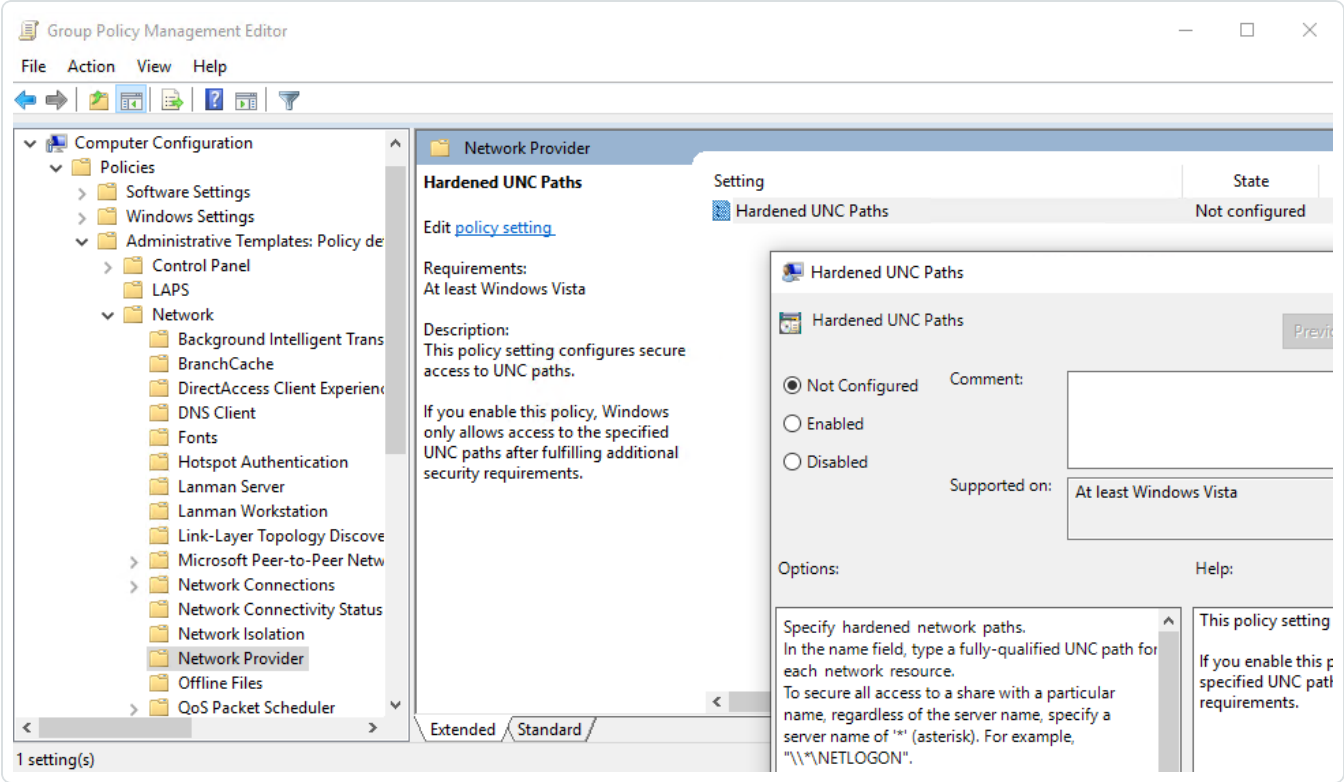
Windows active ce paramètre par défaut et il peut interférer avec Tenable Identity Exposure.

Certaines organisations souhaitent également activer ce paramètre et l'appliquer en utilisant le paramètre GPO associé ou en définissant directement la clé de registre correspondante.

- Les clés de registre liées aux chemins renforcés UNC se trouvent dans « `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths` » :



- Le paramètre GPO correspondant se trouve dans « `Configuration ordinateur\Modèles d'administration\Réseau\Fournisseur réseau\Chemins d'accès UNC renforcés` » :



L'application du durcissement SYSVOL se produit lorsque les paramètres « `RequireMutualAuthentication` » et « `RequireIntegrity` » d'un chemin UNC faisant référence à SYSVOL, par exemple « `\\*\SYSVOL` », ont la valeur « `1` ».

Signes de problèmes de durcissement SYSVOL

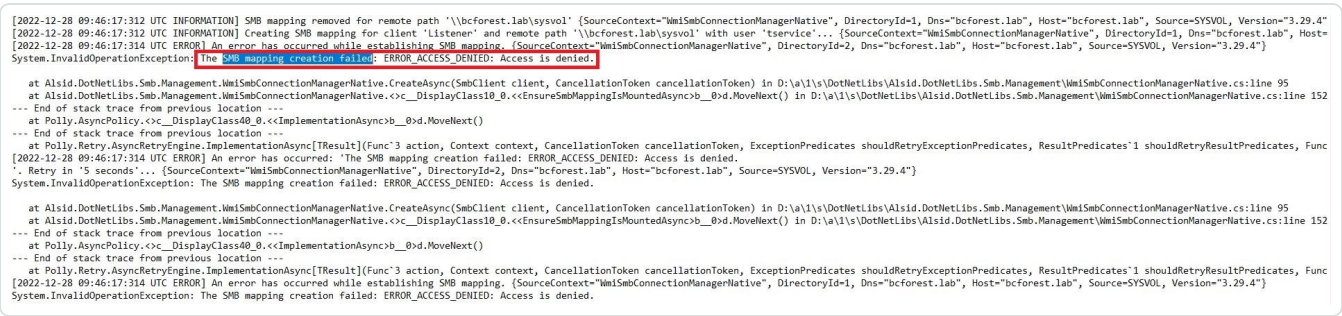
Lorsque vous suspectez que le durcissement SYSVOL interfère avec Tenable Identity Exposure, vérifiez les éléments suivants :

1. Dans Tenable Identity Exposure, accédez à **Système** > **Gestion des domaines** pour afficher le statut d'initialisation LDAP et SYSVOL de chaque domaine.

   Un domaine ayant une connectivité normale affiche un indicateur vert, tandis qu'un domaine ayant des problèmes de connectivité peut afficher un indicateur d'exploration indéfiniment.



2. Sur le Directory Listener ou la machine Relay, ouvrez le dossier des journaux : `<Dossier d'installation>\DirectoryListener\logs`.
3. Ouvrez le fichier journal Ceti et recherchez la chaîne « SMB mapping creation failed » (Échec de la création du mappage SMB) ou « Access is denied » (accès refusé). Les journaux d'erreurs contenant cette phrase indiquent que le durcissement UNC est probablement en place sur le Directory Listener ou la machine Relay.



Options de remédiation

Il existe deux options de remédiation possibles : Passage à l'authentification Kerberos ou Désactivation du durcissement SYSVOL.

Passage à l'authentification Kerberos

Il s'agit de l'option privilégiée, car elle évite de désactiver la fonction de durcissement.

Le durcissement SYSVOL n'interfère avec Tenable Identity Exposure que lors de la connexion au(x) contrôleur(s) de domaine surveillé(s) à l'aide de l'authentification NTLM. En effet, NTLM n'est pas compatible avec le paramètre « `RequireMutualAuthentication=1` ». Tenable Identity Exposure prend également en charge Kerberos. Il n'est pas nécessaire de désactiver le durcissement SYSVOL si vous configurez et utilisez correctement Kerberos. Pour plus d'informations, voir Authentification Kerberos.

Désactivation du durcissement SYSVOL

Si vous ne pouvez pas passer à l'authentification Kerberos, vous avez également la possibilité de désactiver le durcissement SYSVOL.

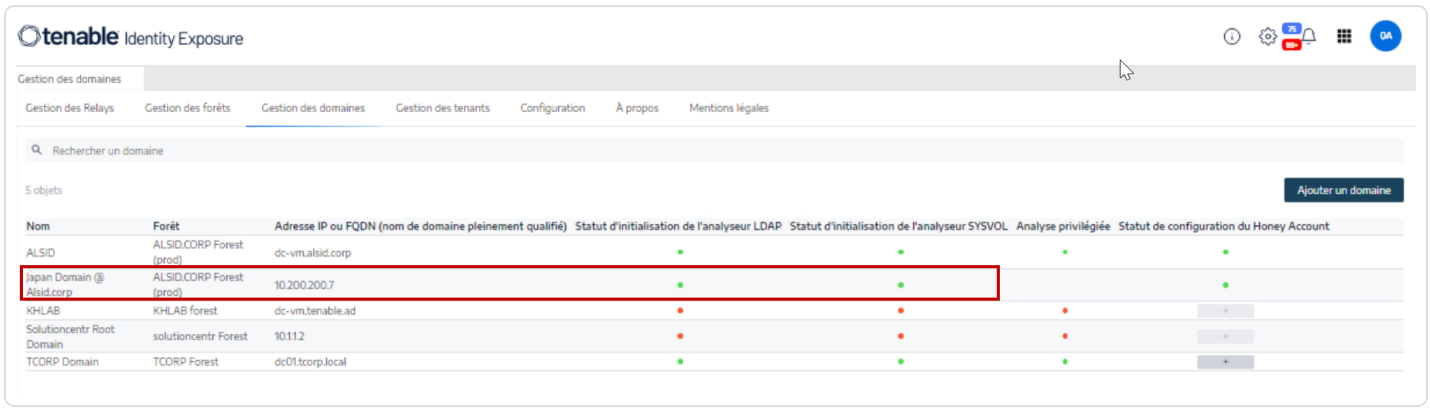
Windows active le durcissement SYSVOL par défaut. Il n'est donc pas suffisant de supprimer la clé de registre ou le paramètre GPO. Vous devez explicitement le désactiver et appliquer ce changement uniquement sur la machine qui héberge le Directory Listener (sur site) ou le Relay (SaaS avec Secure Relay). Cela n'affecte pas les autres machines, et il n'est jamais nécessaire de désactiver le durcissement SYSVOL sur les contrôleurs de domaine eux-mêmes.

Les programmes d'installation Tenable Identity Exposure utilisés sur la machine qui héberge le Directory Listener (sur site) ou le Relay (SaaS avec Secure Relay) désactivent déjà le durcissement SYSVOL localement. Cependant, une GPO ou un script de votre environnement peut supprimer ou remplacer la clé de registre.

Il existe deux cas possibles :

- Si le Directory Listener ou la machine Relay **ne sont pas joints à un domaine** – Vous ne pouvez pas utiliser une GPO pour configurer la machine. Vous devez désactiver le durcissement SYSVOL dans le registre (voir Registre – Interface graphique ou Registre – PowerShell).
- Si le Directory Listener ou la machine Relay **sont joints à un domaine** (ce que Tenable Identity Exposure ne recommande pas) – Vous pouvez appliquer le paramètre directement ou dans le registre (voir Registre – Interface graphique ou Registre – PowerShell) ou utiliser une GPO. Quelle que soit la méthode choisie, vous devez vous assurer qu'une GPO ou un script ne puisse pas écraser la clé de registre. Vous pouvez le faire de deux manières :
    - Examinez attentivement toutes les GPO qui s'appliquent sur cette machine.
    - Appliquez la modification et attendez un peu, ou forcez l'application des GPO à l'aide de la commande « `gpupdate /force` » et vérifiez que la clé de registre a conservé sa valeur.

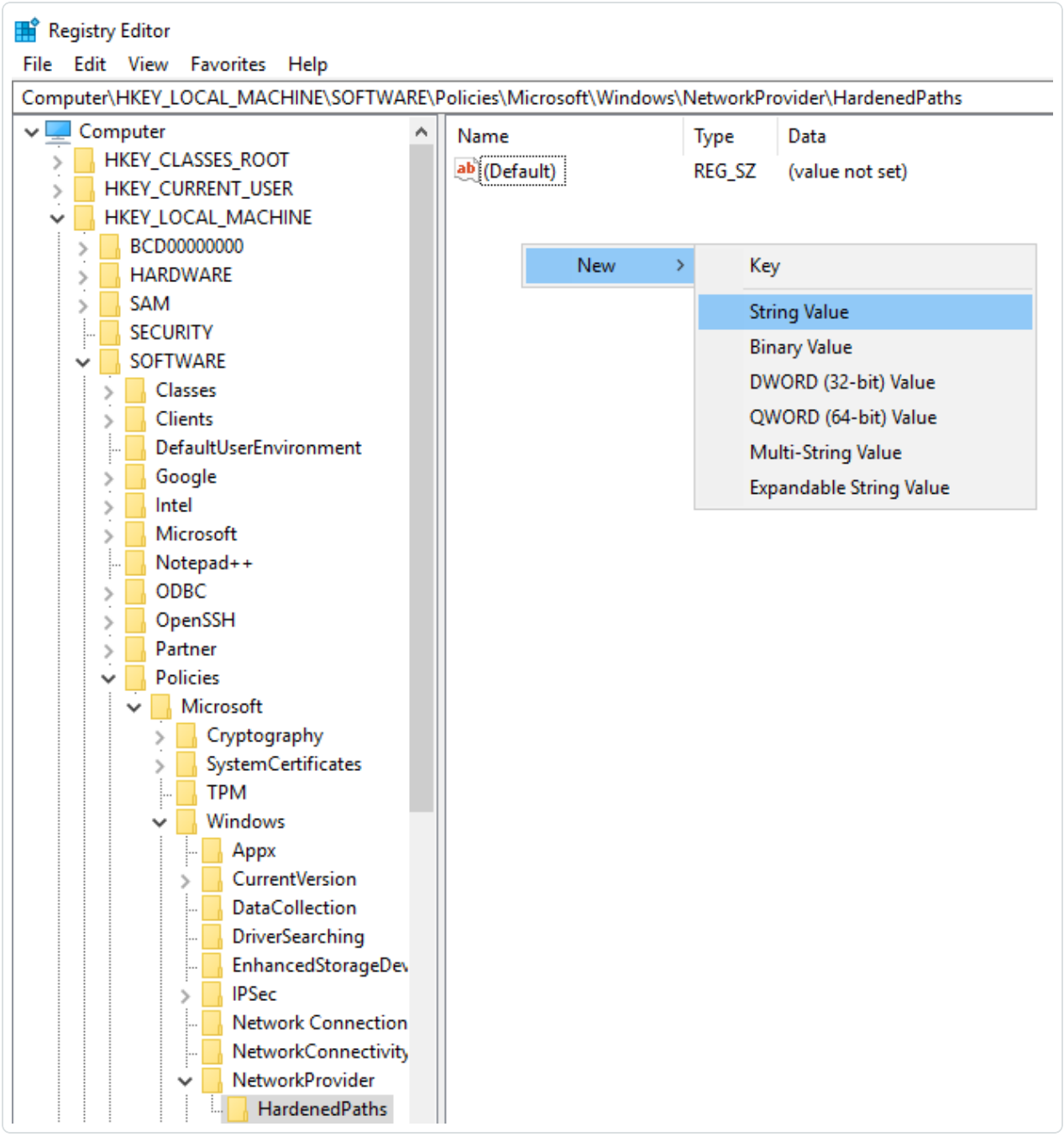
Après avoir redémarré le Directory Listener ou la machine Relay, l'indicateur d'exploration du domaine modifié doit devenir vert :



Registre – Interface graphique

Pour désactiver le durcissement SYSVOL dans le registre à l'aide de l'interface graphique :

1. Connectez-vous au Directory Listener ou à la machine Relay avec des droits d'administration.
2. Ouvrez l'éditeur de registre et accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`.
3. Créez comme suit la clé « `\\*\SYSVOL` » si elle n'existe pas déjà :
    a. Cliquez avec le bouton droit dans le volet de droite et choisissez **Nouveau** > **Valeur de chaîne**.



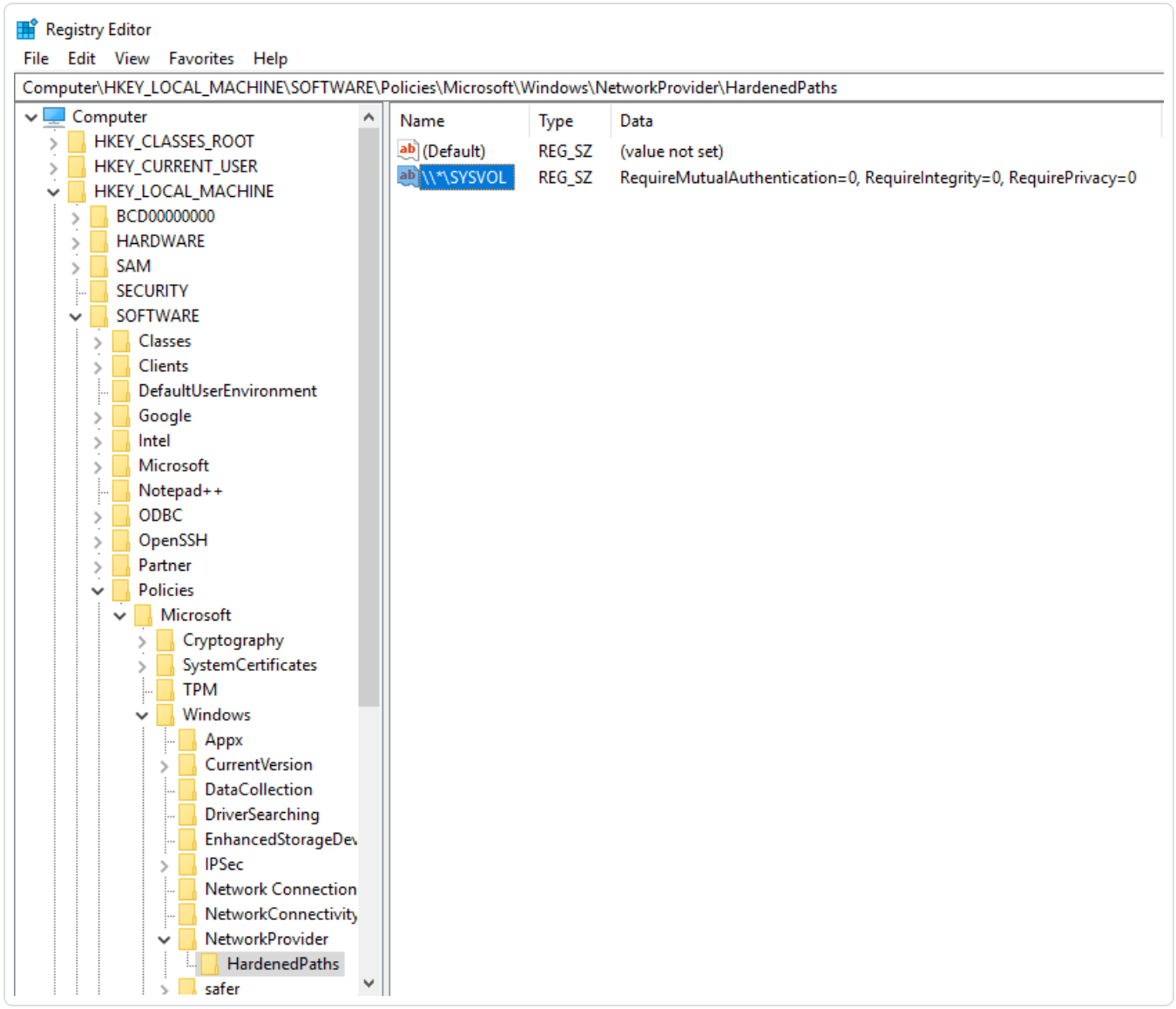
b. Dans le champ Nom, saisissez `\\*\SYSVOL`.

4. Double-cliquez sur la clé « `\\*\SYSVOL` » (nouvellement créée ou existante) pour ouvrir la fenêtre **Modification de la chaîne**.

5. Dans le champ de données **Valeur**, saisissez la valeur suivante : `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0`

6. Cliquez sur **Enregistrer**.

   Le résultat se présente comme suit :



7. Redémarrez l'ordinateur.

Registre – PowerShell

Pour désactiver le durcissement SYSVOL dans le registre en utilisant PowerShell :

1. Collectez les valeurs actuelles des clés de registre des chemins durcis UNC pour référence en utilisant la commande PowerShell suivante :

```
Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
```

2. Définissez la valeur recommandée :

```
New-ItemProperty -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -
Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
```

3. Redémarrez l'ordinateur.

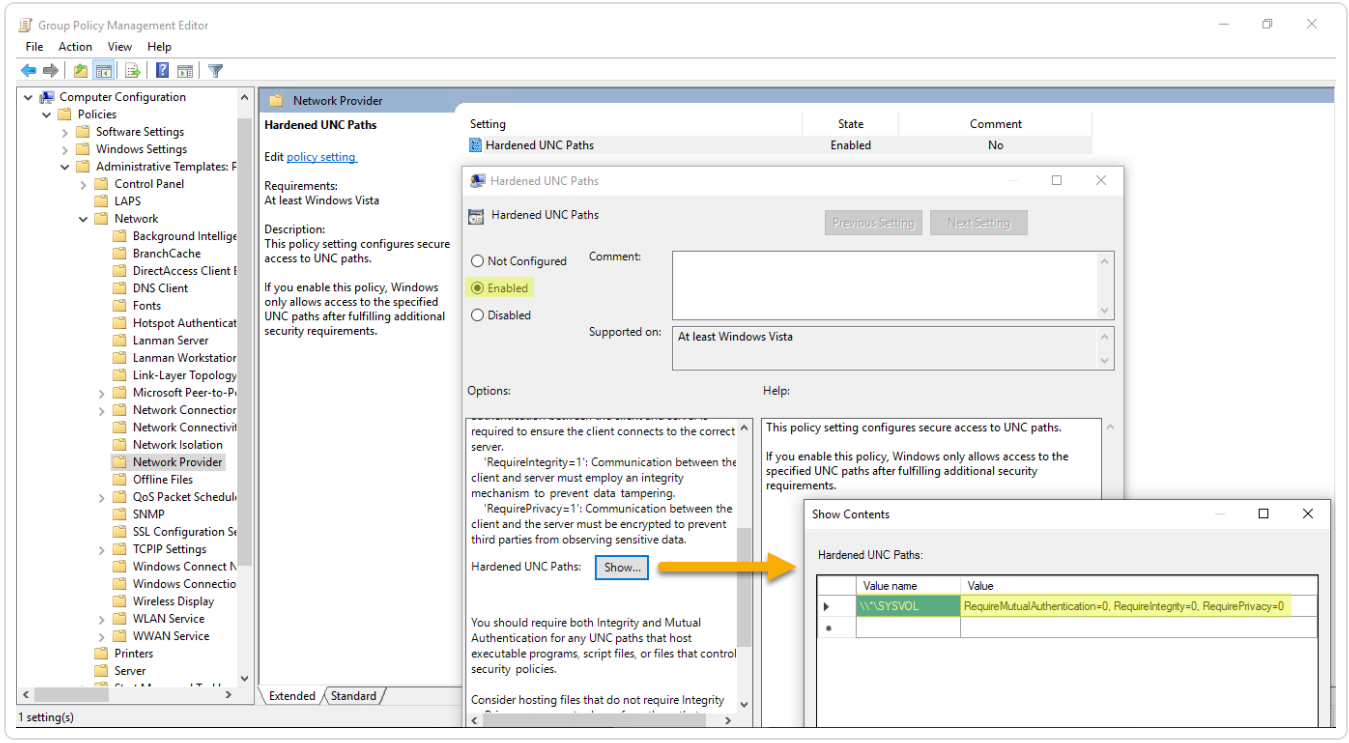
GPO

Condition préalable : vous devez vous connecter en tant qu'utilisateur Active Directory avec les droits nécessaires pour créer des GPO sur le domaine et pour les lier à l'unité d'organisation qui contient le Tenable Identity Exposure Directory Listener ou la machine Relay.

Pour désactiver le durcissement SYSVOL à l'aide d'une GPO :

1. Ouvrez la console de gestion des stratégies de groupe.
2. Créez une GPO.
3. Modifiez la GPO et accédez à l'emplacement suivant : `Configuration ordinateur\Modèles d'administration\Réseau\Fournisseur réseau\Chemins d'accès UNC renforcés`.
4. Activez ce paramètre et créez un chemin UNC durci avec :
   - Nom de la valeur =`\\*\SYSVOL`
   - Valeur = `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0`

   Le résultat se présente comme suit :

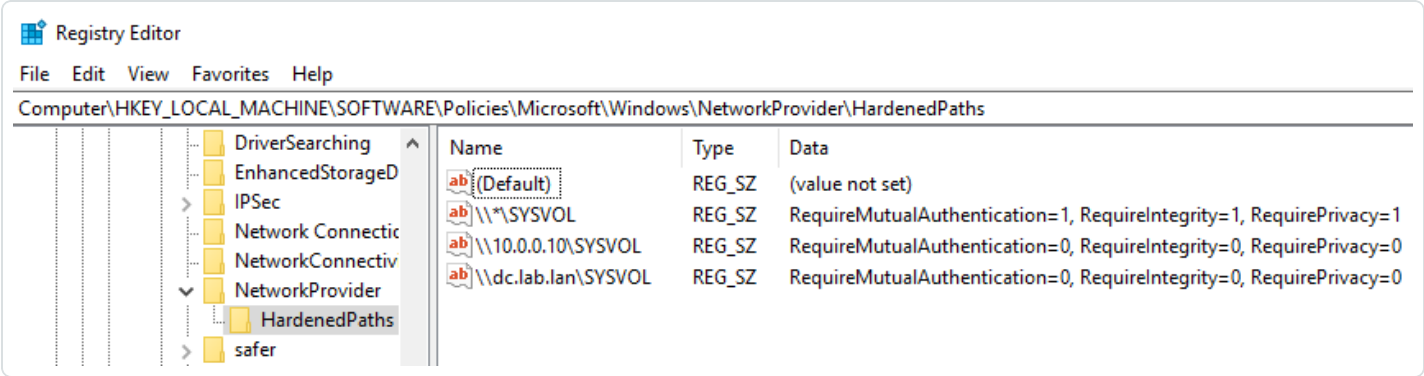


5. Cliquez sur **OK** pour confirmer.
6. Liez cette GPO à l'unité d'organisation qui contient le Tenable Identity Exposure Directory Listener ou la machine Relay. Vous pouvez également utiliser la fonction de filtrage de groupe de sécurité pour vérifier que cette GPO s'applique uniquement à cette machine.

Exceptions spécifiques de chemin UNC

Les procédures précédentes désactivent le durcissement SYSVOL en utilisant un chemin UNC générique : « `\\*\SYSVOL` ». Vous pouvez également le désactiver uniquement pour une adresse IP ou un FQDN spécifique. Cela signifie que vous pouvez garder les paramètres de chemins durcis UNC activés (avec la valeur « `1` ») pour « `\\*\SYSVOL` » et avoir une exception correspondant à chaque adresse IP ou FQDN d'un contrôleur de domaine configuré dans Tenable Identity Exposure.

L'image suivante montre un exemple de durcissement SYSVOL activé pour tous les serveurs (« `*` »), à l'exception de « `10.0.0.10` » et « `dc.lab.lan` », qui sont des contrôleurs de domaine que nous avons configurés dans Tenable Identity Exposure :



Vous pouvez ajouter ces paramètres supplémentaires à l'aide du registre ou des GPO en suivant les méthodes décrites ci-dessus.

Remarque : vous devez spécifier la valeur exacte configurée dans Tenable Identity Exposure (par exemple, vous ne pouvez pas spécifier une adresse IP si la configuration Tenable Identity Exposure utilise un FQDN.). Veillez également à mettre à jour ces clés chaque fois que vous modifiez une adresse IP ou un FQDN dans la page de gestion des domaines Tenable Identity Exposure.

Risques liés à la désactivation du durcissement SYSVOL

Le durcissement SYSVOL étant une fonctionnalité de sécurité, sa désactivation peut soulever des inquiétudes légitimes.

- Machines non jointes à un domaine – La désactivation du durcissement SYSVOL ne présente aucun risque. Étant donné que ces machines n'appliquent pas de GPO, elles ne reçoivent pas de contenu du partage SYSVOL à exécuter.
- Machines jointes à un domaine (Directory Listener ou machine Relay), ce que Tenable Identity Exposure ne recommande pas – S'il existe un risque potentiel d'attaque par une interception entre le Directory Listener ou la machine Relay et les contrôleurs de domaine, la désactivation du durcissement SYSVOL présente un risque. Dans ce cas, Tenable Identity Exposure recommande de passer plutôt à l'authentification Kerberos.

La désactivation affecte le Directory Listener ou la machine Relay, mais pas les autres ordinateurs de domaine ni les contrôleurs de domaine.

Utilitaire système (handle.exe)

`Handle.exe` est un processus Windows légitime que Tenable Identity Exposure utilise pour obtenir des informations détaillées sur l'utilisation des ressources système, en particulier sur les

descripteurs ouverts pour tous les processus système. Pour plus d'informations, voir la documentation Microsoft.

Assurez-vous que votre logiciel antivirus ne le bloque pas.