Guide de l'utilisateur et de l'administrateur Tenable Identity Exposure 3.x

Dernière révision : 5 avril 2024

Copyright © 2024 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 Tenable Identity Exposure

Dernière mise à jour : 30/04/2024

Tenable Identity Exposure (anciennement Tenable.ad) 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.

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

Pour démarrer, voir Premiers pas avec Tenable Identity Exposure.

> **Remarque :** Tenable Identity Exposure peut être acheté seul ou dans le cadre de la suite Tenable One. Pour plus d'informations, voir Tenable One.

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

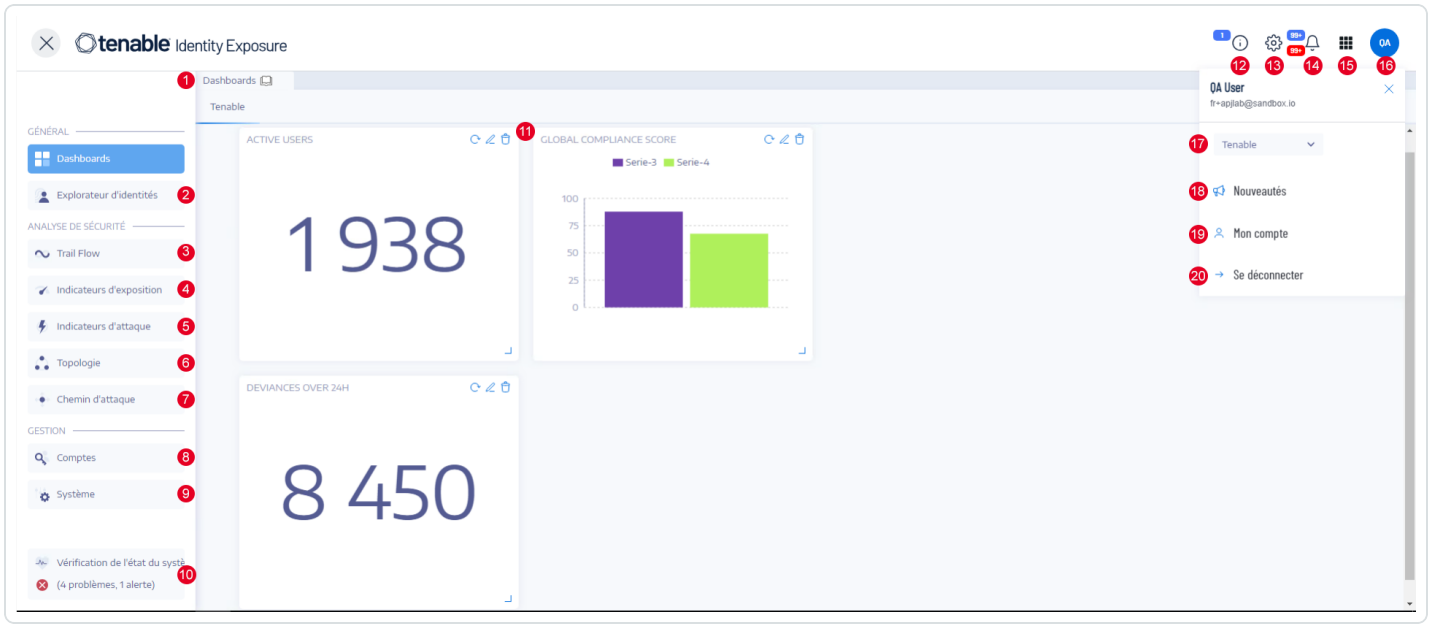
> **Conseil :** pour plus d'informations sur la prise en main des produits Tenable One, voir le Guide de déploiement de Tenable One.

Naviguer dans 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 **X** 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	Explorateur d'identités	La vue Explorateur d'identités de Tenable Identity Exposure unifie les identités entre Active Directory et Microsoft Entra ID. Cette vue affiche le score de risque de l'identité (bêta) pour chaque asset répertorié et la

		portée potentielle des identités compromises.
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	Topology	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 Guide de l'administrateur 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	Sélecteur d'applications	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.

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 :

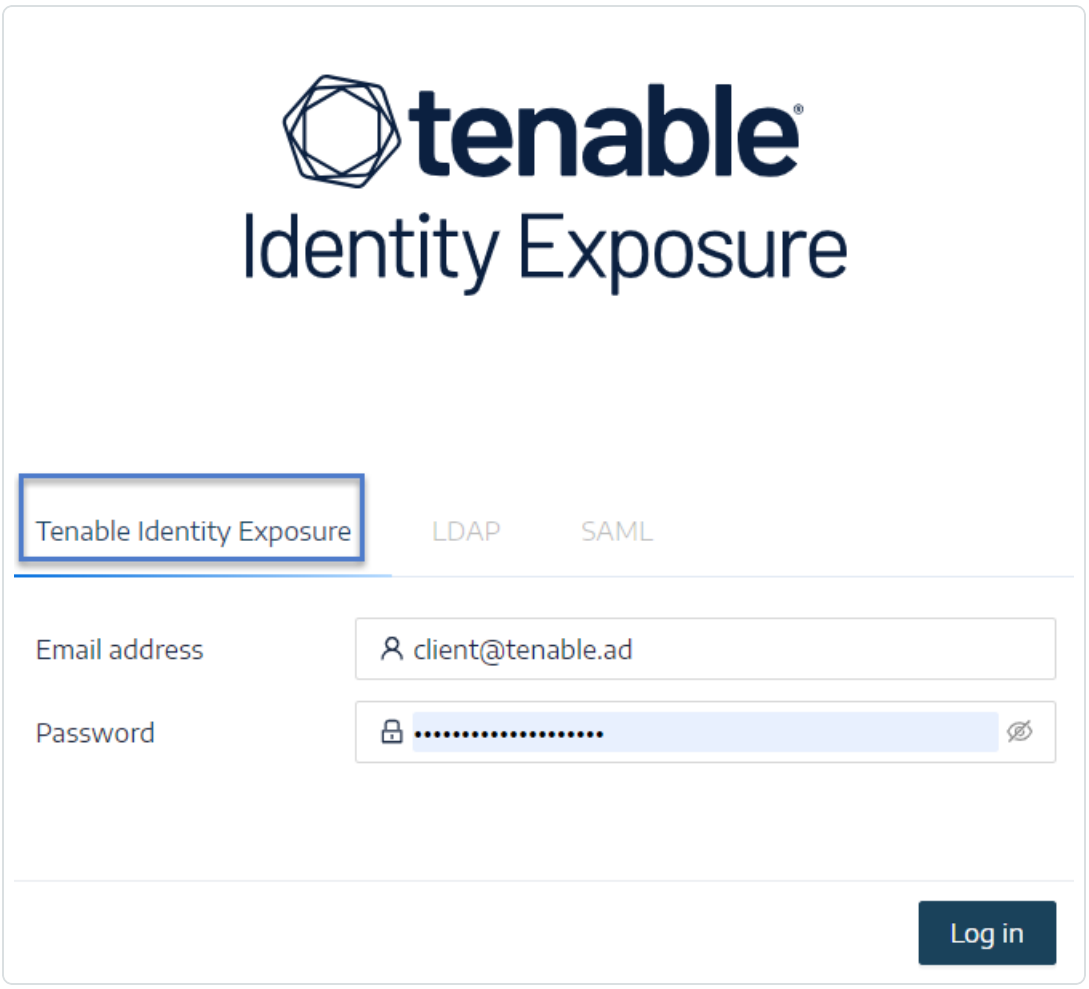
- - Utilisation d'un compte Tenable Identity Exposure
  - Utilisation d'un compte LDAP
  - Utilisation de SAML

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**.

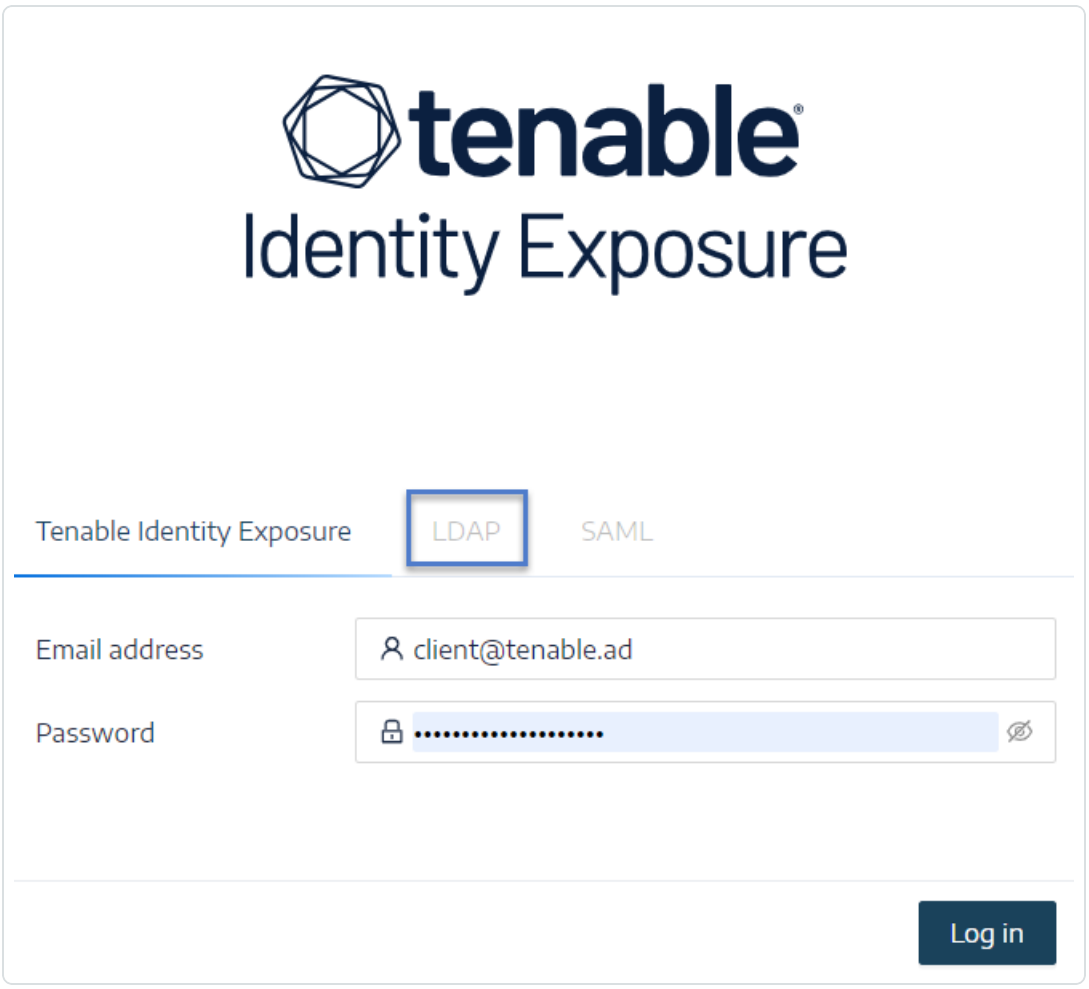
   La page Tenable Identity Exposure apparaît.

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**.

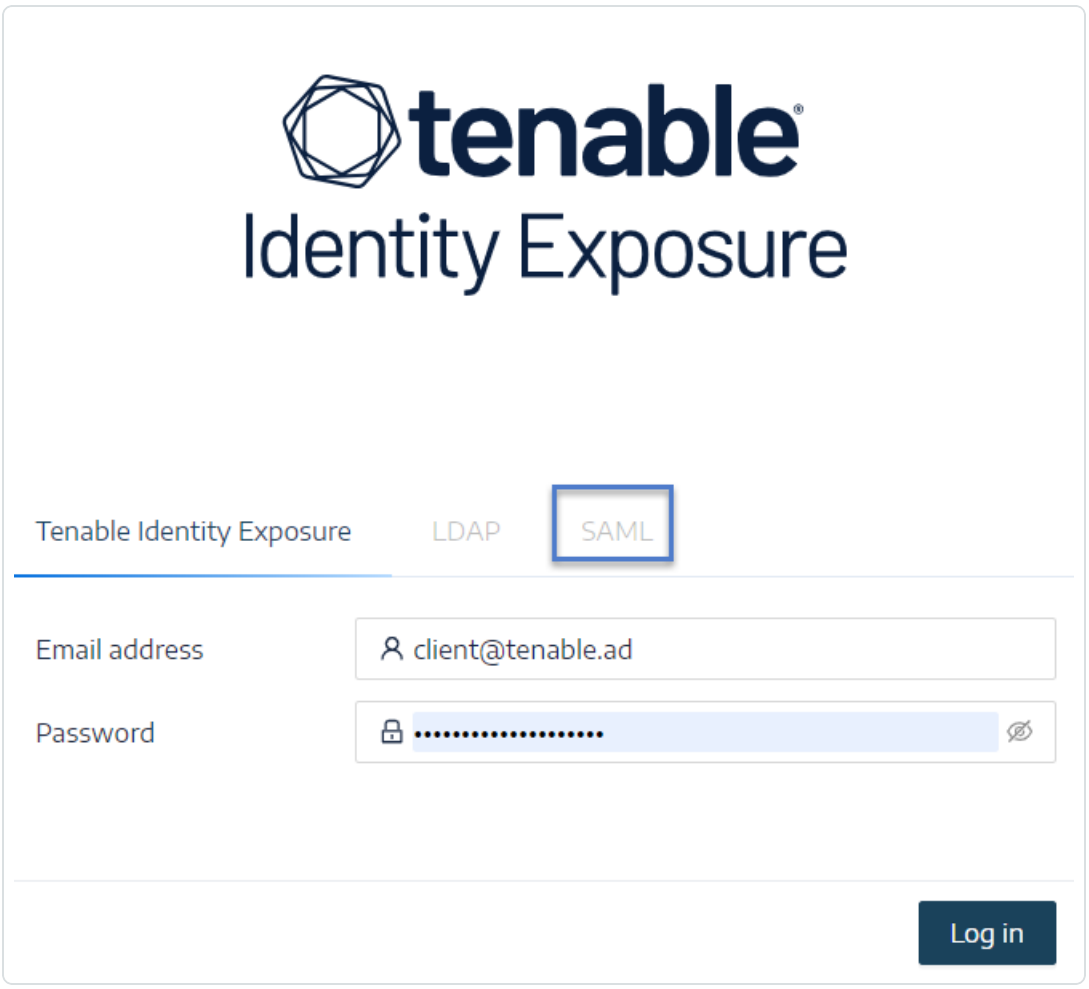
   La page Tenable Identity Exposure apparaît.

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 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.

Accéder à l'espace de travail

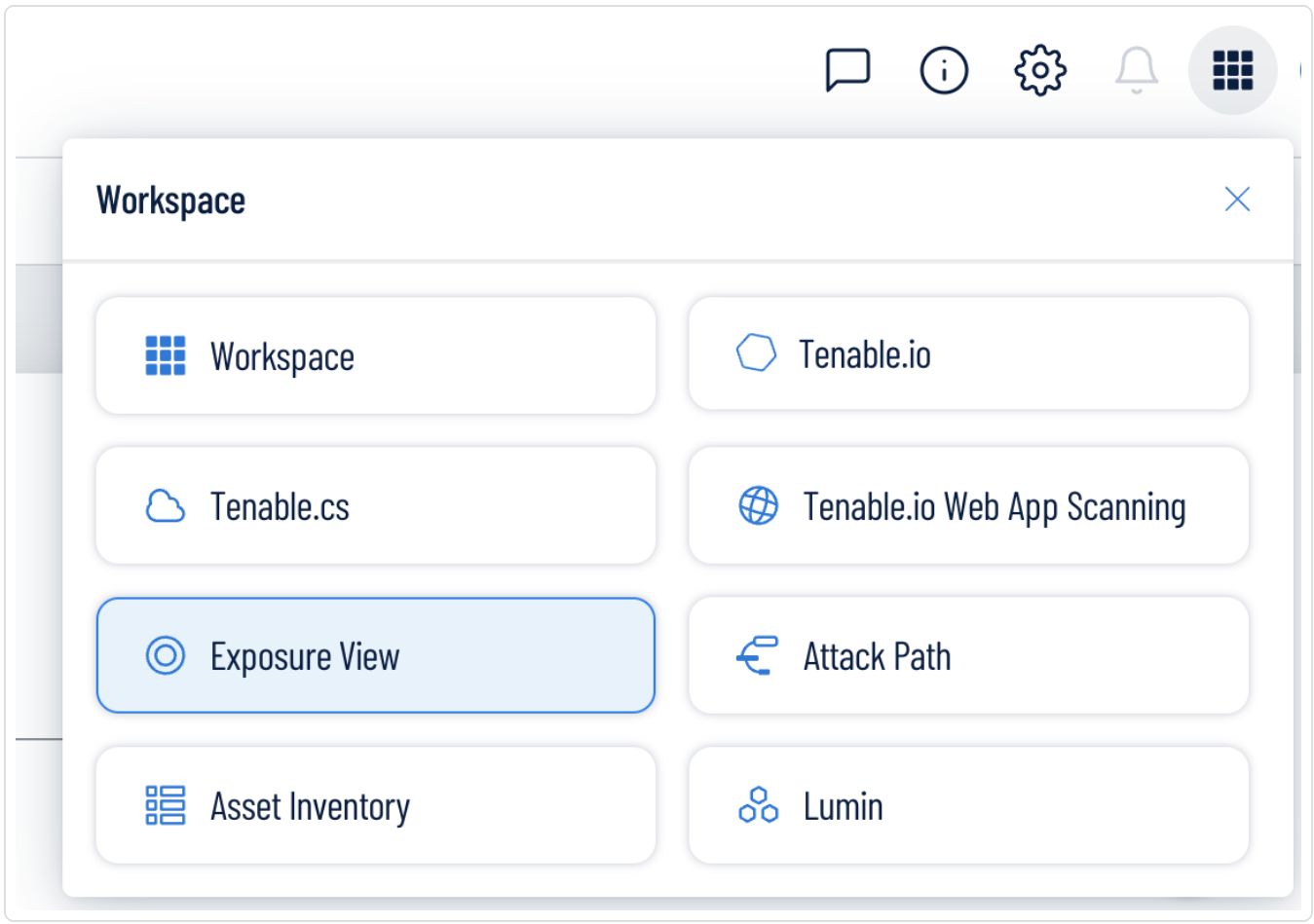
Lorsque vous vous connectez à Tenable, la page **Espace de travail** apparaît par défaut. Sur la page **Espace de travail**, vous pouvez passer d'une application Tenable à une autre ou définir une application par défaut pour y accéder sans afficher la page **Espace de travail** à l'avenir. Vous pouvez également passer d'une application à une autre à partir du menu **Espace de travail** qui apparaît dans la barre de navigation supérieure.

Ouvrir le 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.

Afficher la page Espace de travail

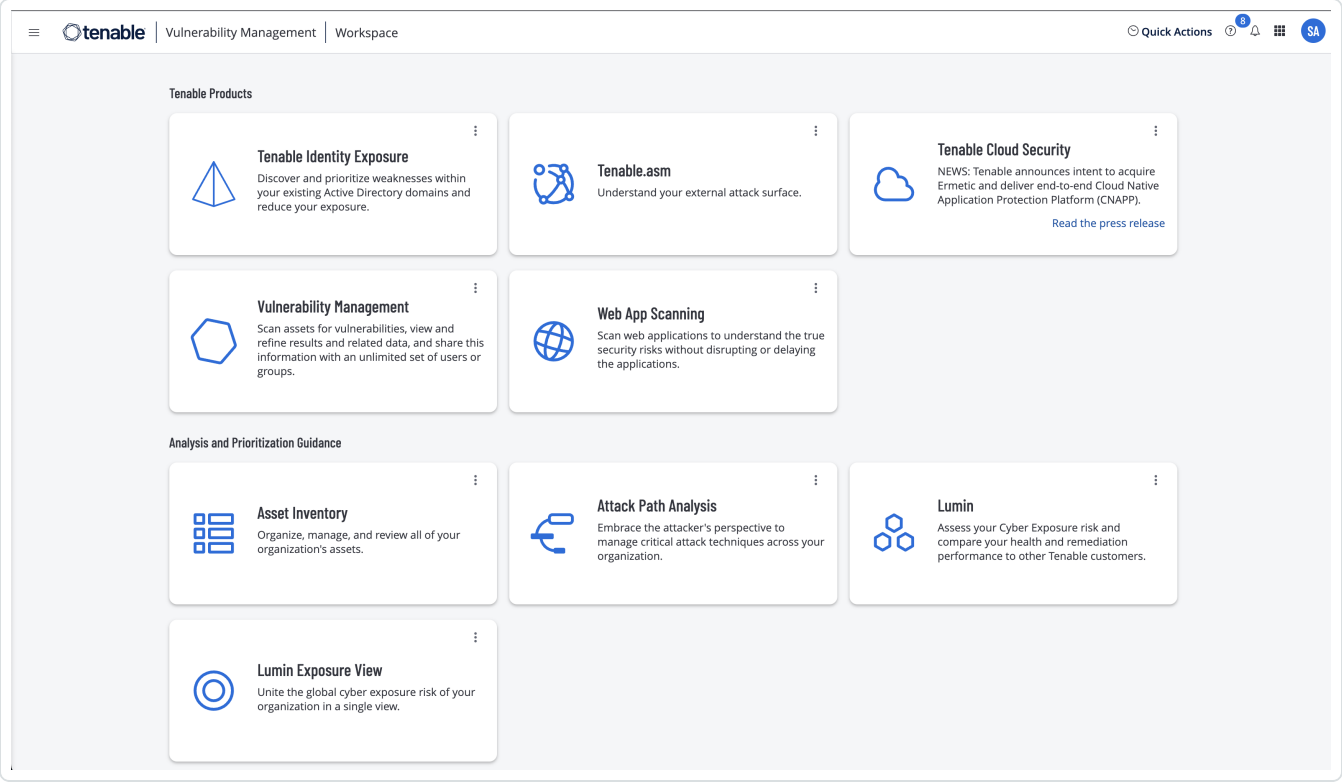
Pour afficher la page Espace de travail :

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 **Espace de travail**.

La page **Espace de travail** apparaît.



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.

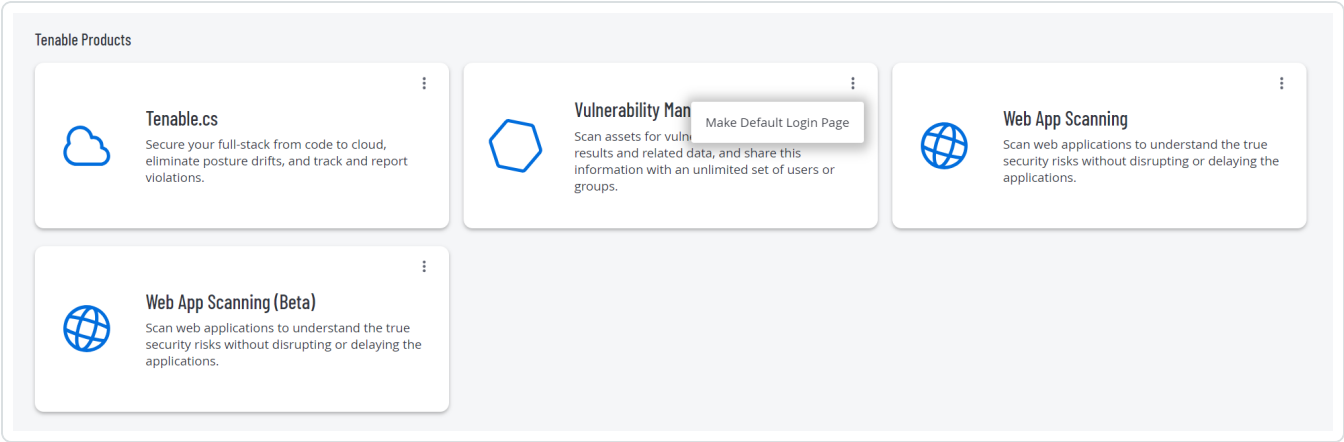
Pour définir une application de connexion par défaut :

1. Connectez-vous à Tenable.

   La page **Espace de travail** apparaît.

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

Un menu apparaît.



3. 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. Connectez-vous à Tenable.

   La page **Espace de travail** apparaît.

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

   Un menu apparaît.

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

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

Préférences utilisateur

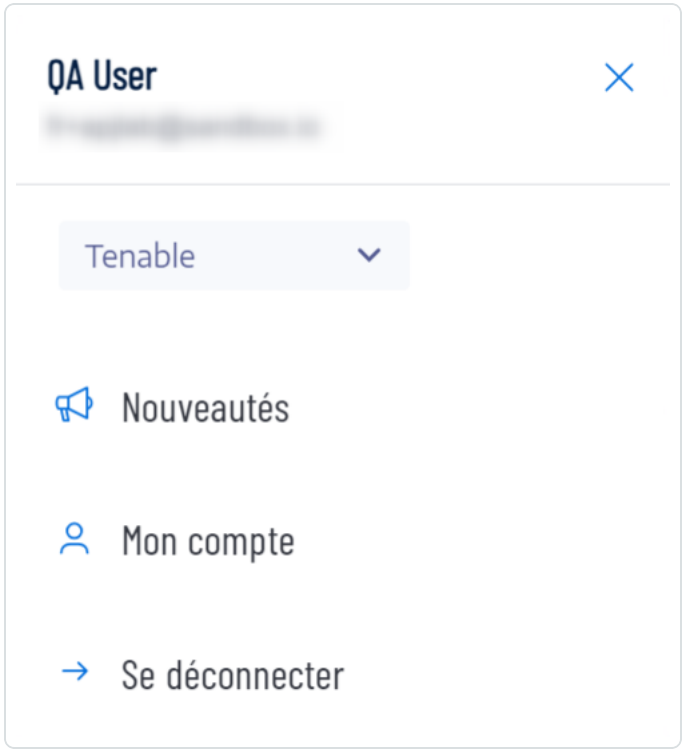
Vous pouvez définir vos préférences utilisateur dans Tenable Identity Exposure.

- 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 **My Account** (Mon compte).

   La page **Preferences** (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 **Save** (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. Fournissez les éléments suivants :

   - Votre ancien mot de passe.
   - Votre nouveau mot de passe.

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

d. 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.

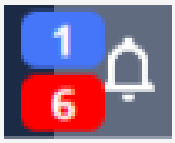
   Un message vous demande confirmation.

> **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**.

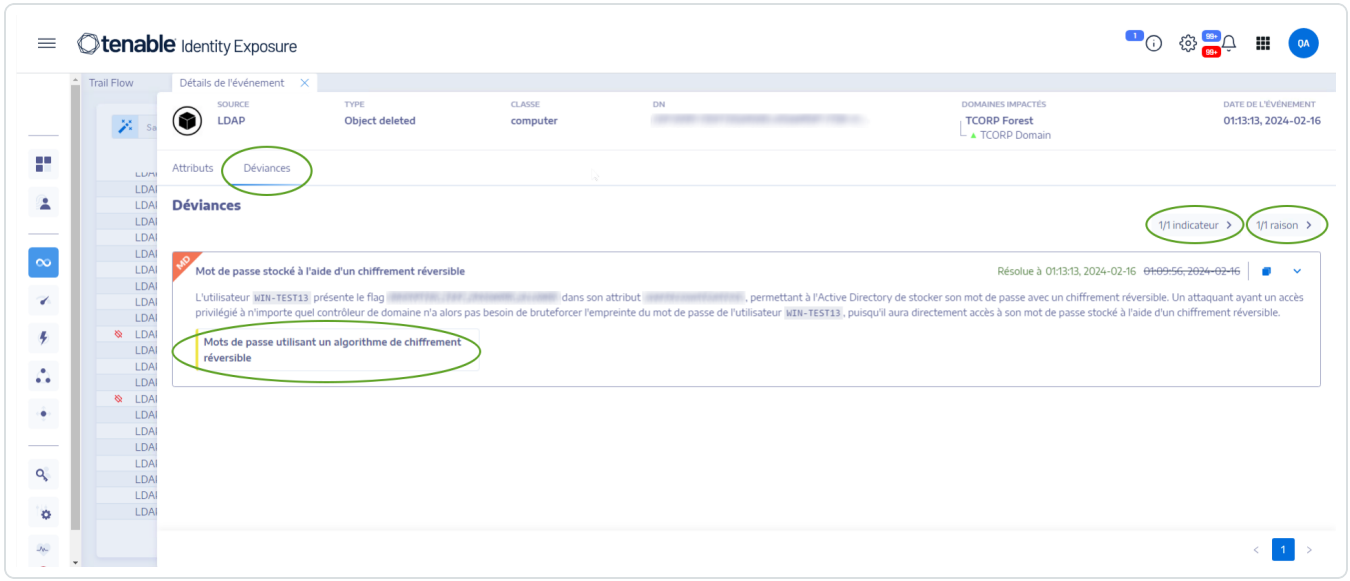
   Le volet Détails de l'événement apparaît avec les informations suivantes :

   - 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.

Tenable Identity Exposure fournit des modèles de dashboards que vous pouvez utiliser pour vous concentrer sur les problèmes prioritaires qui affectent votre organisation, notamment les modèles suivants :

- **Conformité AD et risques principaux** — Score de conformité, évolution et conformité à la criticité du risque
- **AD risque 360** — Évolution de la déviance et problèmes selon le niveau de sévérité de l'indicateur d'exposition
- **Gestion du risque des mots de passe** — Problèmes liés aux mots de passe
- **Surveillance des utilisateurs** — Évolution des utilisateurs AD, nombre de catégories d'utilisateurs
- **Surveillance des administrateurs natifs** — Métriques des comptes d'administration

Pour créer un dashboard à l'aide d'un modèle :

1. Dans Tenable Identity Exposure, cliquez sur  ou sur **Dashboards**. Cette page s'ouvre également par défaut dans Tenable Identity Exposure.
2. Vous pouvez procéder de deux manières :
   - Si le volet est vide : cliquez sur **Ajouter des dashboards**.
   - Si le volet contient déjà au moins un dashboard : cliquez sur  > **Ajouter un nouveau dashboard** dans l'angle supérieur droit.

     Le volet **Configuration des modèles de dashboards** apparaît.
3. Sélectionnez les dashboards à ajouter.
4. Cliquez sur **Ajouter des dashboards**.

5. Un message confirme que Tenable Identity Exposure a créé le dashboard et les widgets. Les nouveaux dashboards apparaissent sous un onglet dans le volet **Dashboards**.

Pour ajouter un dashboard personnalisé :

1. Dans Tenable Identity Exposure, cliquez sur  ou sur **Dashboards**. Cette page s'ouvre également par défaut dans Tenable Identity Exposure.
2. Cliquez sur  > **Ajouter un nouveau dashboard** dans l'angle supérieur droit.

   Le volet **Configuration des modèles de dashboard** apparaît.
3. Sélectionnez le modèle **Dashboard personnalisé** en bas de l'écran.
4. Saisissez le nom du dashboard.
5. Cliquez sur **Ajouter des dashboards**.

   Un message confirme que Tenable Identity Exposure a créé le dashboard. Les nouveaux dashboards apparaissent sous un onglet dans le volet **Dashboards**.
6. Voir Widgets pour plus d'informations sur l'ajout de widgets à votre dashboard.

Pour renommer un dashboard :

1. Dans le volet **Dashboards**, sélectionnez l'onglet du dashboard à renommer.
2. Cliquez sur > **Modifier le nom** dans l'angle supérieur droit.

   Le volet **Configurer le dashboard** apparaît.
3. Dans la zone **Nom**, saisissez le nouveau nom du dashboard.
4. Cliquez sur **Modifier**.

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

Pour supprimer un dashboard :

1. Dans le volet **Dashboards**, sélectionnez l'onglet du dashboard à supprimer.
2. Cliquez sur > **Supprimer le dashboard** dans l'angle supérieur droit.

Le volet **Supprimer le dashboard** apparaît pour vous demander de confirmer la suppression.

3. Cliquez sur **Supprimer**.

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

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. ■ Sélectionner 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

Explorateur d'identités

Autorisations : pour accéder à la configuration et à la visualisation des données pour Microsoft Entra ID, votre rôle utilisateur doit disposer des autorisations appropriées. Pour plus d'informations, voir Définir les autorisations d'un rôle.

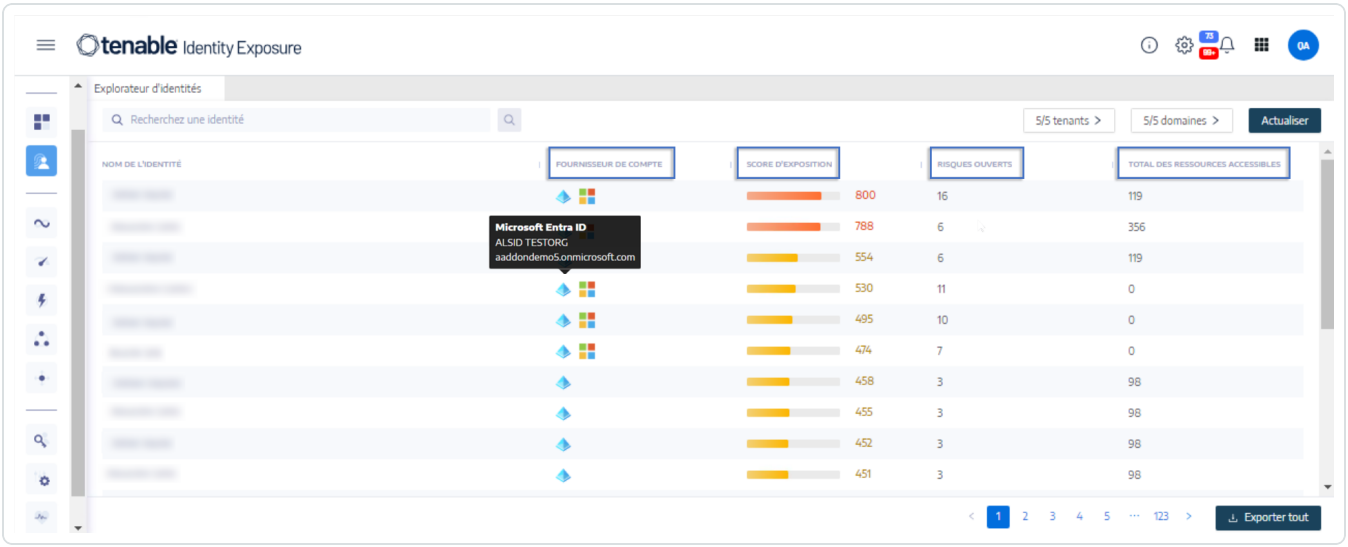
La vue Explorateur d'identités de Tenable Identity Exposure unifie les identités entre Active Directory et Microsoft Entra ID. Cette vue affiche le score de risque de l'identité (bêta) de chaque asset répertorié et la portée potentielle des identités compromises.

Pour accéder à l'Explorateur d'identités :

Remarque : l'Explorateur d'identités n'est visible que si vous utilisez la fonctionnalité Microsoft Entra ID. Pour plus d'informations, voir Support Microsoft Entra ID.

- Dans Tenable Identity Exposure, cliquez sur l'icône Explorateur d'identités dans la barre de navigation de gauche.

  Le volet **Explorateur d'identités** apparaît.



Le volet **Explorateur d'identité** affiche les informations suivantes pour l'ensemble des ressources accessibles :

- **Nom de l'identité** — Nom du compte utilisateur sous le fournisseur d'identité.
- **Fournisseur de compte** — Fournisseur d'identité.

- **Score d'exposition** — Tenable Identity Exposure calcule cette métrique en évaluant la criticité d'un asset ou d'une identité et ses vulnérabilités pour chaque fournisseur d'identité, et l'agrège pour fournir le score d'exposition global d'une identité donnée.

  > **Remarque** : Tenable Identity Exposure n'affiche le score d'exposition que si vous disposez de la licence Tenable One.

- **Risques ouverts** — Nombre de détections qu'un indicateur d'exposition Microsoft Entra ID effectue lorsqu'il scanne l'asset. Pour plus d'informations, voir Indicateurs d'exposition liés à Microsoft Entra ID.
- **Total des ressources accessibles** — Nombre de ressources, quel que soit leur type, auxquelles cet asset a accès (lecture, écriture, etc.)

Pour rechercher une identité :

1. Dans la zone de **recherche** du volet **Explorateur d'identité**, saisissez le nom de l'utilisateur ou du compte.
2. Cliquez sur l'icône .

   Tenable Identity Exposure affiche les résultats correspondants.

Pour exporter des identités :

1. Au bas du volet de l'**Explorateur d'identités**, cliquez sur **Exporter tout**.

   Le volet **Exporter des identités** apparaît.
2. Cliquez sur **Exporter tout**.

   Tenable Identity Exposure télécharge le fichier vers la machine locale.

Trail Flow

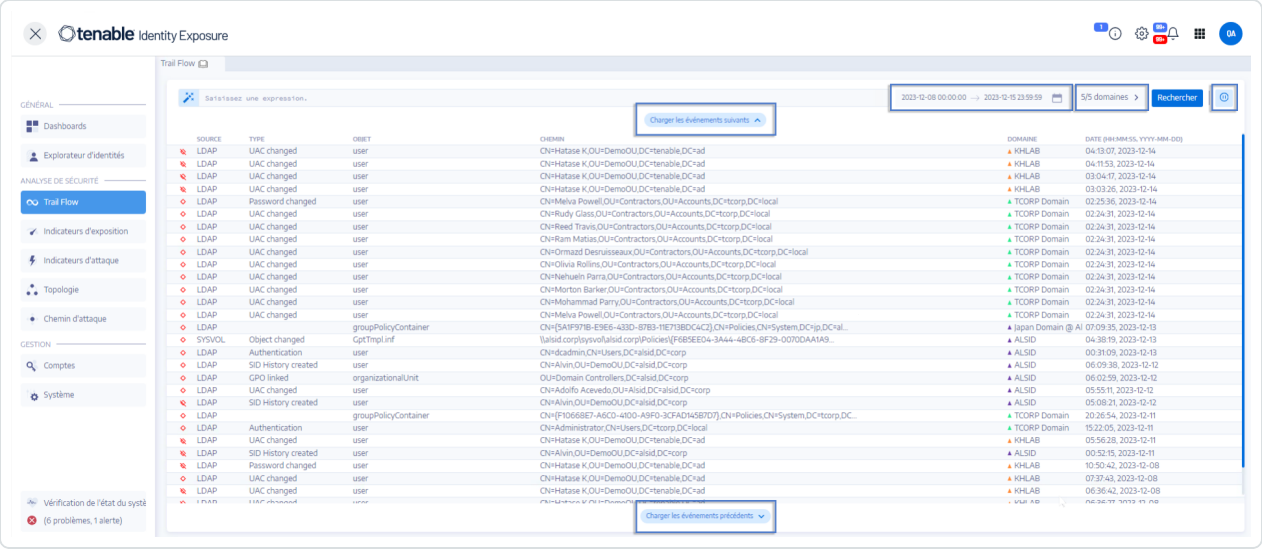
Le Trail Flow de Tenable Identity Exposure affiche la surveillance et l'analyse en temps réel des événements qui affectent votre infrastructure AD. Il permet d'identifier les vulnérabilités critiques et les mesures correctives recommandées.

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.

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 :

1. En haut de la page **Trail Flow**, cliquez sur la zone du calendrier.
2. Sélectionnez une date de début et une date de fin.
3. Cliquez sur **Rechercher**.

   Tenable Identity Exposure met à jour le tableau Trail Flow avec la période sélectionnée.

Pour sélectionner un domaine :

1. En haut de la page **Trail Flow**, cliquez sur **n/n domaines >**.

   Le volet **Forêts et domaines** apparaît.

2. Sélectionnez les forêts et les domaines.

3. Cliquez sur **Filtrer sur la sélection**.

   Tenable Identity Exposure met à jour le tableau Trail Flow et affiche des informations concernant la forêt et le domaine sélectionnés.

Pour afficher un événement :

- Dans le tableau Trail Flow, cliquez sur une ligne contenant l'événement à explorer.

  Le volet Détails de l'événement apparaît. Pour plus d'informations, voir Détails d'un événement.

Pour suspendre Trail Flow et le redémarrer :

- Effectuez l'une des actions suivantes :
  - Cliquez sur l'icône ⏸ pour suspendre le Trail Flow.

    La suspension du Trail Flow arrête le défilement vertical automatique des événements les plus récents, mais l'analyse continue de s'exécuter en arrière-plan et permet d'effectuer une recherche sur les événements.
  - Cliquez sur l'icône ▶ pour redémarrer le Trail Flow.

Pour charger les événements suivants ou précédents :

- Sur la page Trail Flow, effectuez l'une des opérations suivantes :
  - Cliquez sur Charger les événements suivants.
  - Cliquez sur Charger les événements 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

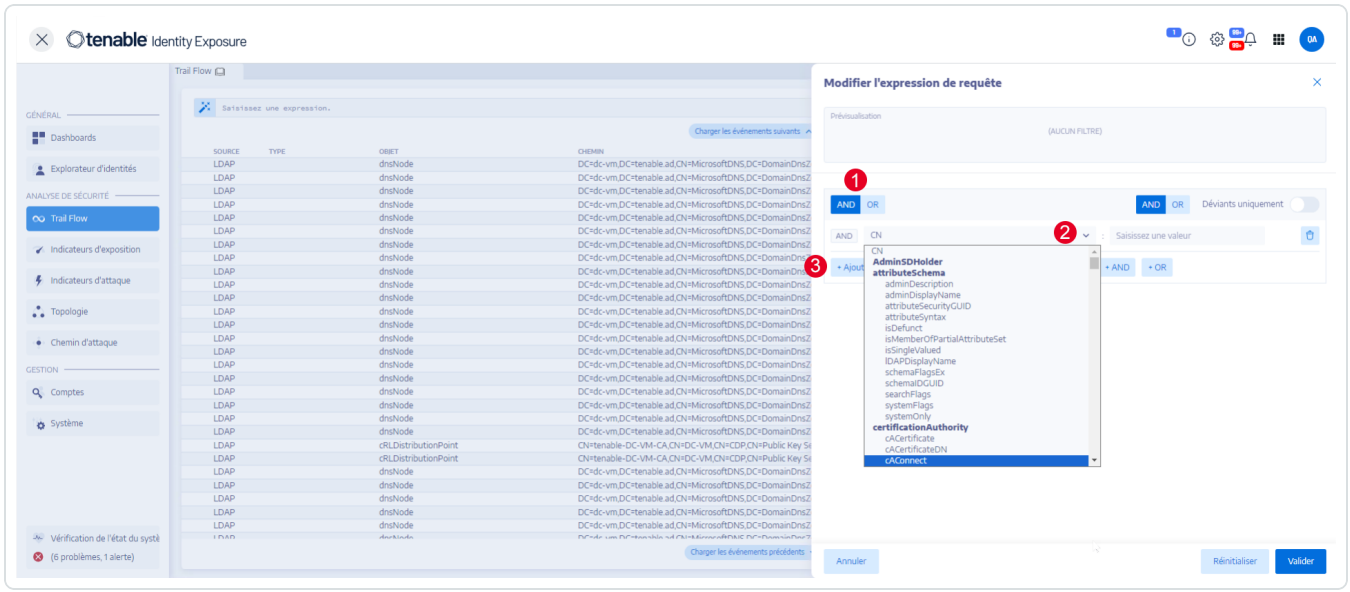
L'assistant de recherche vous permet de créer et de combiner des expressions de requête.

- 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 :

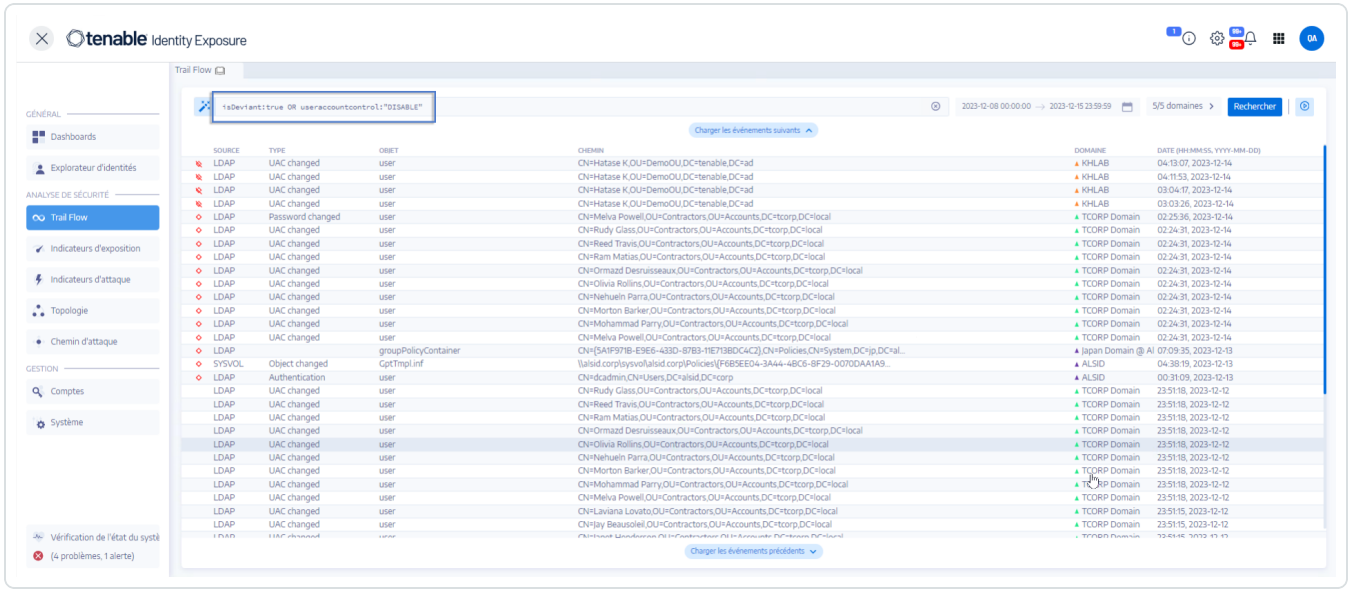
1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Dans la zone de recherche, saisissez une expression de requête.
3. Vous pouvez filtrer les résultats de la recherche comme suit :
    - Cliquez dans la zone **Calendrier** pour sélectionner une date de début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

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.



Grammaire et syntaxe

Une expression de requête manuelle utilise la grammaire et la syntaxe suivantes :

- Grammaire : `EXPRESSION [OPERATOR EXPRESSION]*`
- Syntaxe : `__KEY__ __SELECTOR__ __VALUE__`

  où :

  - `__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" and types:"SCRIPTSini"`

  > **Remarque** : ici, `types` fait référence à l'attribut d'objet et non pas à l'en-tête de colonne.

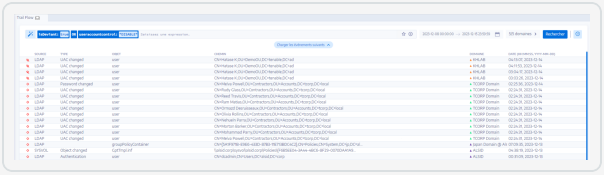
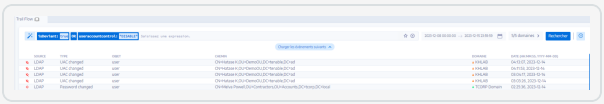
Personnaliser les requêtes Trail Flow

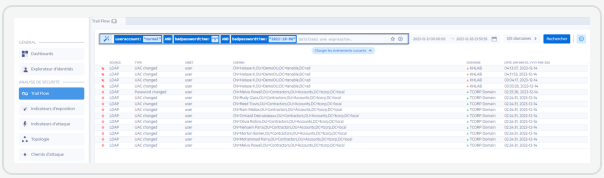
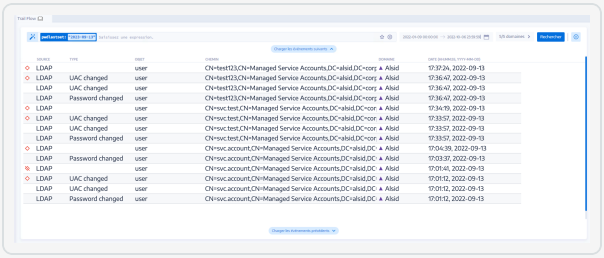
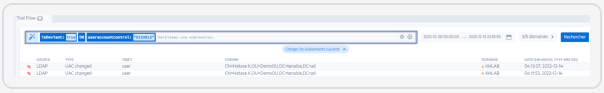
Le Trail Flow permet d'étendre les fonctionnalités Tenable Identity Exposure au-delà de la surveillance par défaut des indicateurs d'exposition et des indicateurs d'attaque. Vous pouvez créer des requêtes personnalisées pour récupérer rapidement des données et également utiliser la requête comme une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

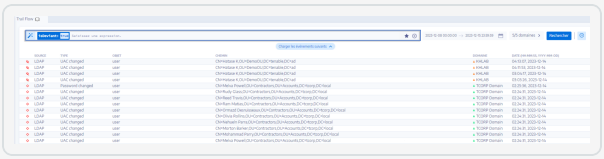
Les exemples suivants montrent des requêtes personnalisées pratiques dans Tenable Identity Exposure.

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.

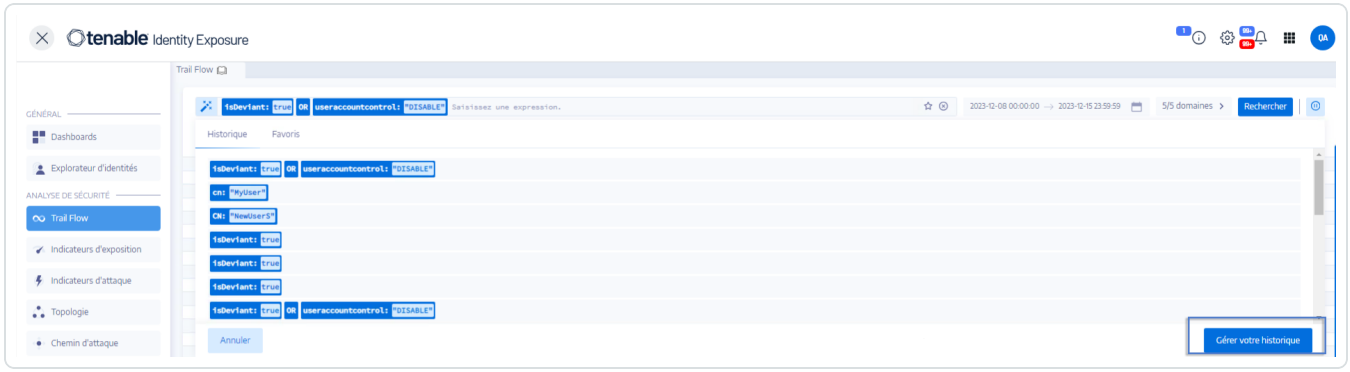
Pour utiliser une expression de requête de l'historique :

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

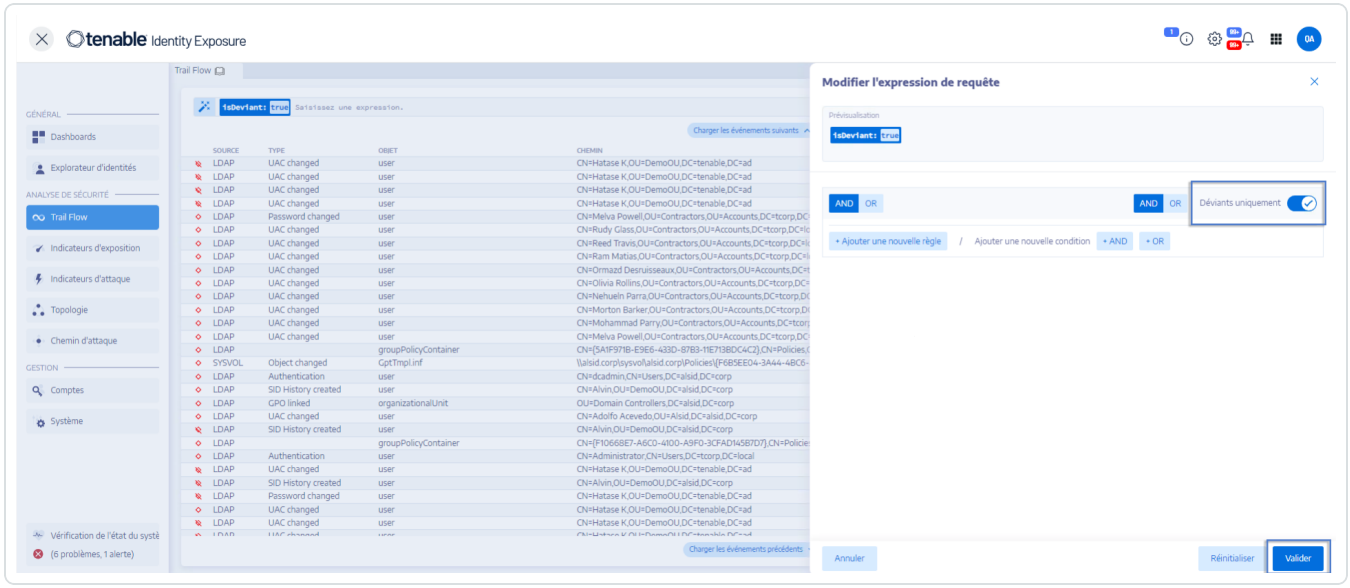
Afficher les événements déviants

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

Pour afficher uniquement les événements déviants :

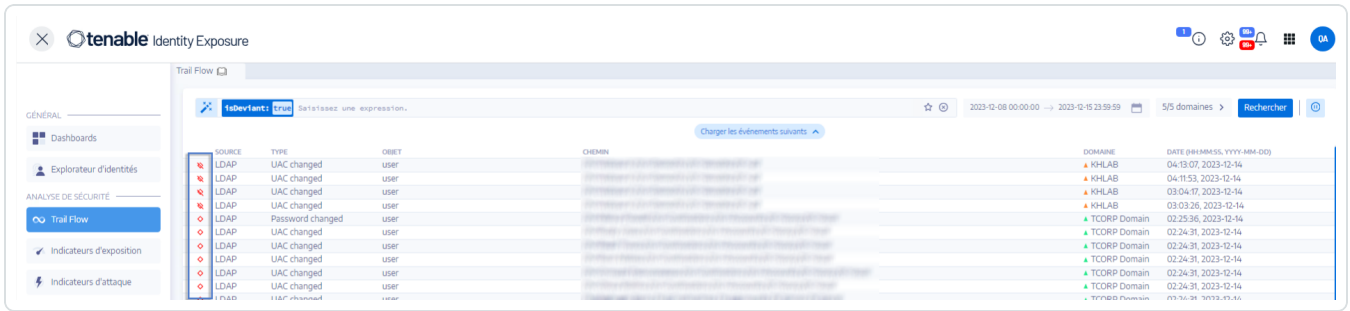
1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez sur l'icône en regard de la zone de recherche.

   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.



où :

- 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.

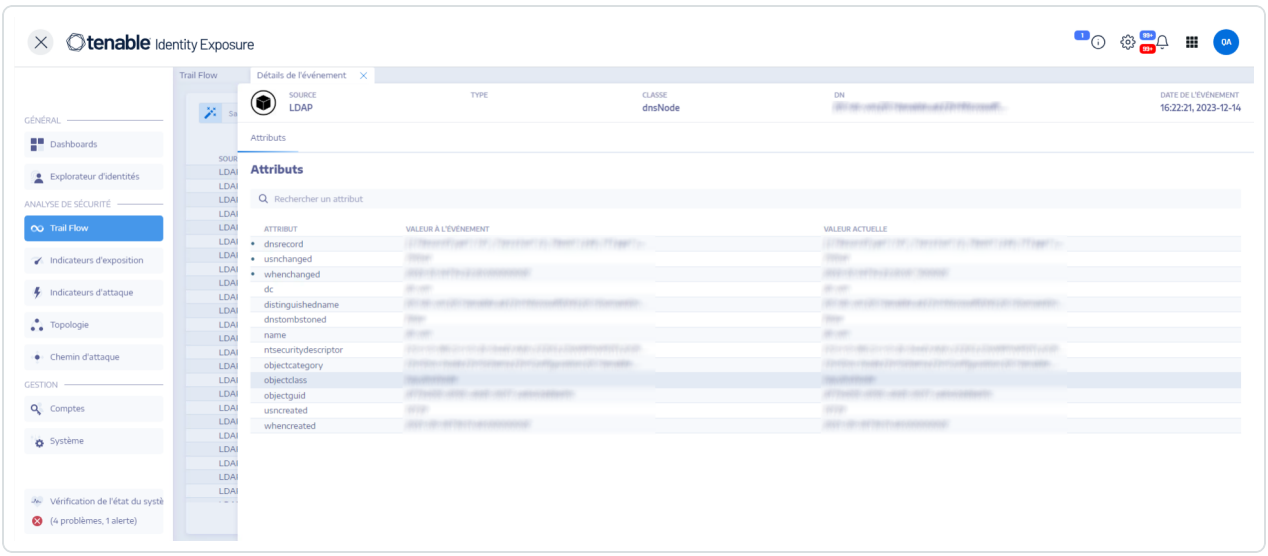


Tableau des attributs

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

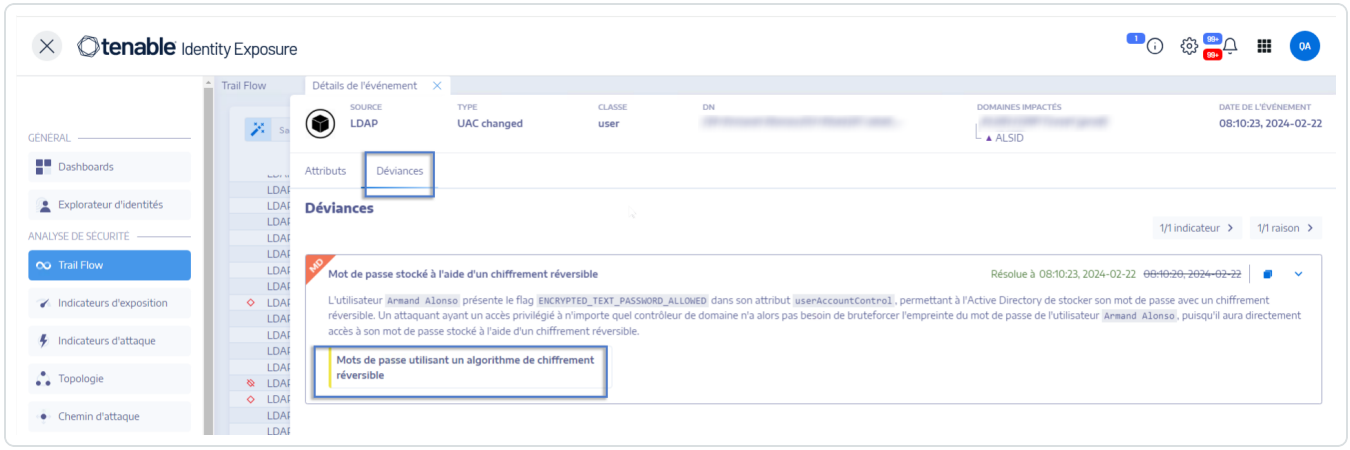
Si un événement du Trail Flow contient des déviances, le volet Détails de l'événement les affiche également pour vous permettre d'accéder à la source du problème.

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 :

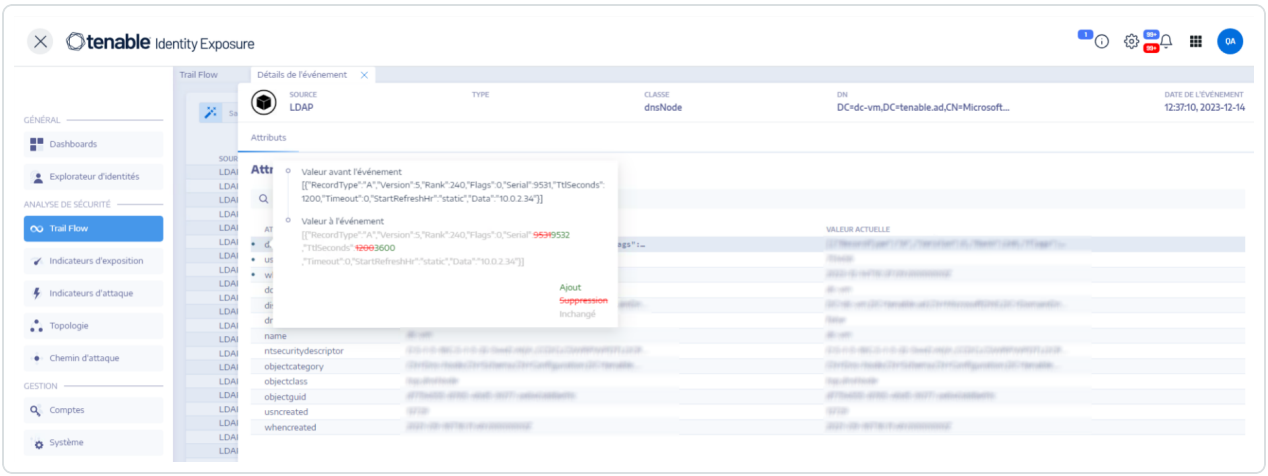
1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** dans la barre de navigation sur la partie gauche.

   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**



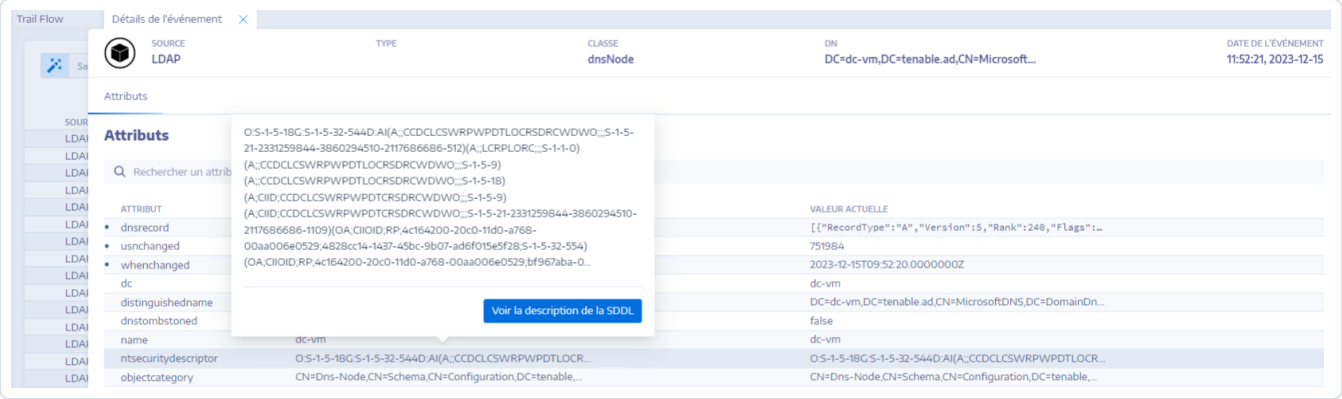
Attribut « ntsecuritydescriptor »

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 :

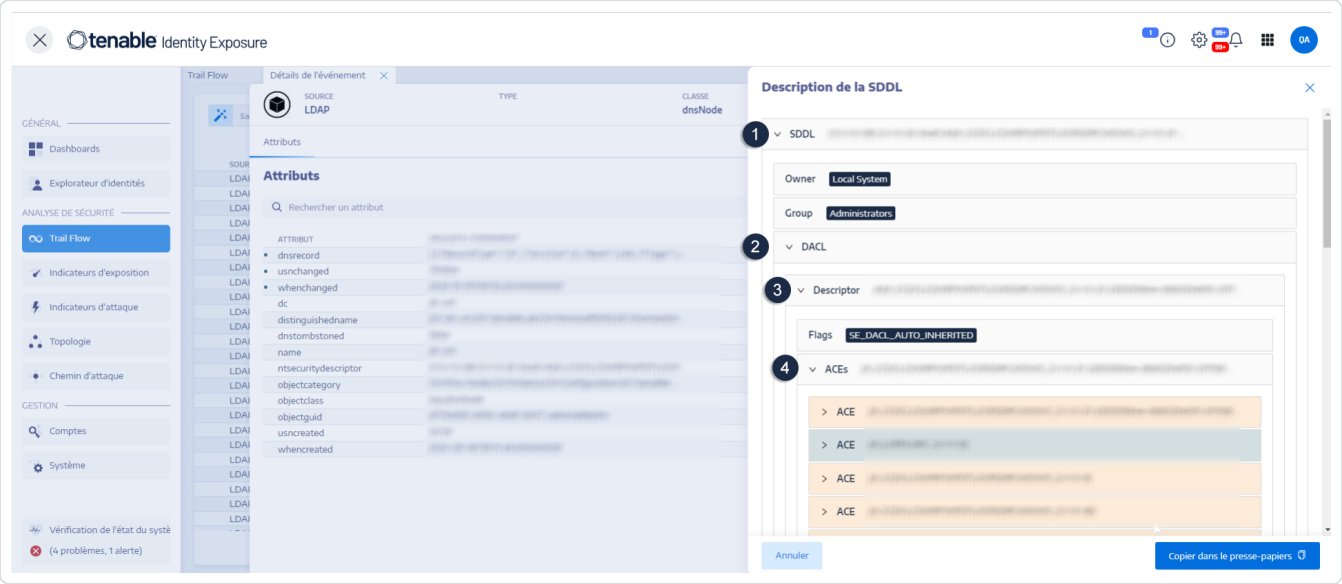
1. Dans Tenable Identity Exposure, cliquez sur **Trail Flow** pour ouvrir la page Trail Flow.
2. Cliquez pour sélectionner une entrée dans le tableau Trail Flow.

   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) **.



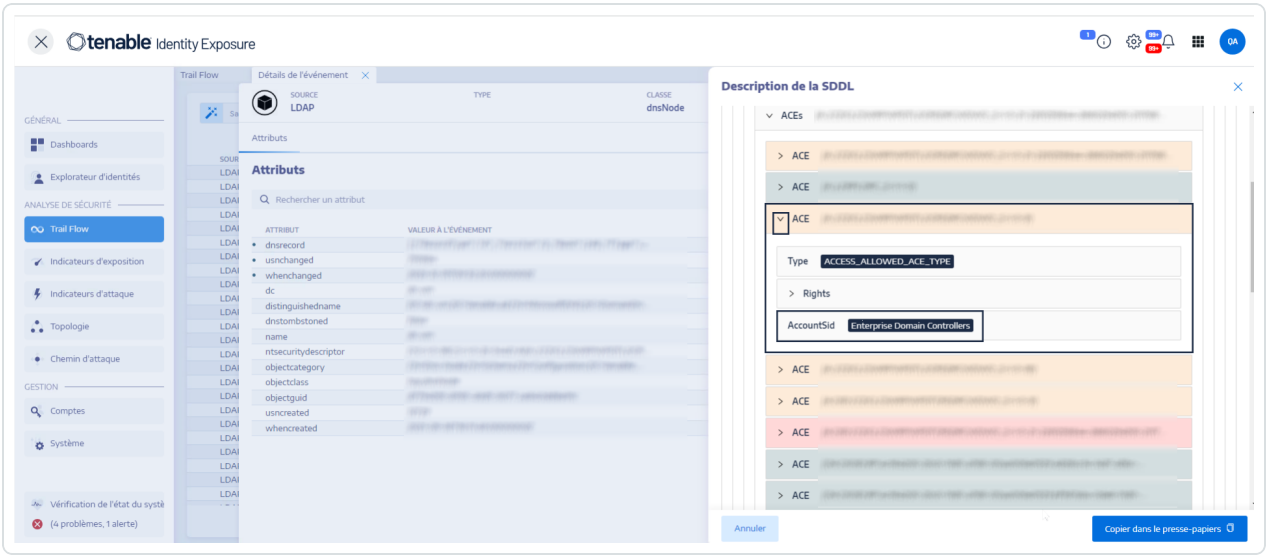
4. Cliquez sur **Voir la description de la SDDL**.

   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

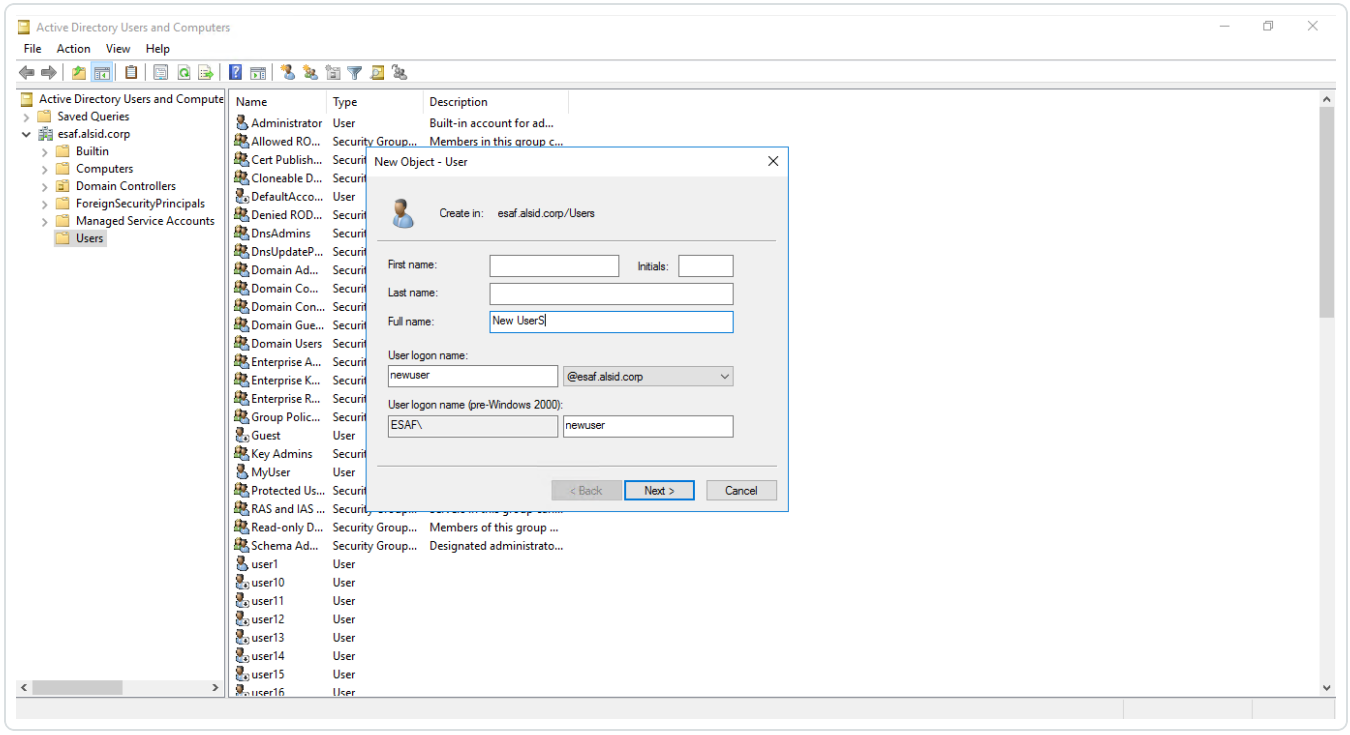
Pour comprendre le comportement du Trail Flow, deux exemples montrent comment une opération que vous effectuez dans votre interface Active Directory (AD) est répercutée dans la page Trail Flow.

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.

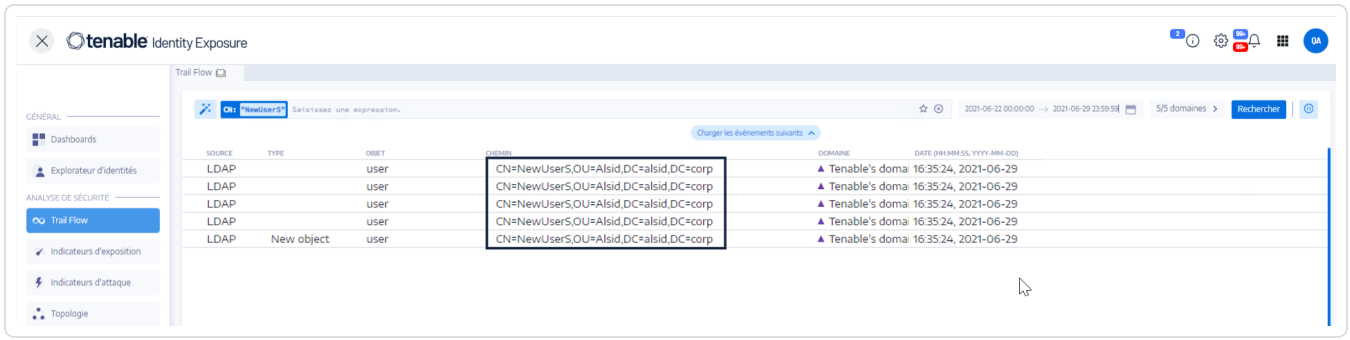
Remarque : ces exemples ne sont pas exhaustifs et ne peuvent couvrir toutes les situations possibles.

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.

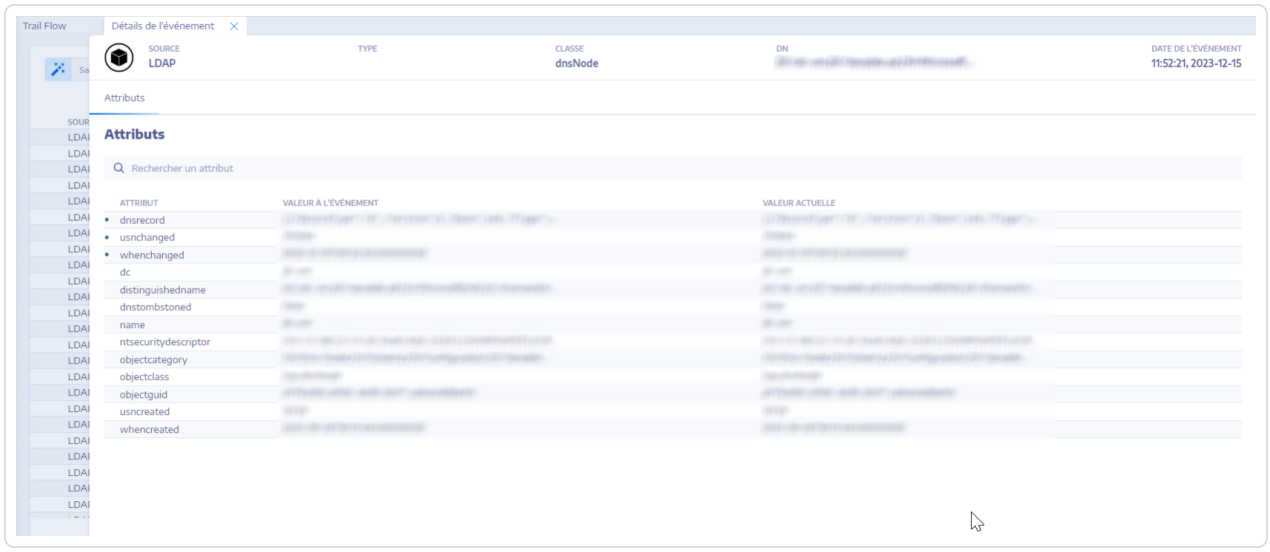


- Côté utilisateur final, Tenable Identity Exposure met à jour la page **Trail Flow**. Consultez la colonne **Type** indiquant *Nouvel objet*.



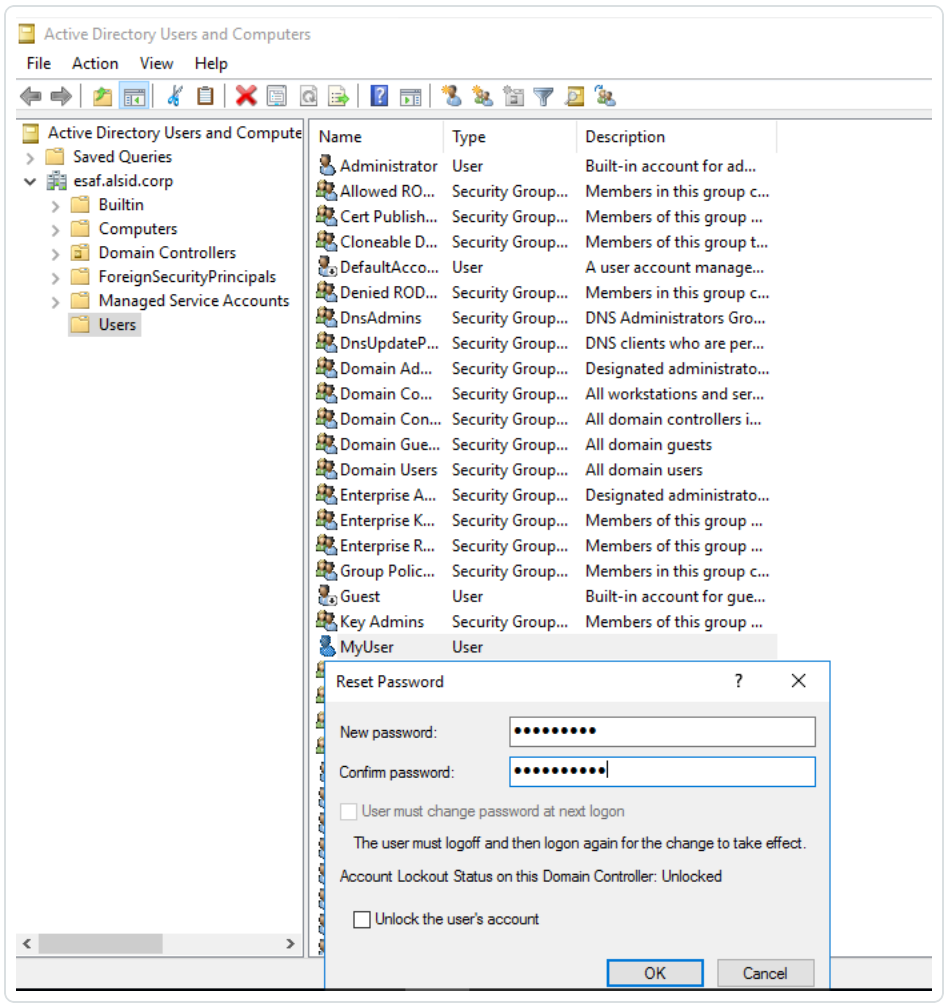
- La page **Détails de l'événement** reflète également ce changement. Le point bleu à gauche des noms d'attributs indique qu'une modification a eu lieu.

  Pour plus de détails sur les attributs, voir Détails d'un événement.

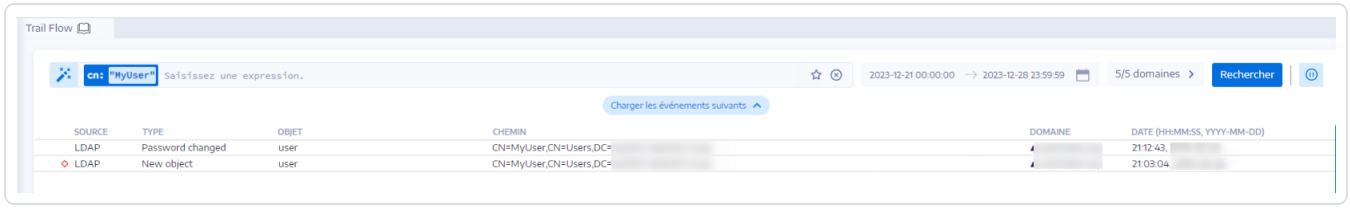


Que se passe-t-il dans le Trail Flow lorsque vous modifiez le mot de passe d'un utilisateur AD ?

- Côté administrateur, vous saisissez diverses informations pour réinitialiser le mot de passe d'un utilisateur.

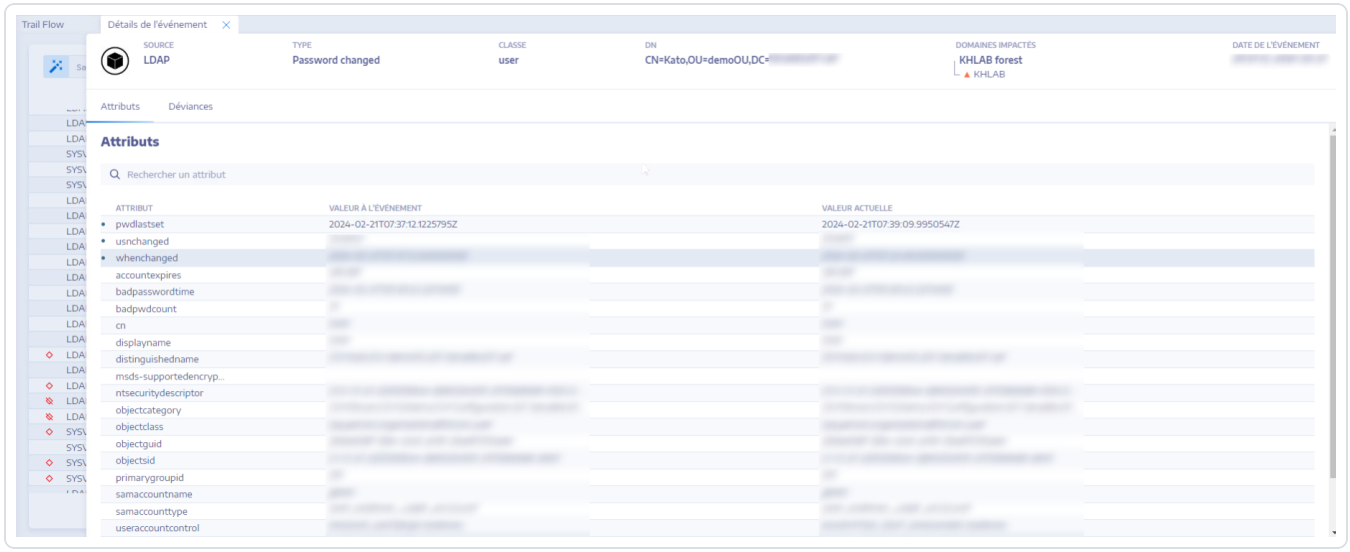


- Côté utilisateur final, Tenable Identity Exposure met à jour la page **Trail Flow**. Consultez la colonne **Type** indiquant « Mot de passe mis à jour ».



- 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

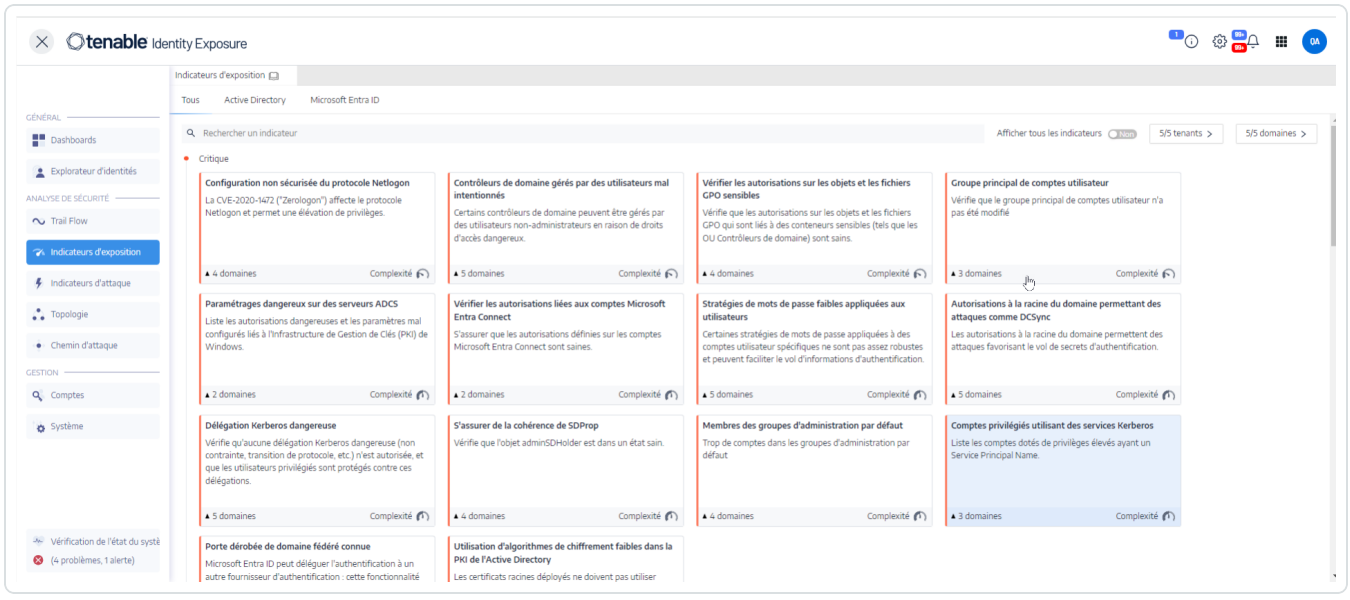
Tenable Identity Exposure mesure la maturité de la sécurité de vos infrastructures AD par le biais d'indicateurs d'exposition (IoE) et attribue des niveaux de sévérité au flux d'événements qu'il surveille et analyse. Tenable Identity Exposure déclenche des alertes lorsqu'il détecte des régressions de 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**.



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.

Voir aussi

- Détails d'un indicateur d'exposition
- Objets déviants
- Rechercher des objets déviants
- Ignorer un objet déviant
- 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
- 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.

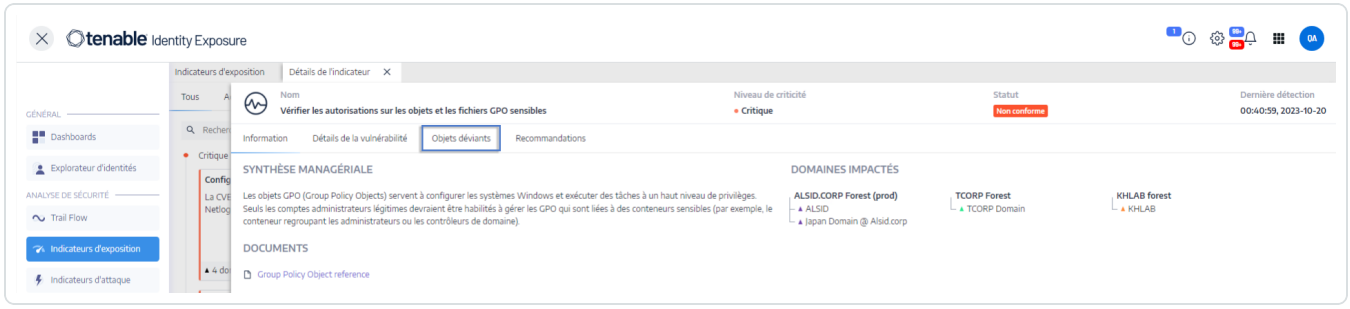
Pour afficher des objets déviants :

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.

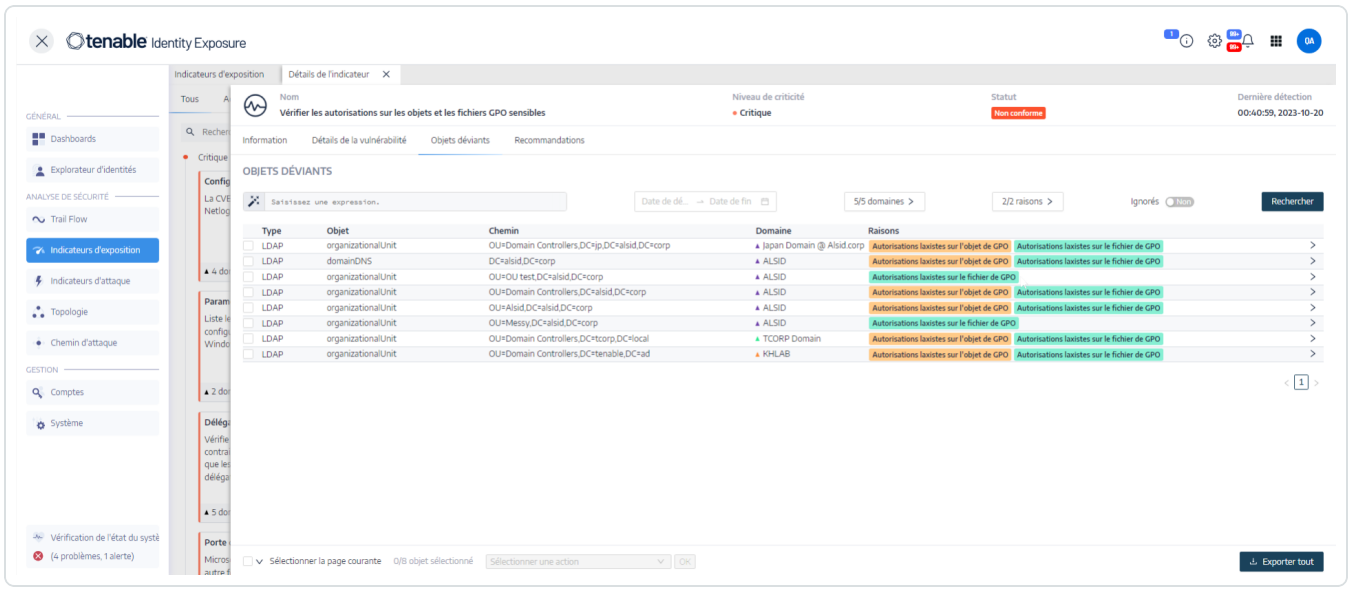
2. Cliquez sur une tuile d'**Indicateur d'exposition** sur la page.

   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
- Attributs incriminants

Rechercher des objets déviants

Vous pouvez rechercher les objets déviants manuellement ou à l'aide de l'assistant.

Recherche via l'assistant

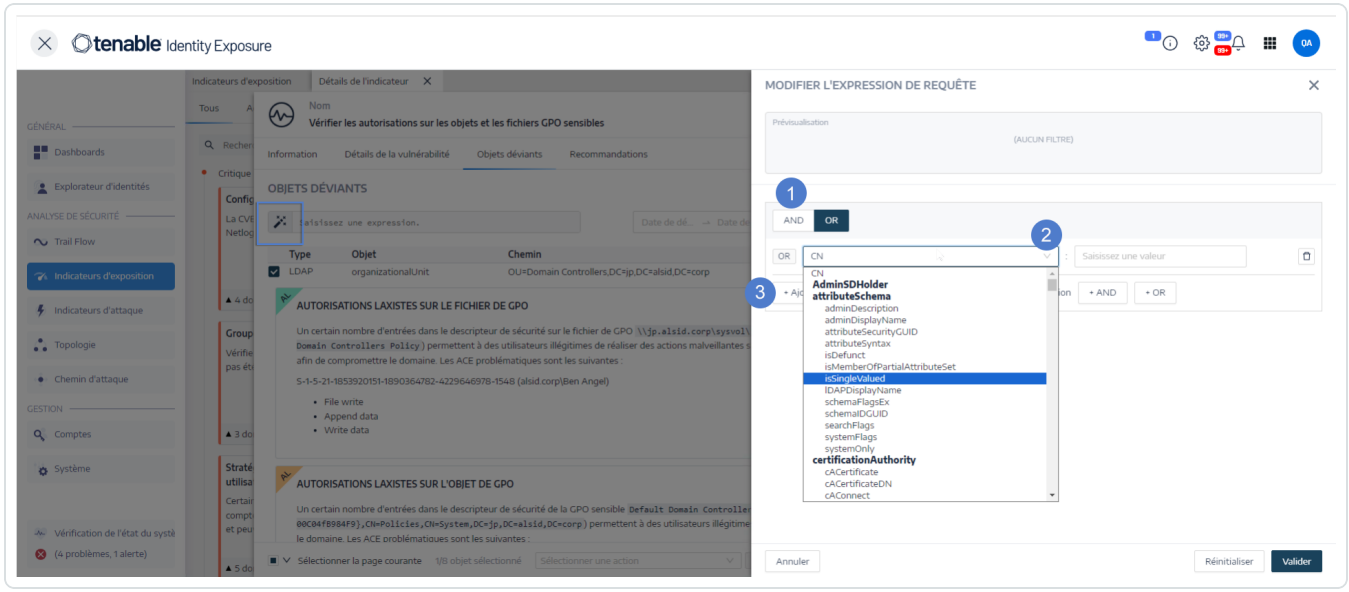
L'assistant de recherche permet de créer des expressions de requête.

- 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 🗑.

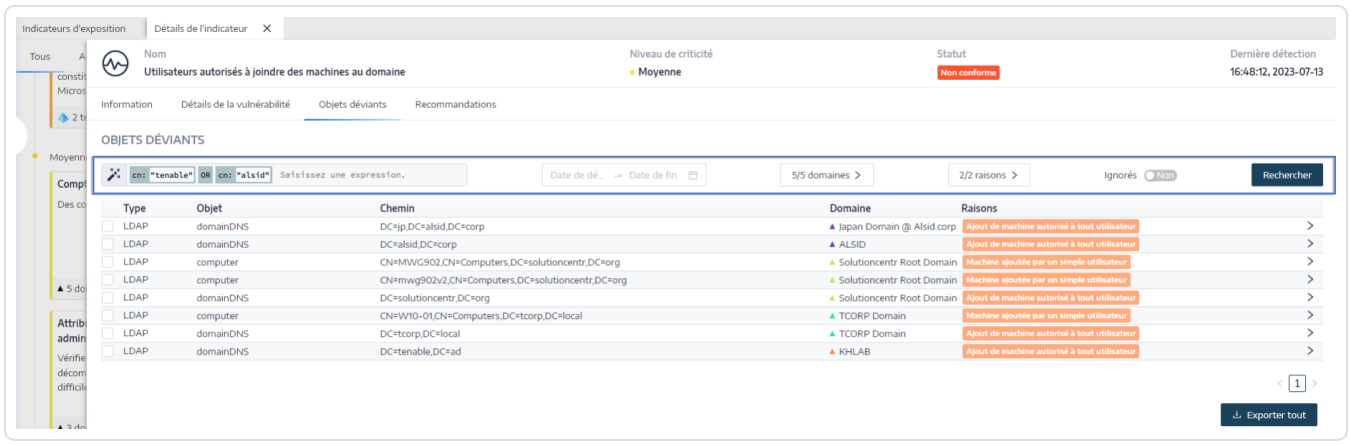
6. Cliquez sur **Valider** pour lancer la recherche ou sur **Réinitialiser** pour modifier les expressions de requête.

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__`

  où :
    - `__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" and 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
- Attributs incriminants

Ignorer un objet déviant

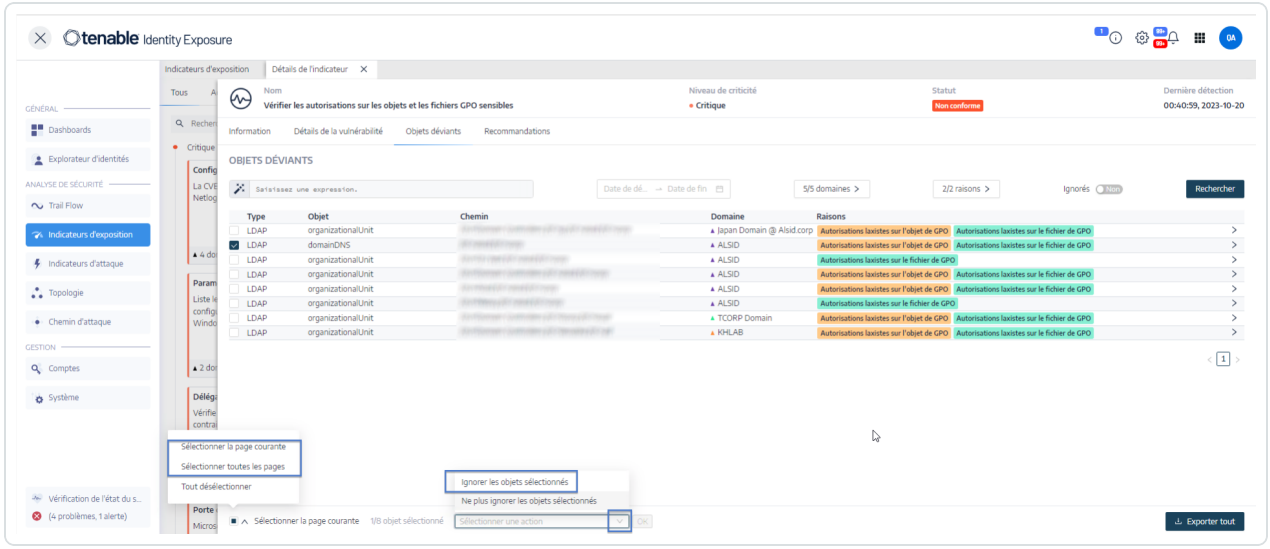
Pour éviter d'encombrer l'écran au cours d'une investigation ou de la création d'un rapport, vous pouvez filtrer certains objets déviants en forçant Tenable Identity Exposure à les ignorer sur une période donnée. Vous pouvez choisir d'ignorer un ou plusieurs objets déviants. Vous pouvez appliquer un filtre personnalisé immédiatement ou spécifier la période sur laquelle activer le filtre.

Remarque : ignorer un objet ne le résout pas dans Tenable Identity Exposure.

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.

Voir aussi

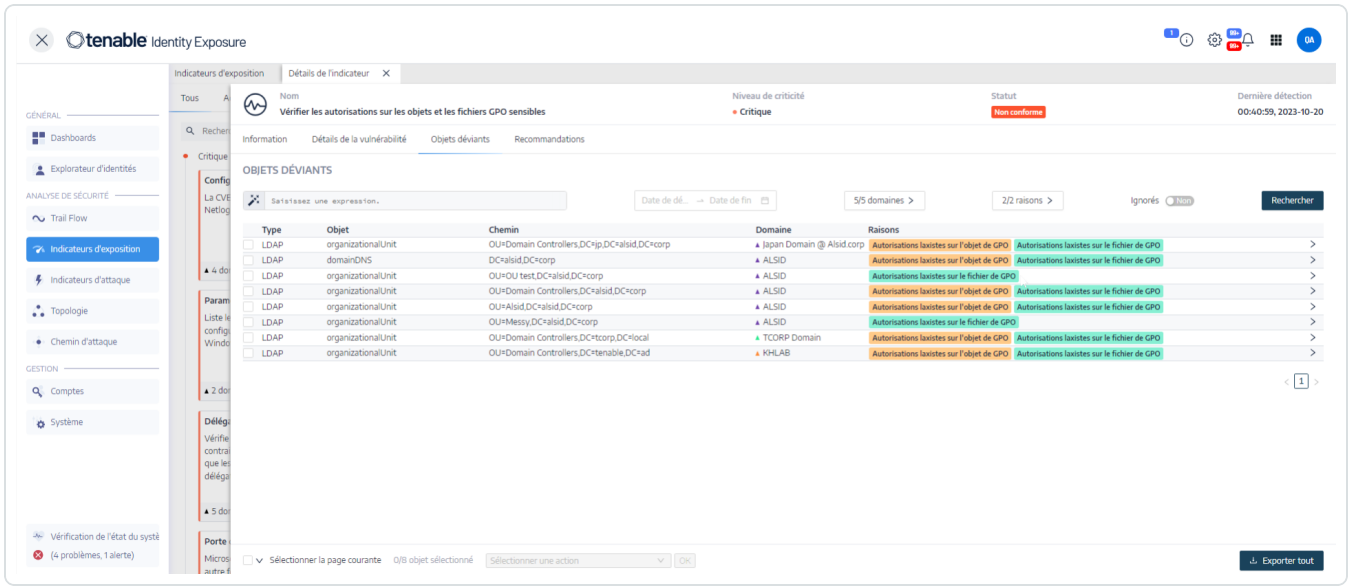
- Indicateurs d'exposition
- Détails d'un indicateur d'exposition
- Objets déviants
- Rechercher des objets déviants
- Attributs incriminants

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.

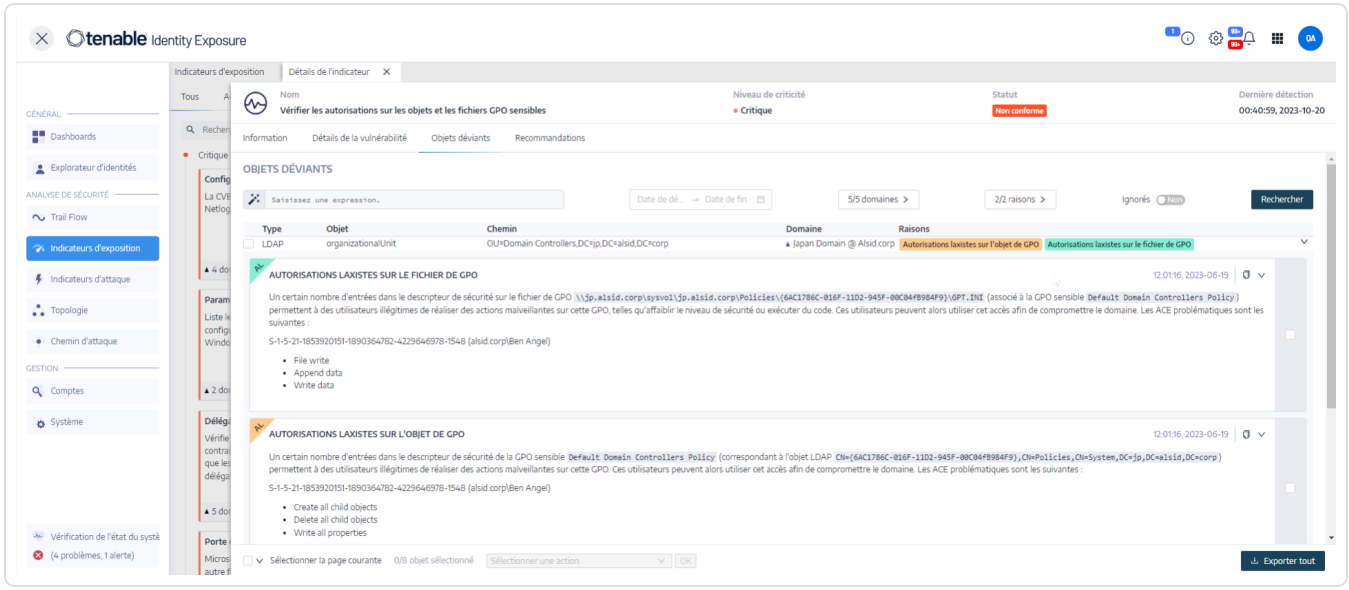
Pour afficher les attributs incriminants :

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

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
- Application de stratégies de mot de passe faible 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.

Indicateurs d'exposition liés à Microsoft Entra ID

Indicateurs d'exposition spécifiques à Microsoft Entra ID

Tenable Identity Exposure dispose d'indicateurs d'exposition (IoE) dédiés qui envoient des alertes relatives aux vulnérabilités potentielles des assets dans Microsoft Entra ID.

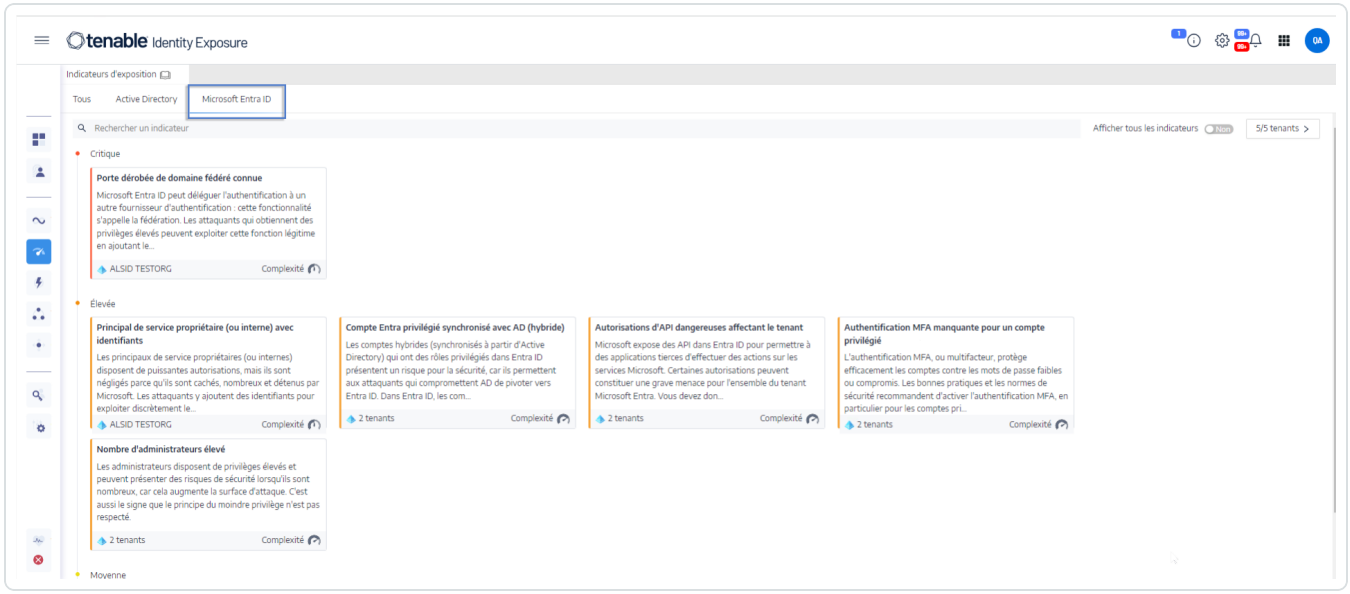
Pour afficher les IoE Microsoft Entra ID :

1. Dans Tenable Identity Exposure, cliquez sur l'icône IoE dans la barre de navigation de gauche.

   Le volet IoE apparaît.

2. Cliquez sur l'onglet **Microsoft Entra ID**.

   Tenable Identity Exposure montre les IoE liés à Microsoft Entra ID qui ont déclenché des détections.



3. Cliquez sur la tuile contenant l'IoE à analyser.
4. Le volet Détails de l'indicateur apparaît avec les informations suivantes :
   - **Informations sur les vulnérabilités** : comment l'exposition à une attaque potentielle peut se produire.

- **Détections** : détails sur le type de fournisseur d'identité et description du risque.
- **Recommandations** : étapes pour remédier à la menace.

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.

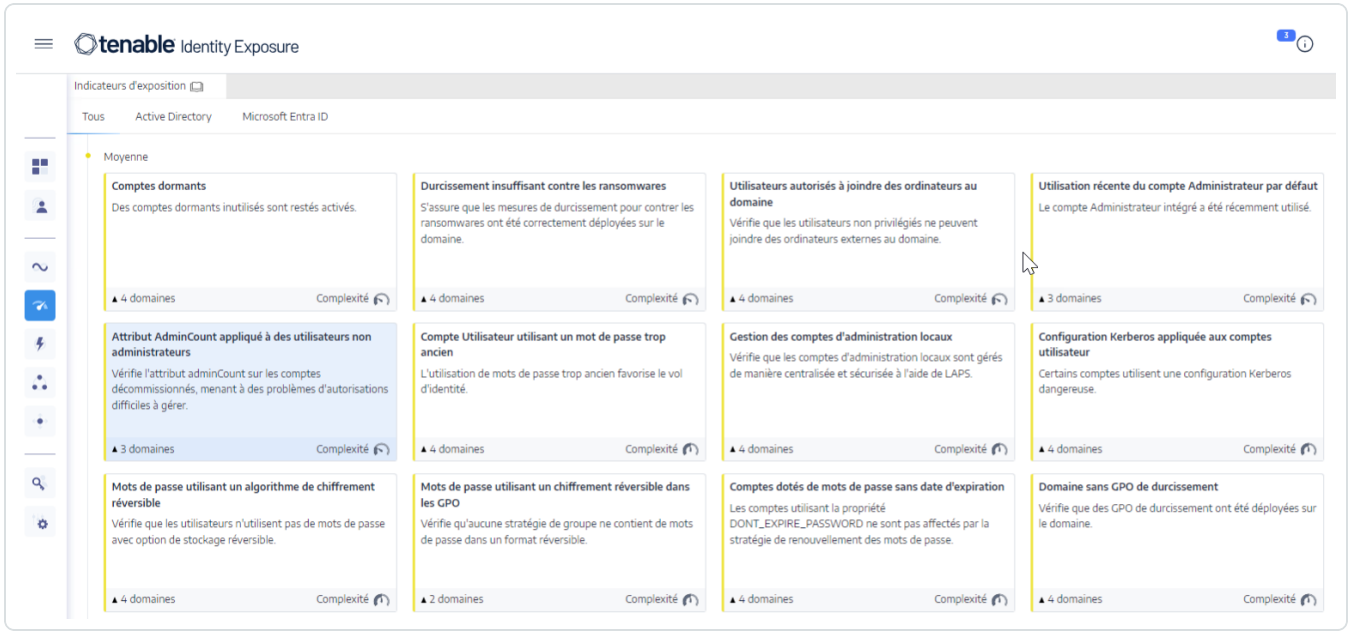
Cet IoE de niveau moyen ne signale que les comptes utilisateur et les groupes actifs avec cet attribut et exclut les groupes privilégiés avec des membres légitimes dont l'attribut `adminCount` est défini sur `1`.

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.

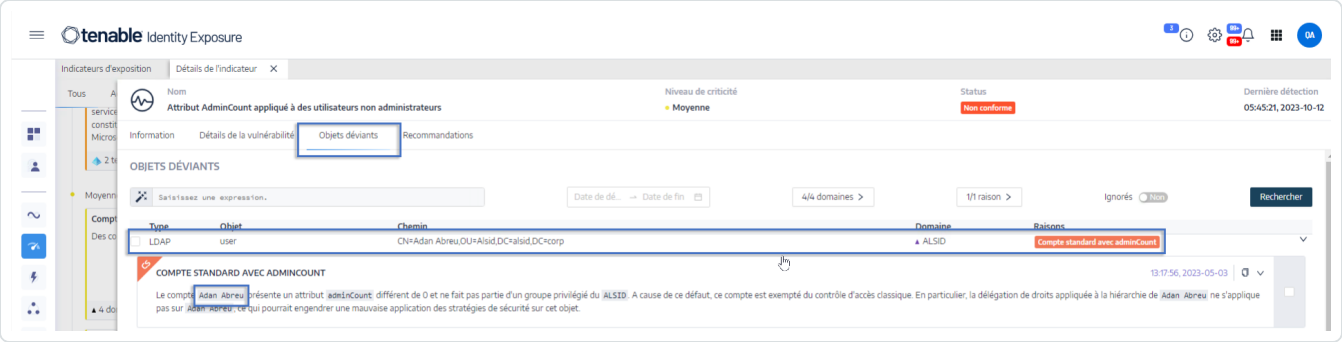
   Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des objets déviants.

2. Cliquez sur la tuile de l'IoE **Attribut adminCount appliqué à des utilisateurs non administrateurs**.



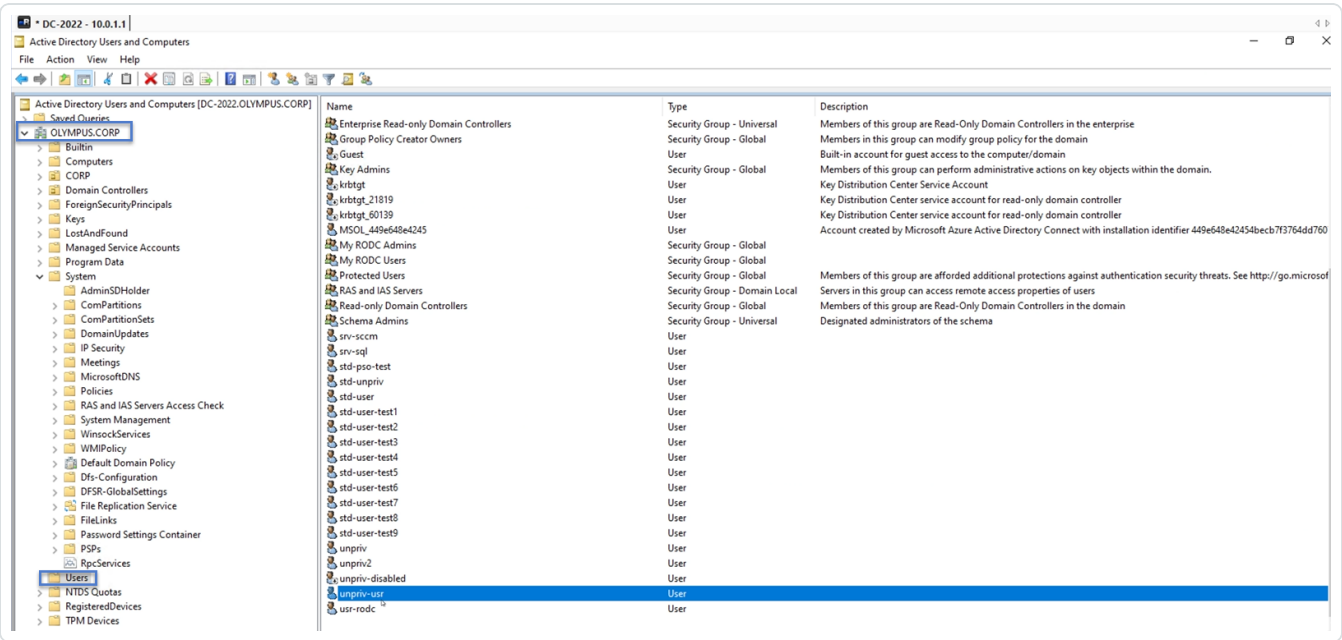
Le volet **Détails de l'indicateur** apparaît.

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`)



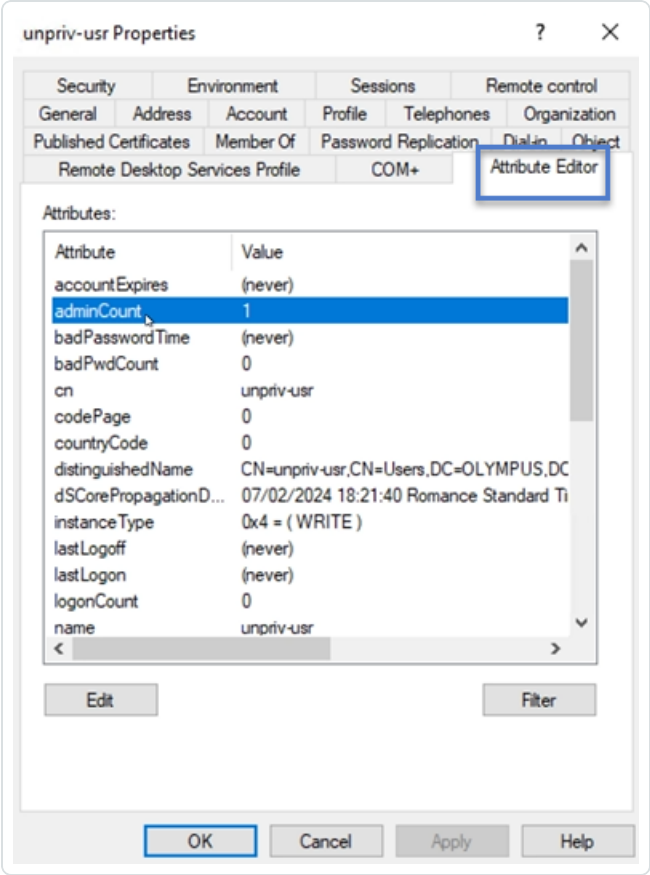
4. Dans le gestionnaire de bureau à distance (ou un outil similaire), localisez le nom de domaine et accédez aux **utilisateurs** ainsi qu'au compte signalé par Tenable Identity Exposure.

> **Autorisation requise** : vous devez disposer d'un compte administrateur sur le domaine pour effectuer la procédure.

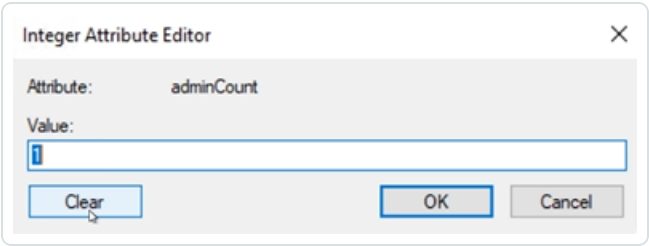


5. Cliquez sur le nom du compte pour ouvrir la boîte de dialogue **Propriétés** et sélectionnez l'onglet **Éditeur d'attributs**.

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.

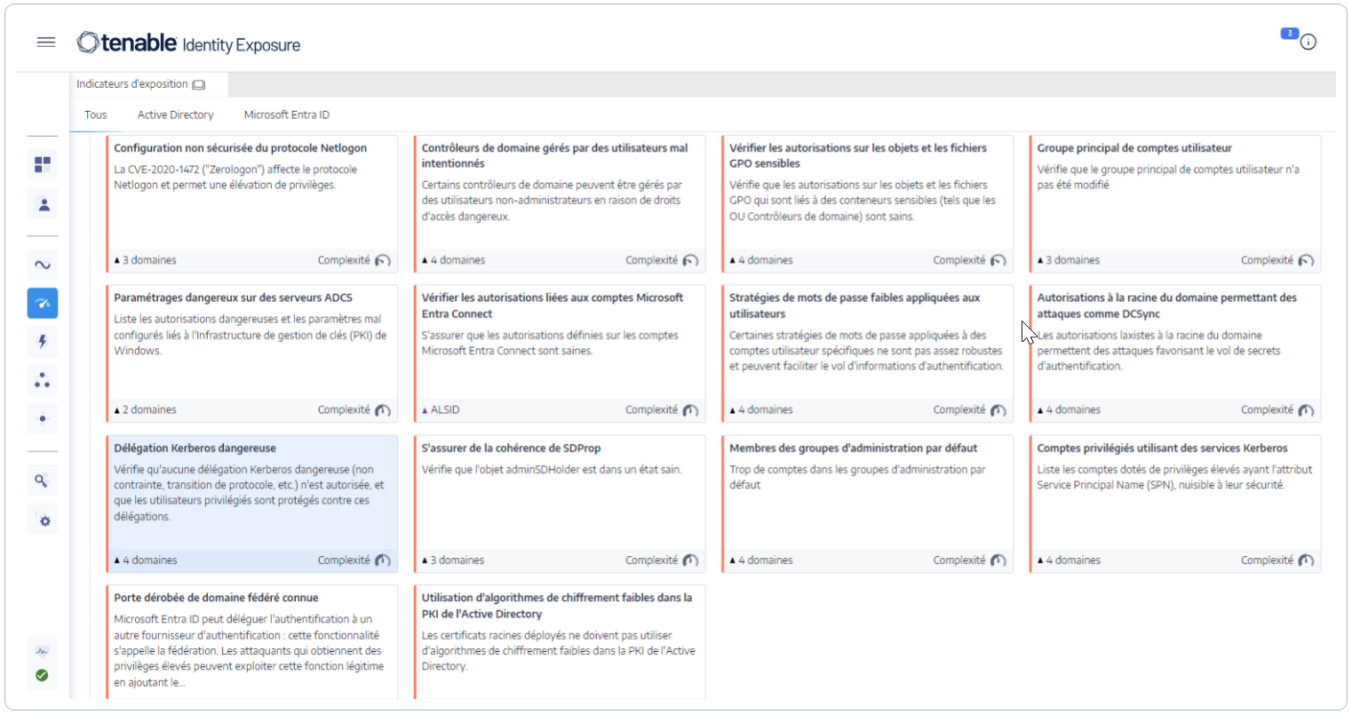
Cet IoE de niveau critique signale tous les comptes avec des attributs de délégation et exclut les comptes désactivés. Les utilisateurs privilégiés ne devraient pas avoir d'attributs de délégation. Pour protéger ces comptes utilisateur, ajoutez-les au groupe « Protected Users » ou marquez-les comme « 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.

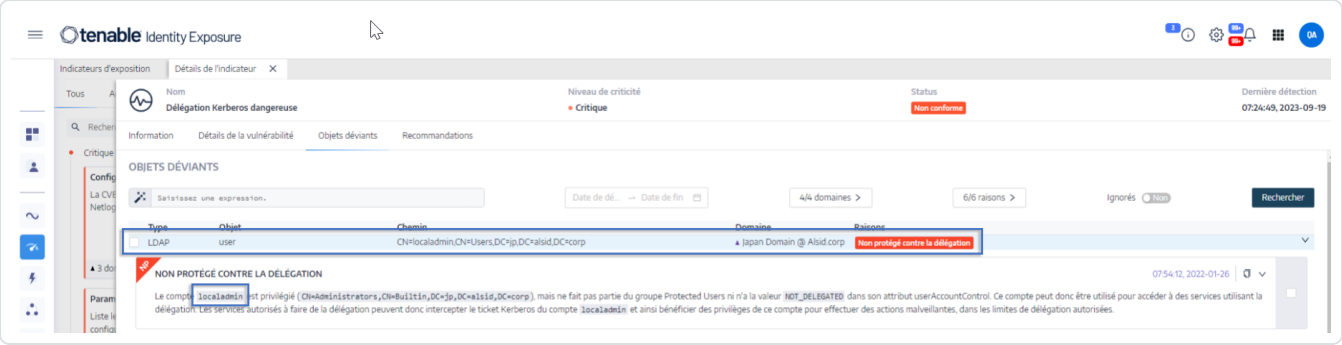
   Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des objets déviants.

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`)

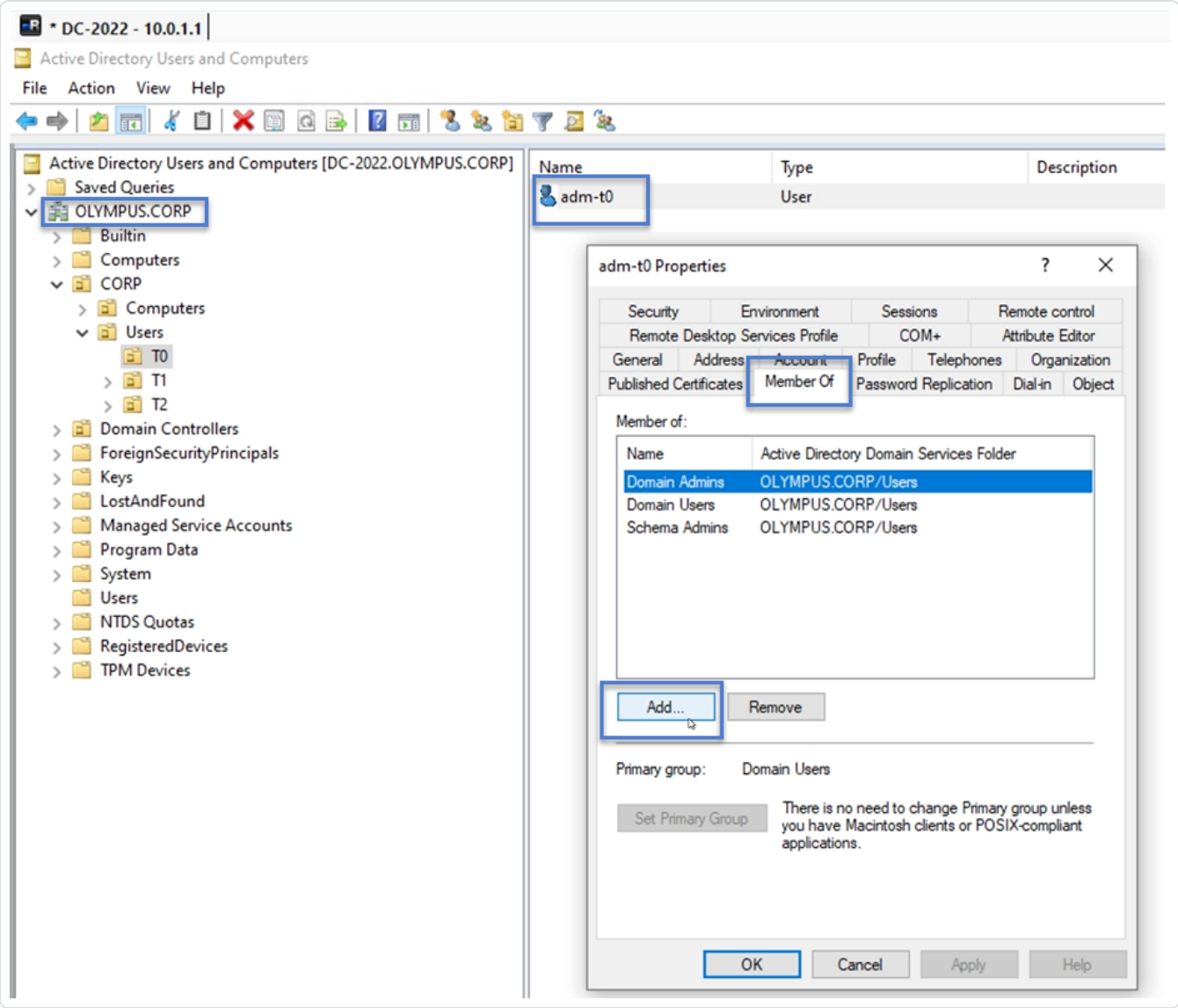


4. Dans le gestionnaire de bureau à distance (ou un outil similaire), localisez le nom de domaine et accédez au domaine et au compte signalés par Tenable Identity Exposure.

> **Autorisation requise** : vous devez disposer d'un compte administrateur sur le domaine pour effectuer la procédure.

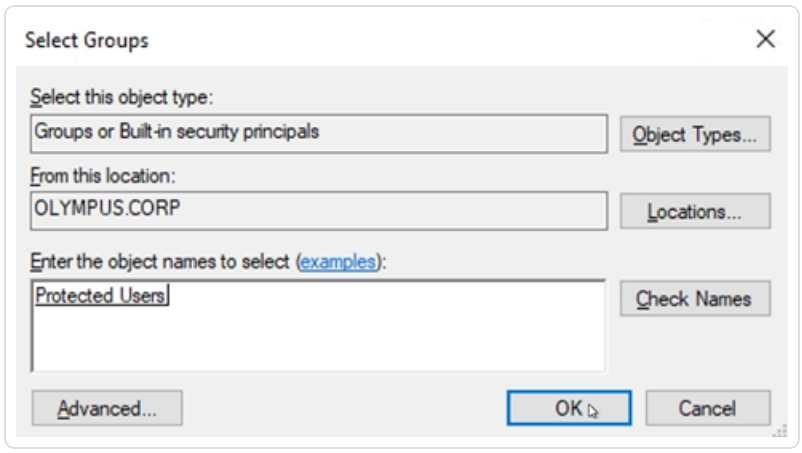
5. Cliquez sur le nom du compte pour ouvrir la boîte de dialogue **Propriétés** et sélectionnez l'onglet **Membre de**.

6. Dans la liste des membres, cliquez sur **Ajouter**.



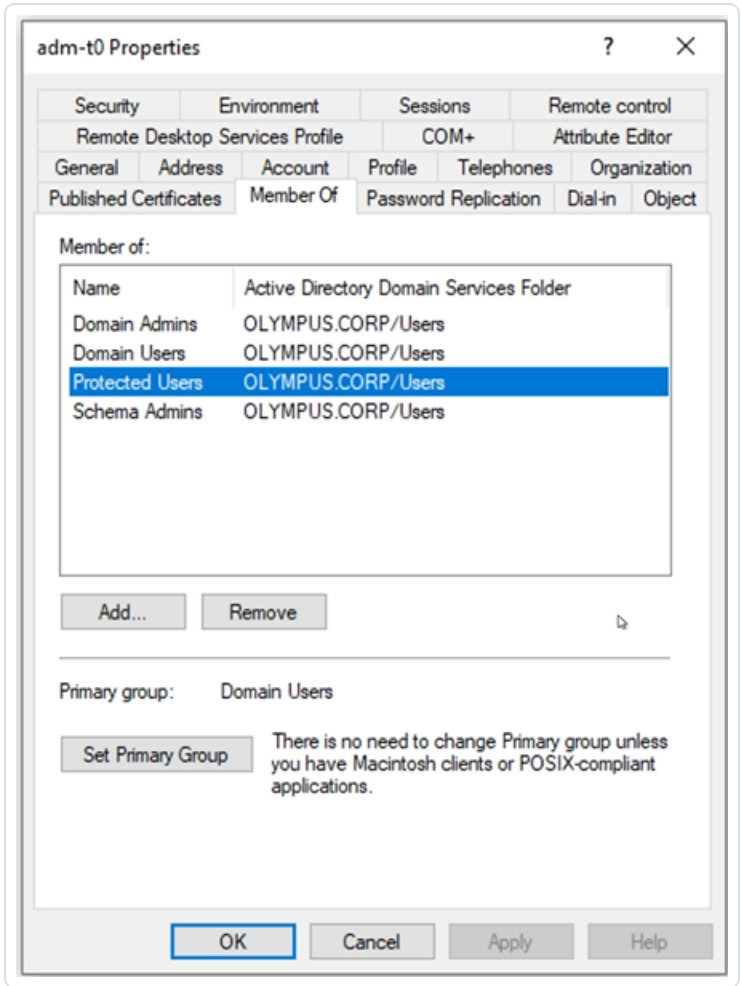
La boîte de dialogue **Sélectionner des groupes** apparaît.

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.

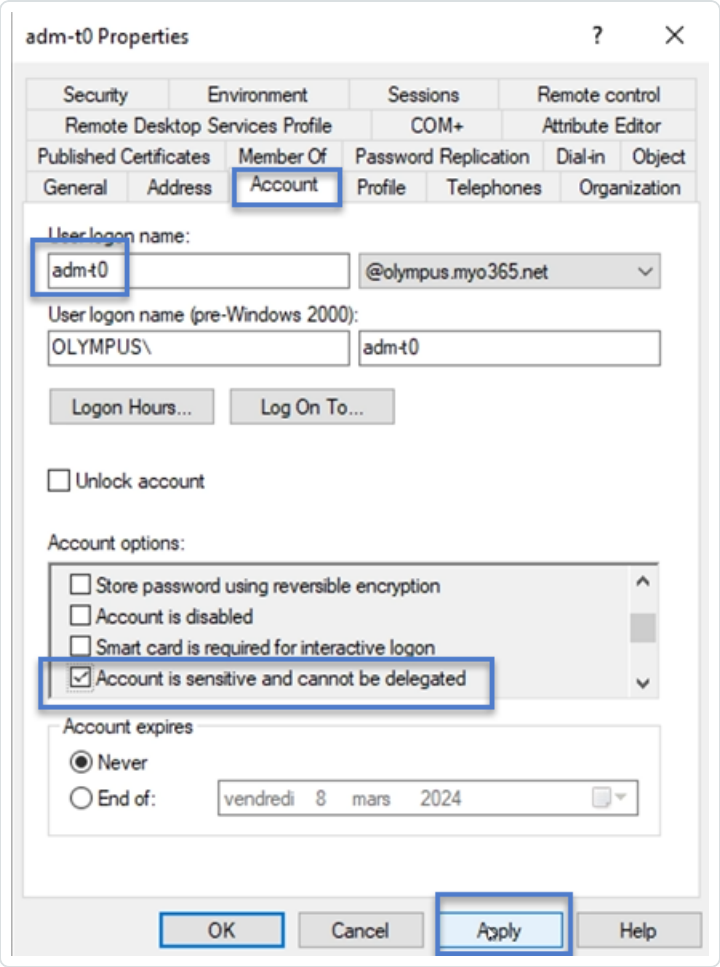
    L'objet déviant n'apparaît plus dans la liste.

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.

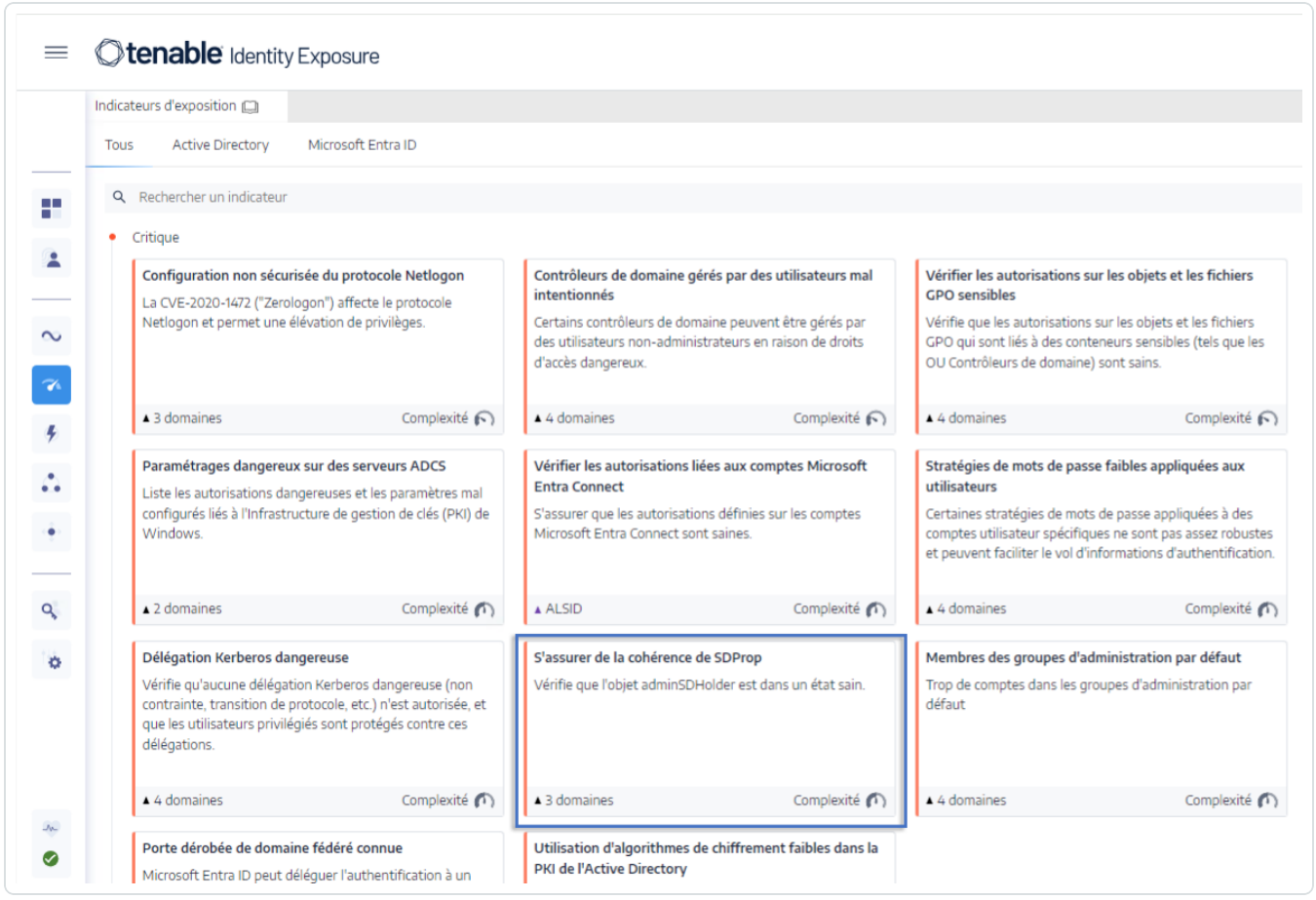
Cet IoE de niveau critique vérifie que les autorisations définies sur l'objet `adminSDHolder` autorisent uniquement un accès privilégié aux comptes administratifs.

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.

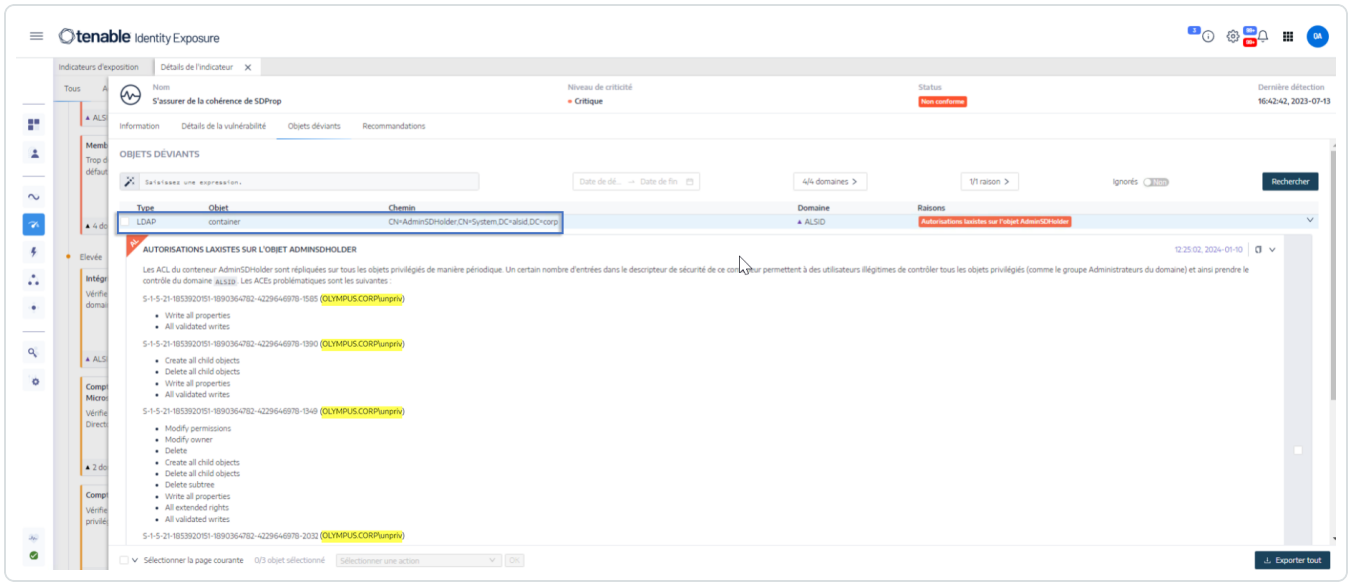
   Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des objets déviants.

2. Cliquez sur la tuile de l'IoE **S'assurer de la cohérence de SDProp**.



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

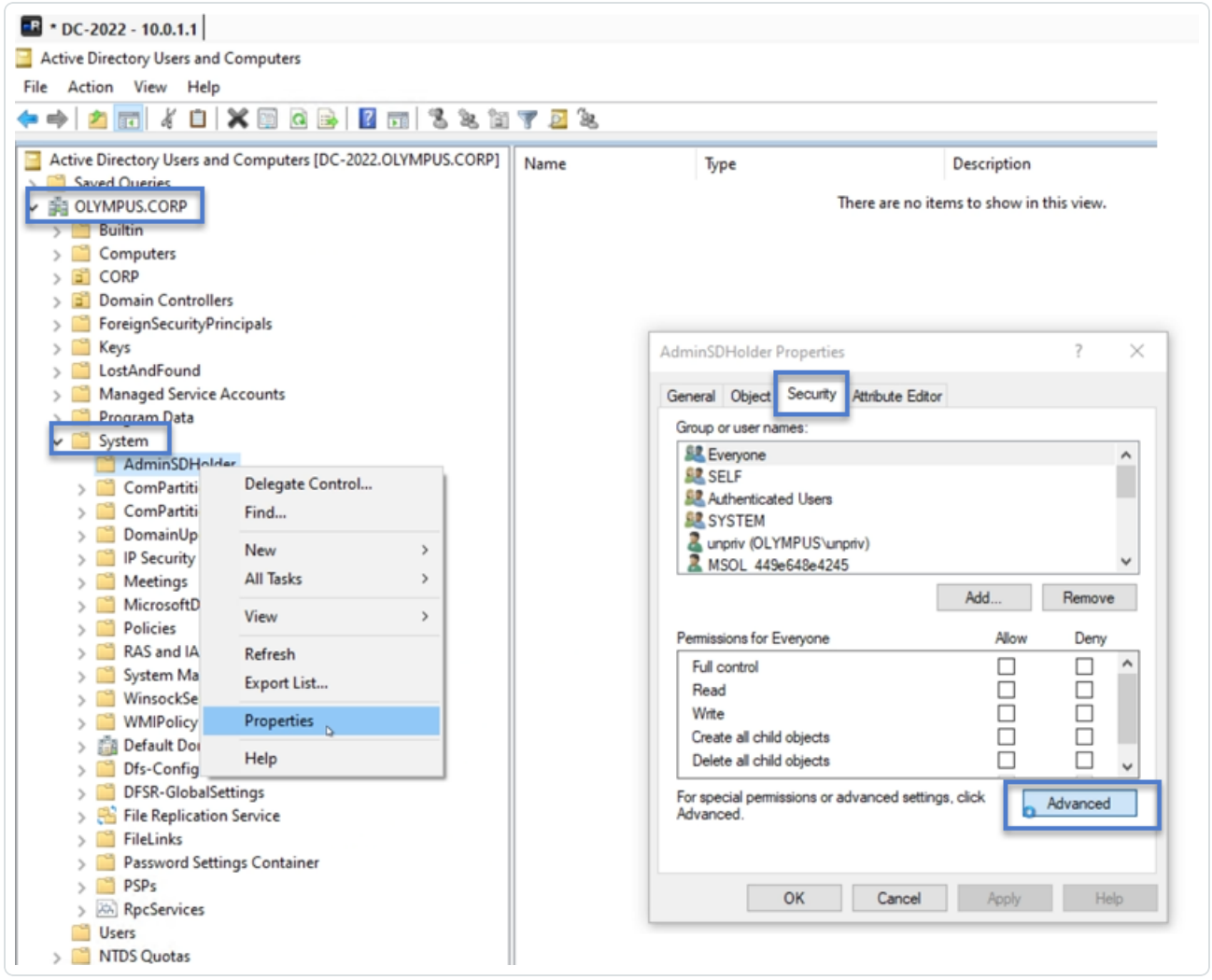
3. Survolez l'objet déviant et cliquez dessus pour afficher ses détails. Notez le nom de domaine et l'autorisation associée signalés par Tenable Identity Exposure (dans cet exemple : `OLYMPUS.CORP .\unpriv`).



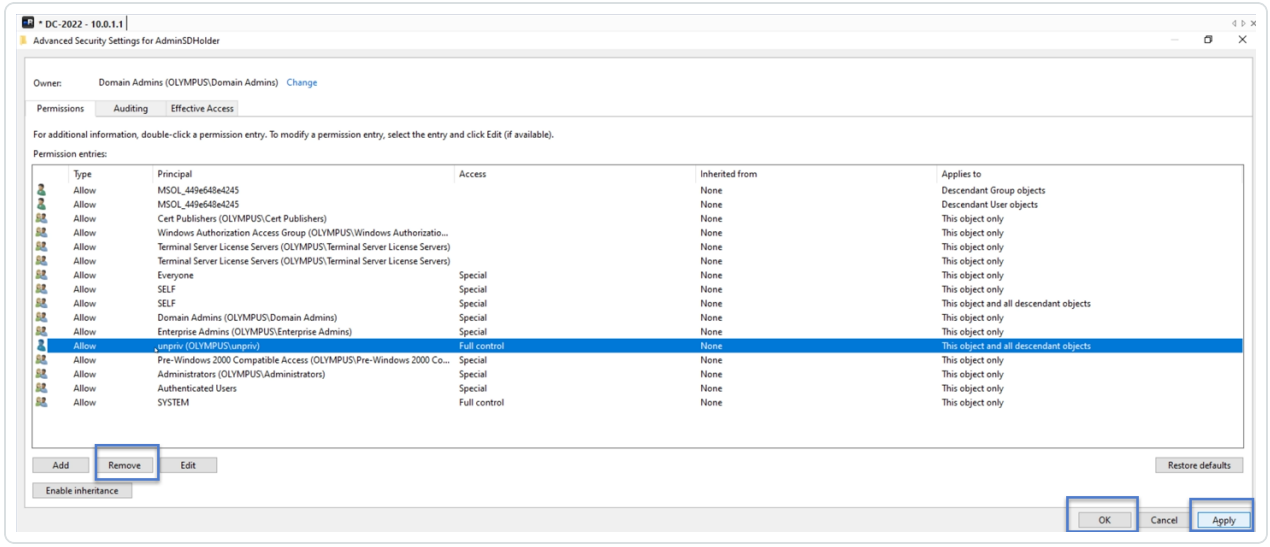
4. Dans le gestionnaire de bureau à distance (ou un outil similaire), localisez le nom de domaine et accédez à **Système** > **AdminSDHolder**.

> **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.

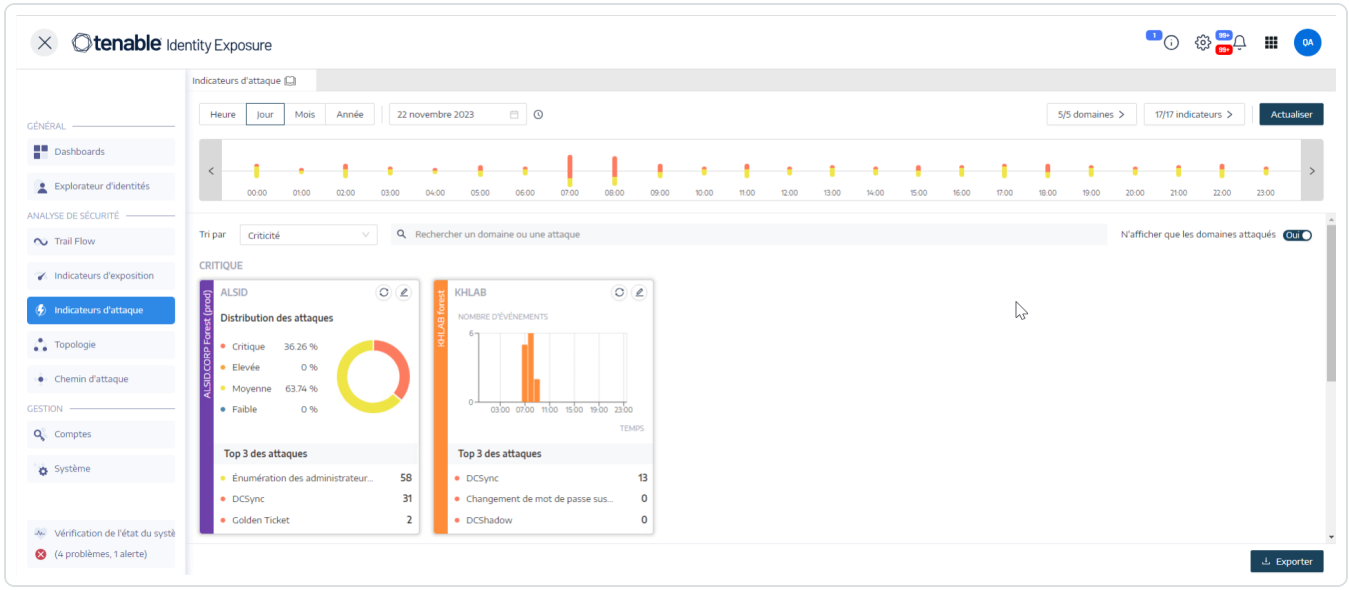
Pour plus d'informations sur des IoA spécifiques, consultez Indicators of Attack and the Active Directory.

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 –	Alertes sur les comportements suspects liés aux actions de reconnaissance ou

Bleu	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.

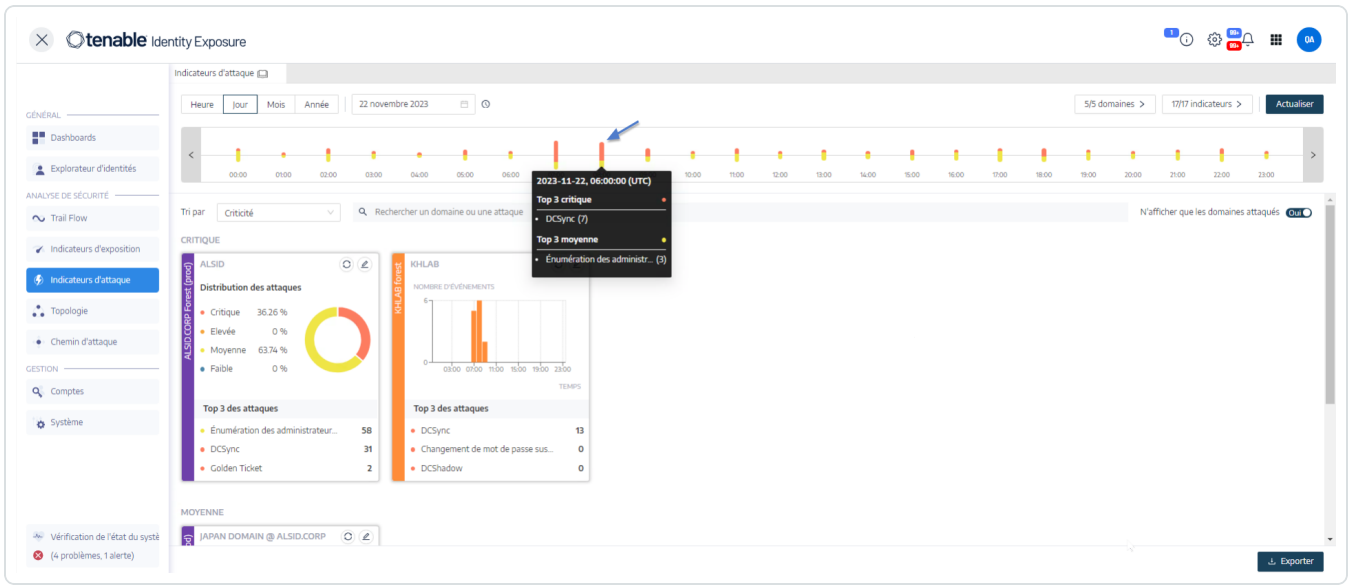
Pour afficher les indicateurs d'attaque :

- 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.



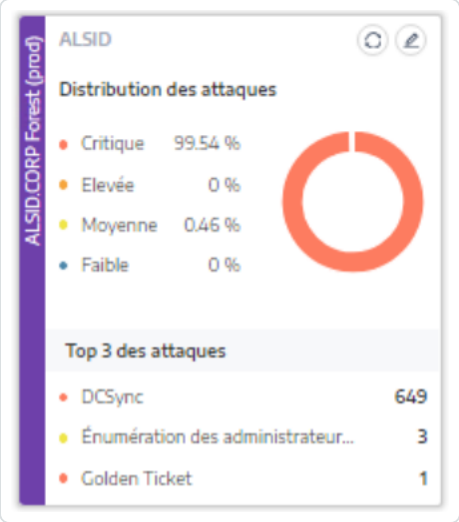
Pour modifier le type de graphique :

1. Cliquez sur l'icône ✎ pour modifier la tuile de domaine.

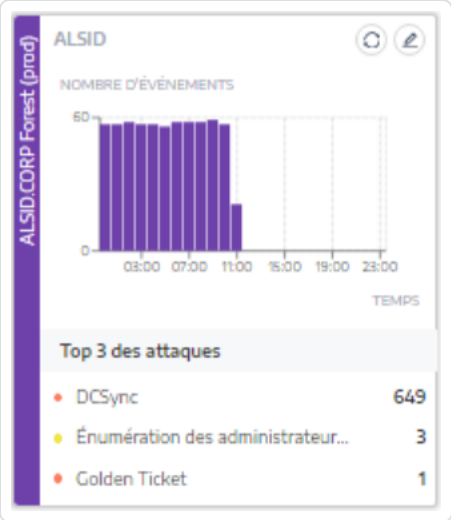
   Le volet **Modifier les informations de la carte** apparaît.

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.

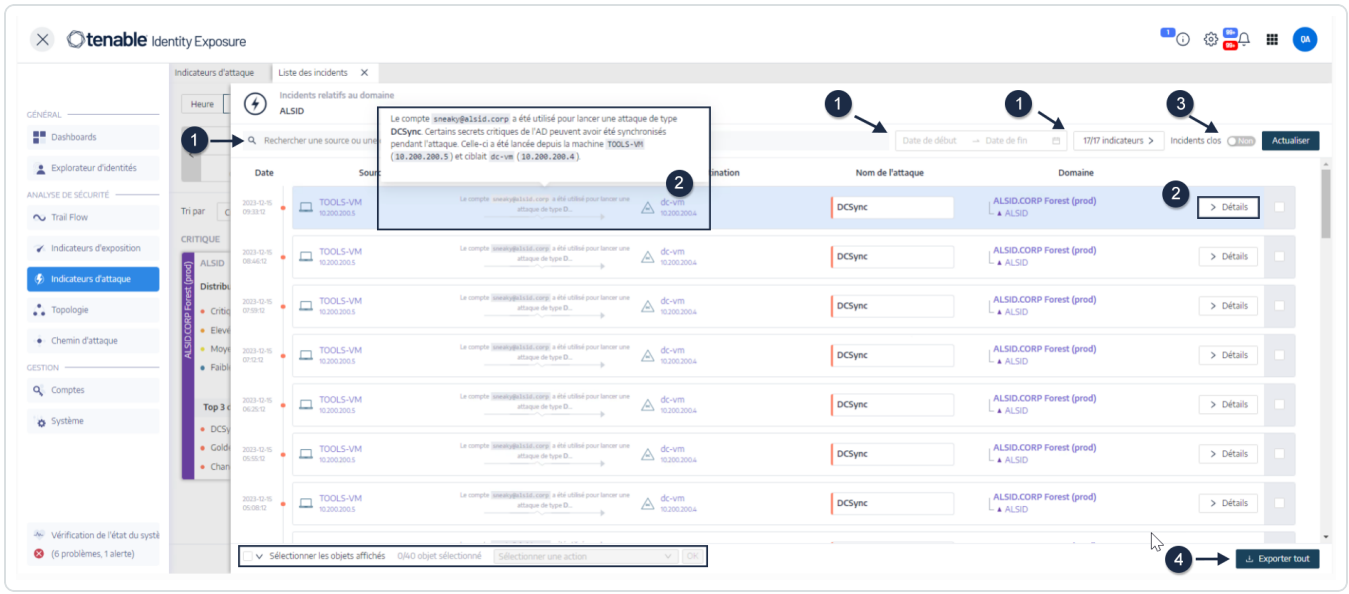
Pour afficher les incidents d'attaque :

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.



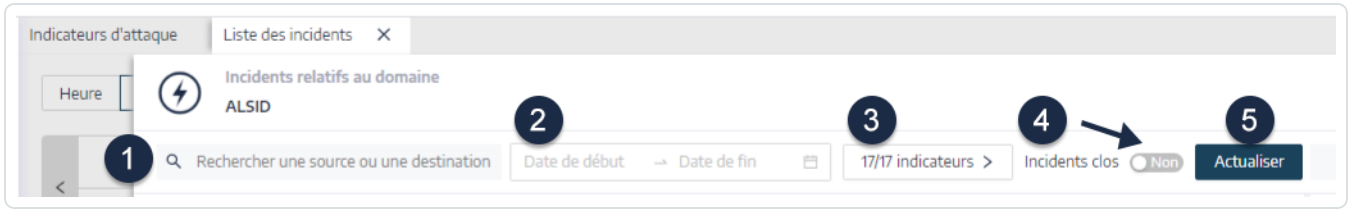
3. Dans cette liste, vous pouvez effectuer les actions suivantes :

   - Définir des critères de recherche pour rechercher des incidents spécifiques ❶ .
   - Accéder à des explications détaillées sur les attaques affectant l'infrastructure AD ❷ .
   - Fermer ou rouvrir un incident ❸ .
   - Télécharger un rapport montrant tous les incidents ❹ .

Pour rechercher un incident :

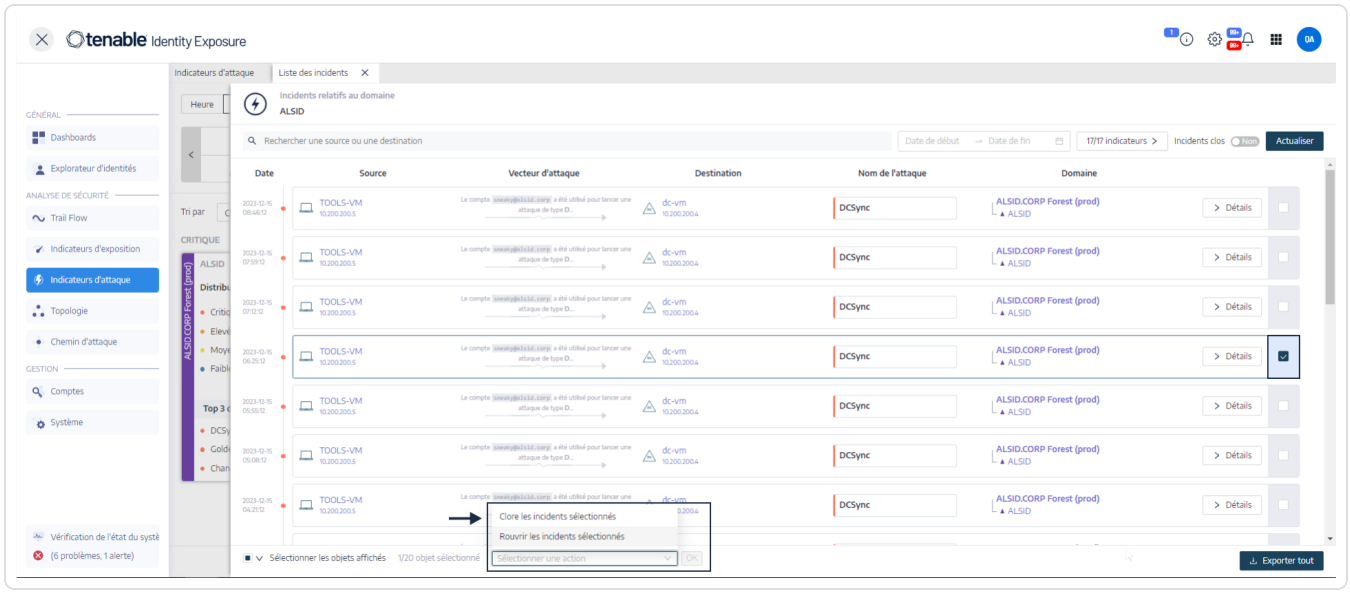
1. Dans la zone de **recherche**, saisissez le nom d'une source ou d'une destination.
2. Cliquez sur le sélecteur de date pour sélectionner les dates de début et de fin de l'incident.
3. Cliquez sur **n/n Indicateurs** pour sélectionner les indicateurs associés.
4. Cliquez sur le curseur **Incidents 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**.

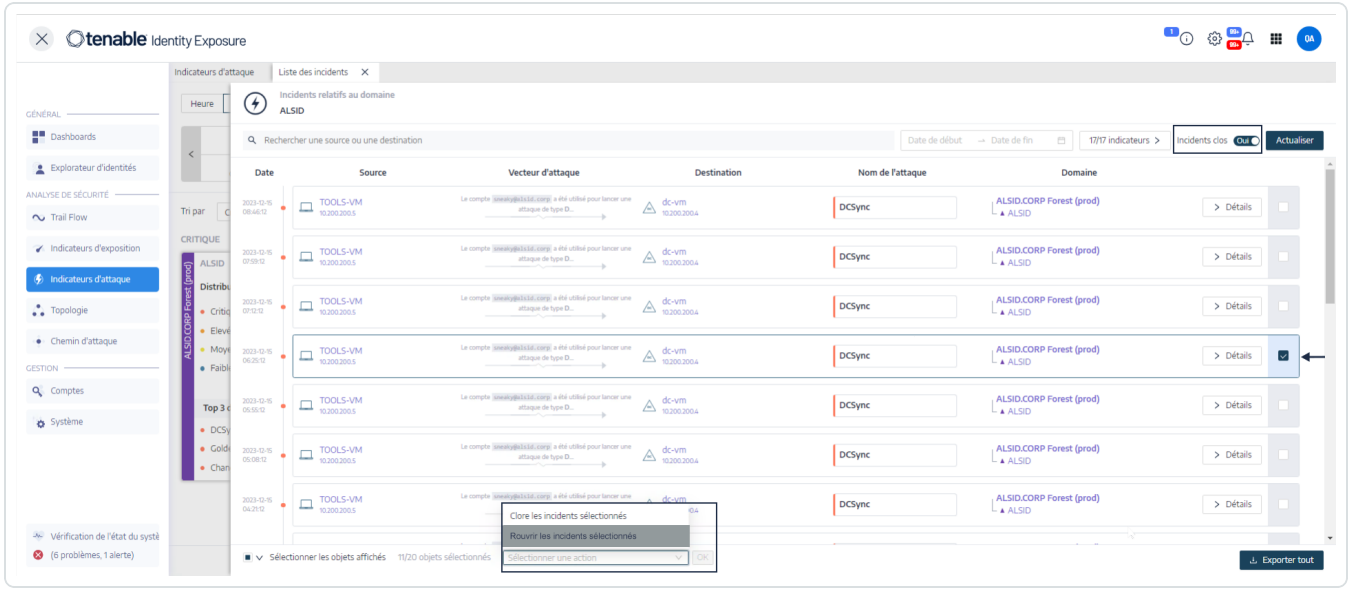
   Un message confirme que Tenable Identity Exposure a clos l'incident et ne l'affiche plus.

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**.

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.

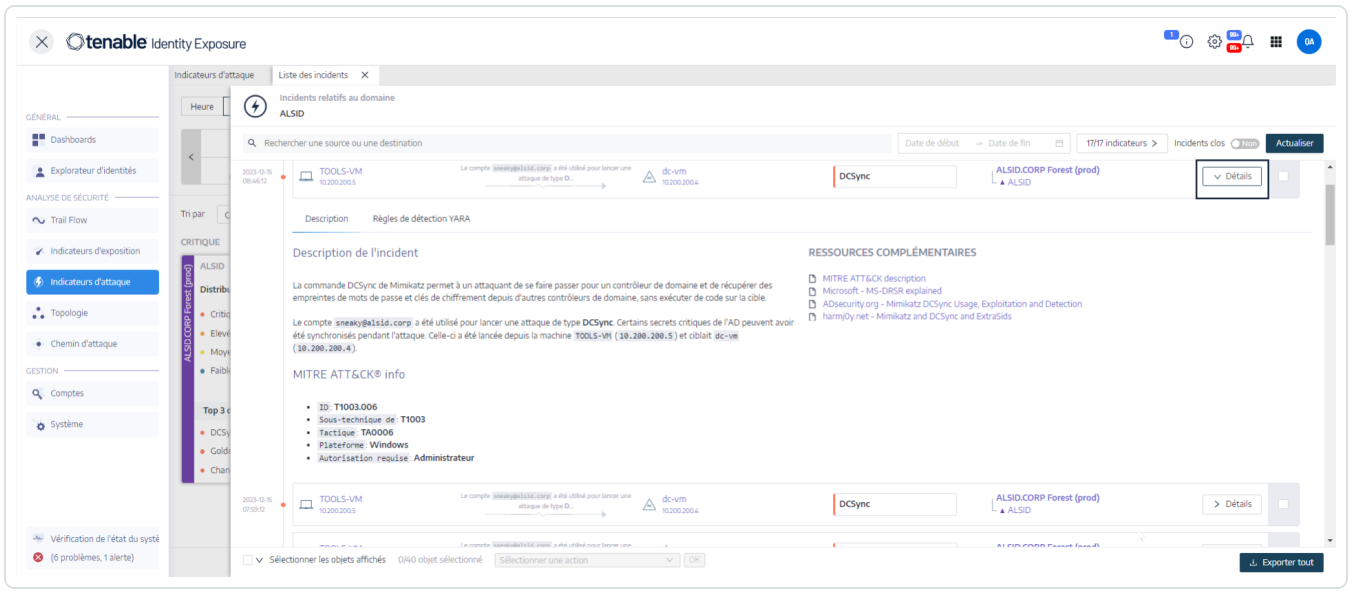
  > **Astuce** : Tenable Identity Exposure peut afficher un maximum de cinq volets lorsque vous cliquez sur plusieurs éléments interactifs (liens, boutons d'action, etc.) dans la **liste des incidents**. Pour fermer tous les volets simultanément, cliquez n'importe où sur la page.

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.

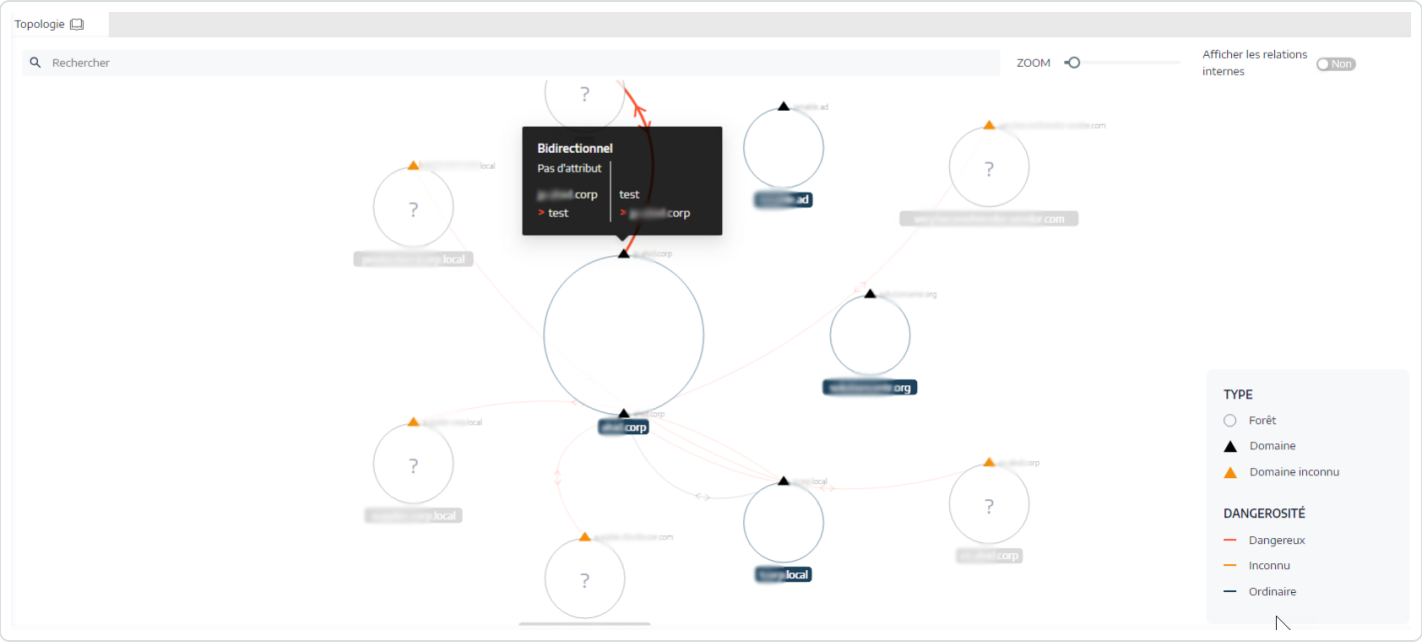
Remarque : YARA est le nom d'un outil principalement utilisé dans la recherche et la détection des logiciels malveillants. Il s'appuie sur des règles pour créer des descriptions de familles de logiciels malveillants sur la base de modèles textuels ou binaires. Une description est essentiellement un nom 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

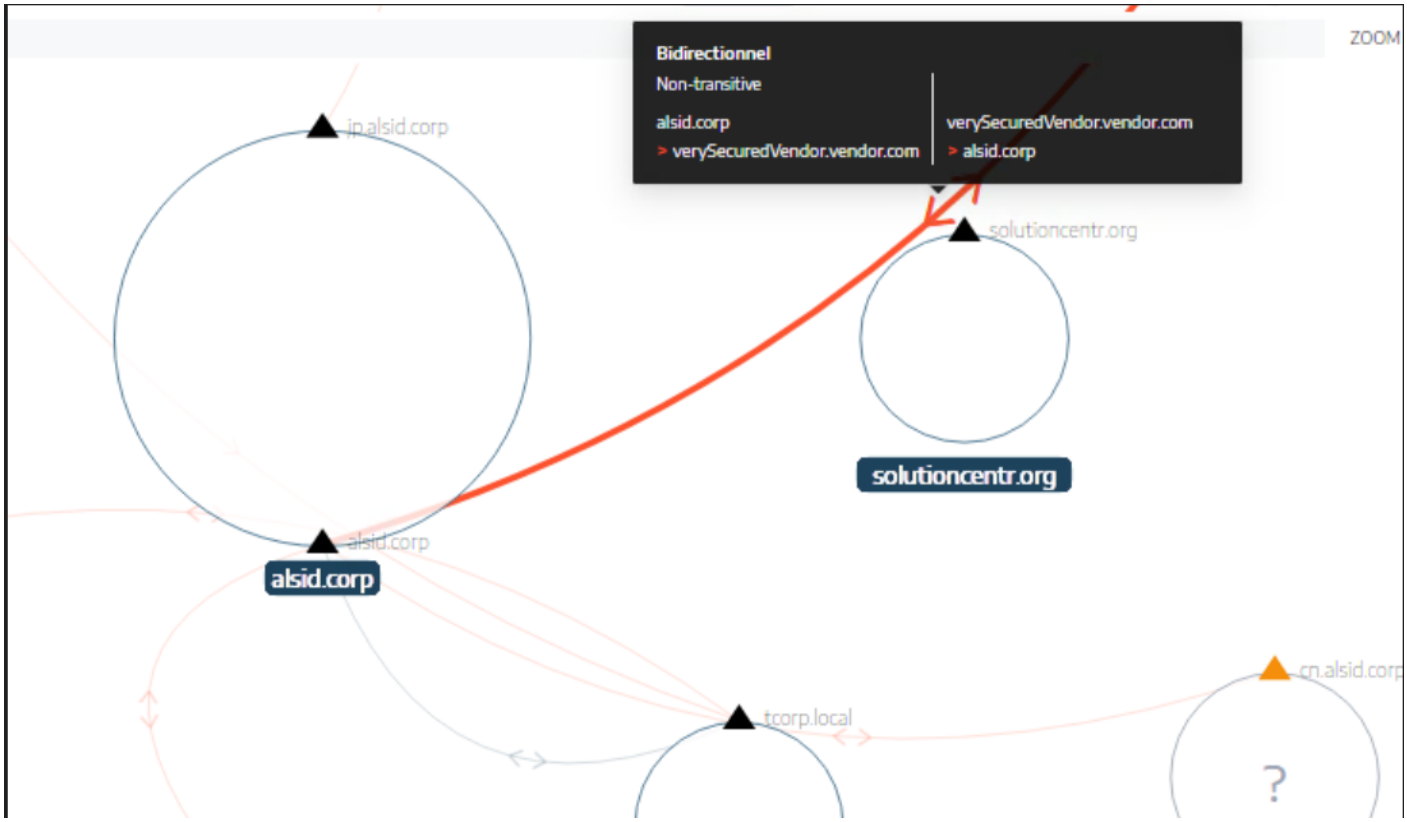
Relations d'approbation

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-	Indique que Tenable Identity Exposure a activé l'authentification

organization authentication	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 :

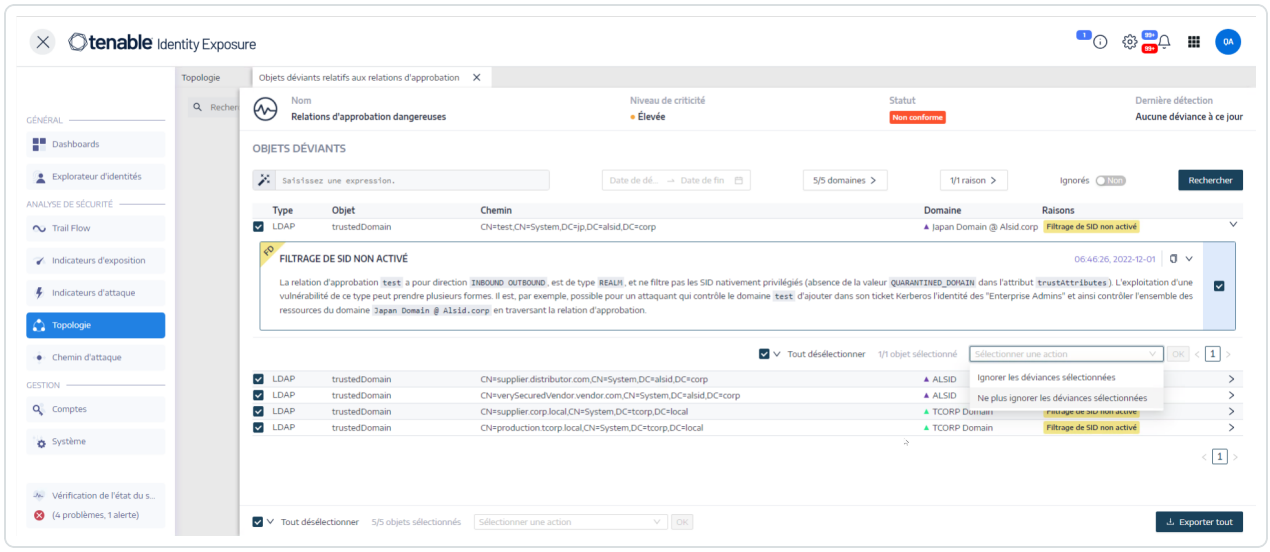
- **Rouge** pour les relations d'approbation dangereuses
- **Orange** pour les relations d'approbation normales
- **Bleu** pour les relations d'approbation inconnues

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

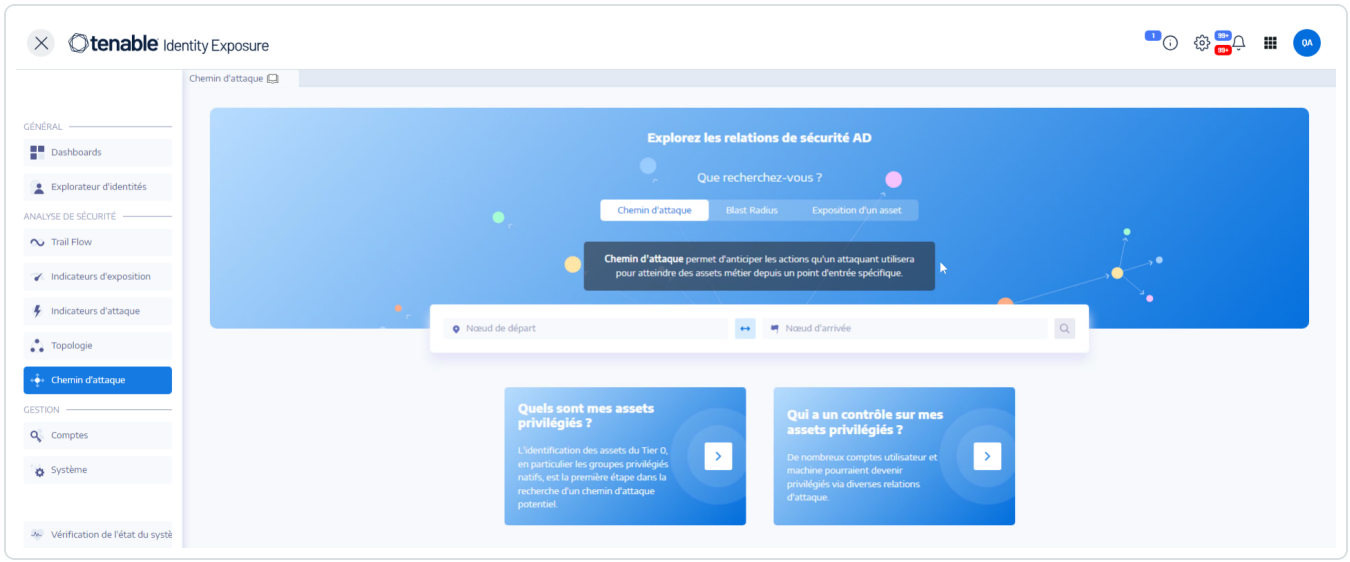
Tenable Identity Exposure offre plusieurs façons de visualiser la vulnérabilité potentielle d'un asset opérationnel à l'aide de représentations graphiques.

- **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.

Pour afficher le chemin d'attaque :

1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

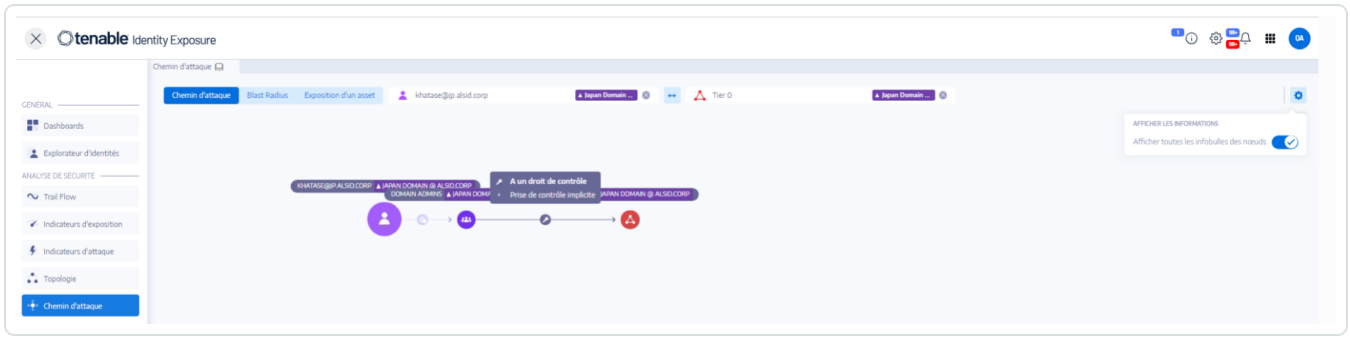
   Le volet **Chemin d'attaque** apparaît.



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 :

   - Cliquez 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.

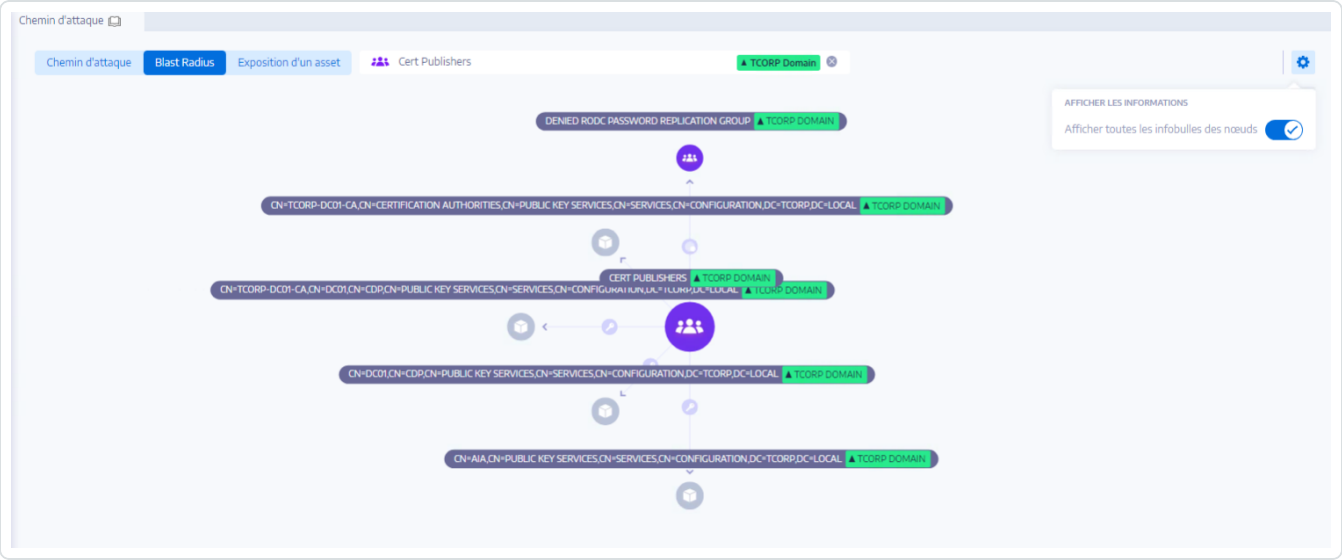
Pour afficher le Blast Radius (rayon d'impact) :

1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

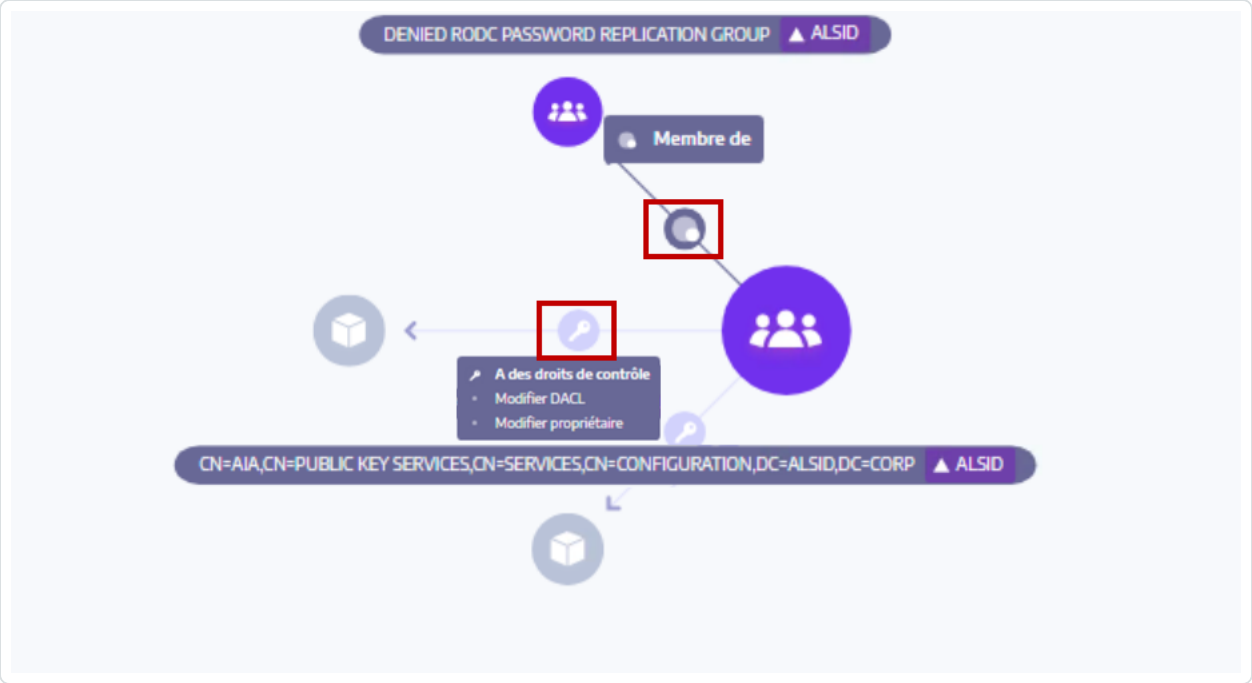
   Le volet **Chemin d'attaque** apparaît.

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 :

1. Pour afficher le Blast Radius (rayon d'impact) :
2. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

   Le volet **Chemin d'attaque** apparaît.

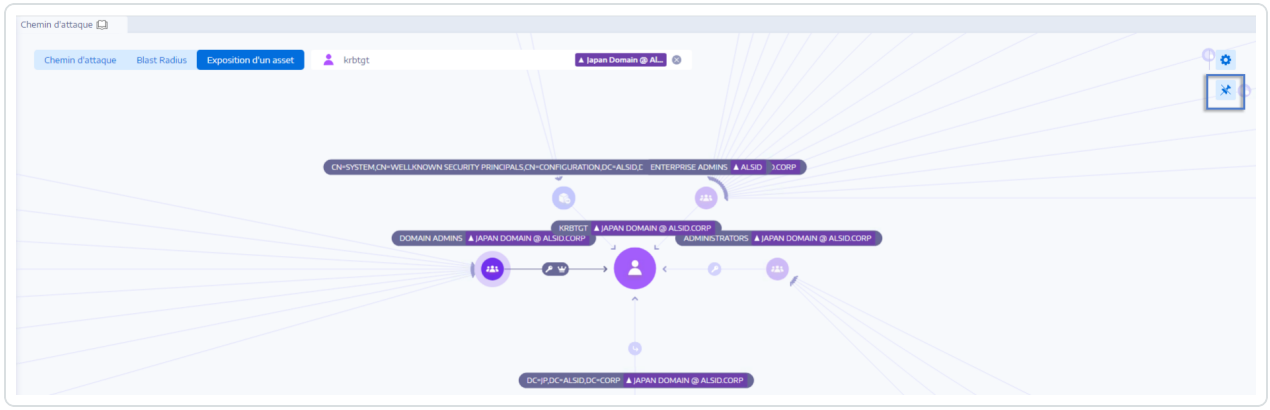
3. Dans la bannière, cliquez sur **Exposition de l'asset**.
4. Dans la zone **Rechercher un objet**, saisissez le nom d'un asset.
5. Cliquez sur l'icône .

   Tenable Identity Exposure affiche les chemins vers l'asset et les relations entre les assets.
6. Cliquez sur les icônes des flèches qui relient les assets pour afficher leurs relations.

Pour épingler un chemin d'attaque :

1. Cliquez sur un nœud dans le chemin d'attaque à mettre en évidence.

   Tenable Identity Exposure épingle le chemin d'attaque sur l'écran.
2. Pour désépingler le chemin d'attaque, cliquez sur l'icône ou sur un autre nœud dans un autre chemin d'attaque.

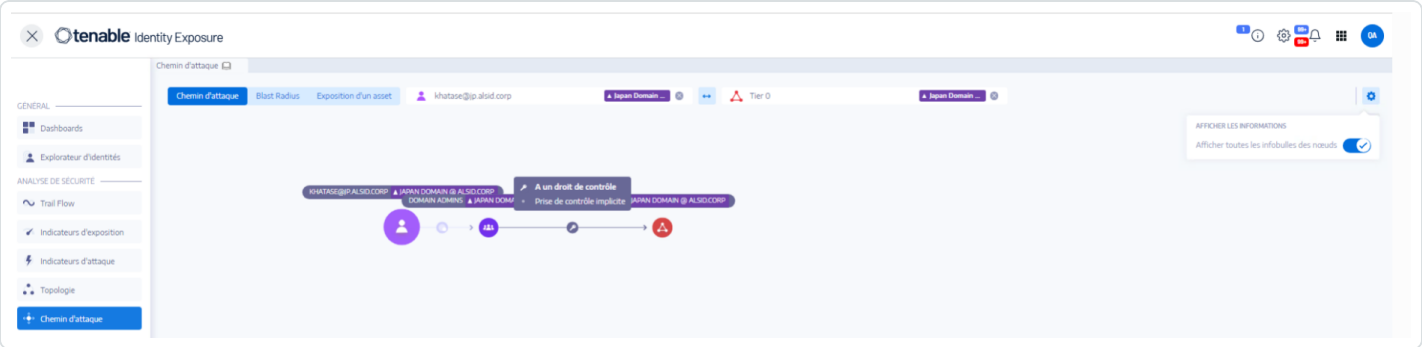


Voir aussi

- Relations 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.

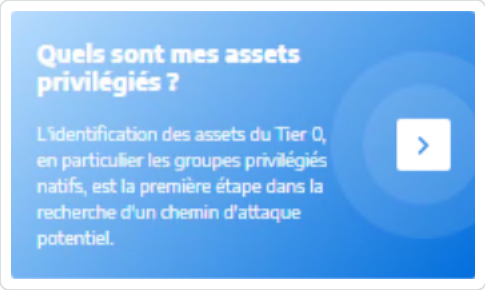
Tenable Identity Exposure répertorie vos assets et vos comptes Tier 0 avec les chemins d'attaque potentiels menant à l'asset.

Pour afficher la liste des assets Tier 0 :

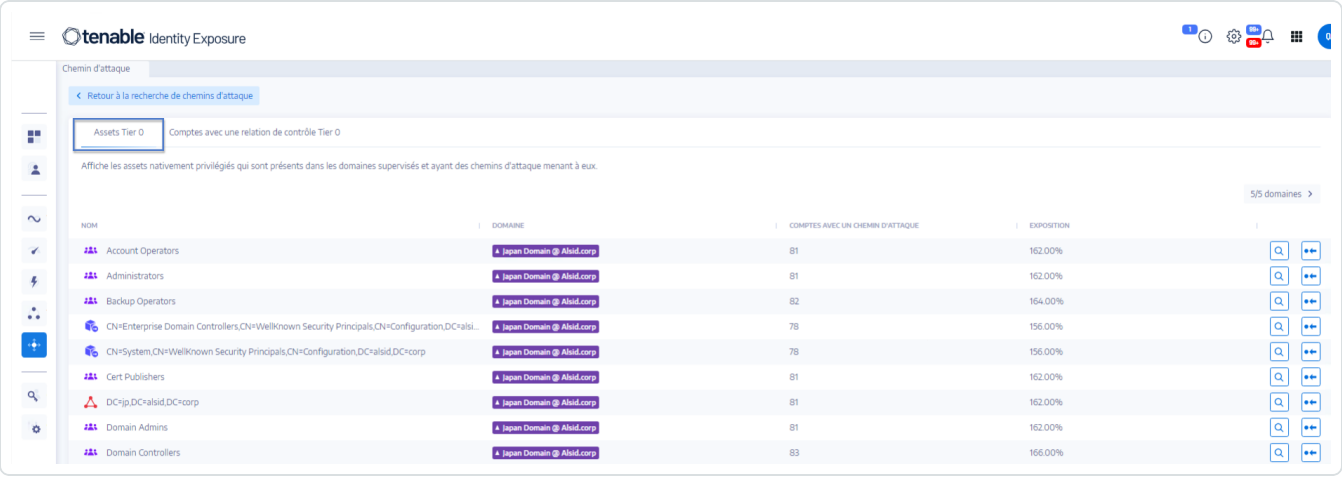
1. Dans Tenable Identity Exposure, cliquez sur l'icône de chemin d'attaque dans la barre de navigation de gauche.

   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 :

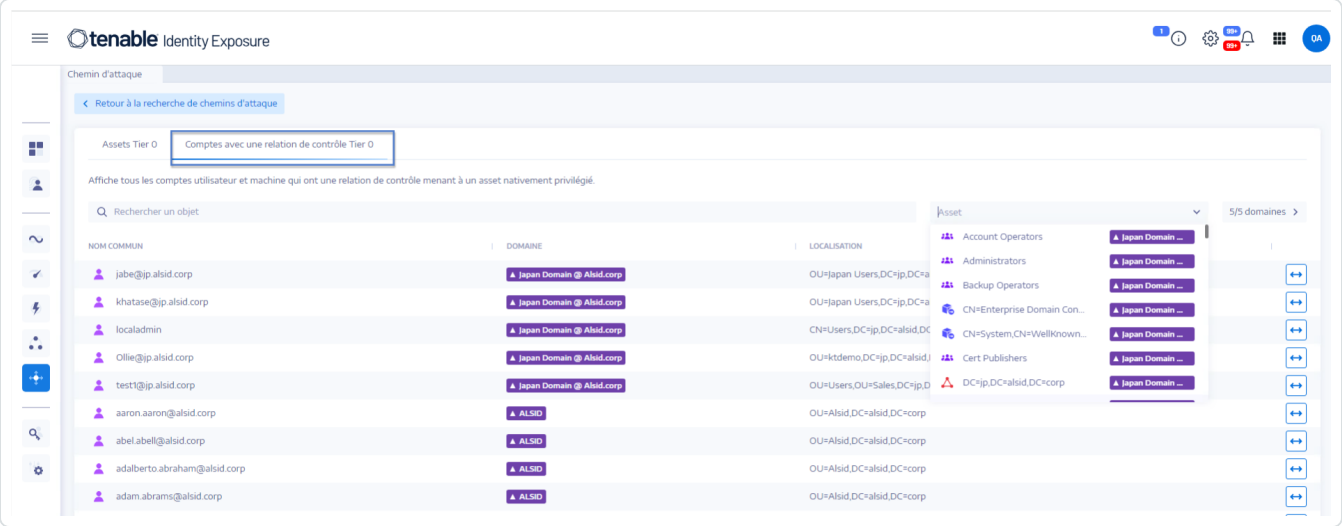
1. Dans Tenable Identity Exposure, cliquez sur l'icône de chemin d'attaque dans la barre de navigation de gauche.

   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.

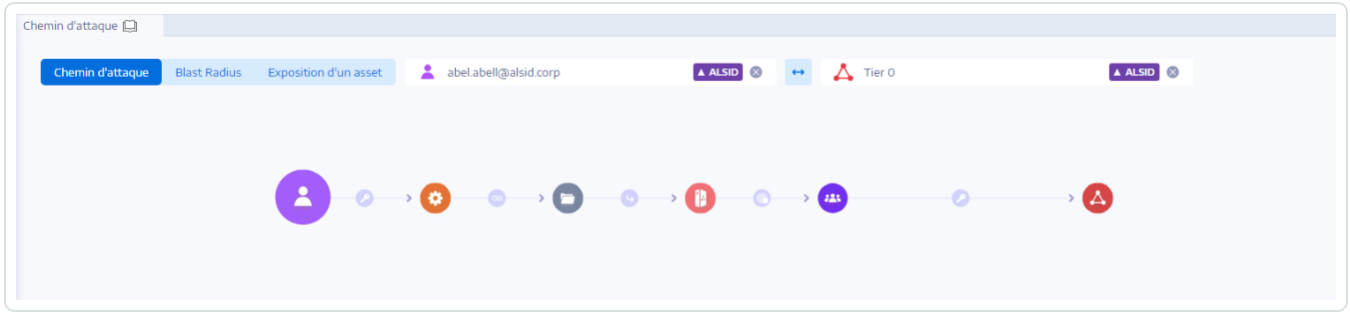
2. Cliquez sur **Filtrer sur la sélection**.

   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 le groupe `class`.
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 organisationnelle (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.

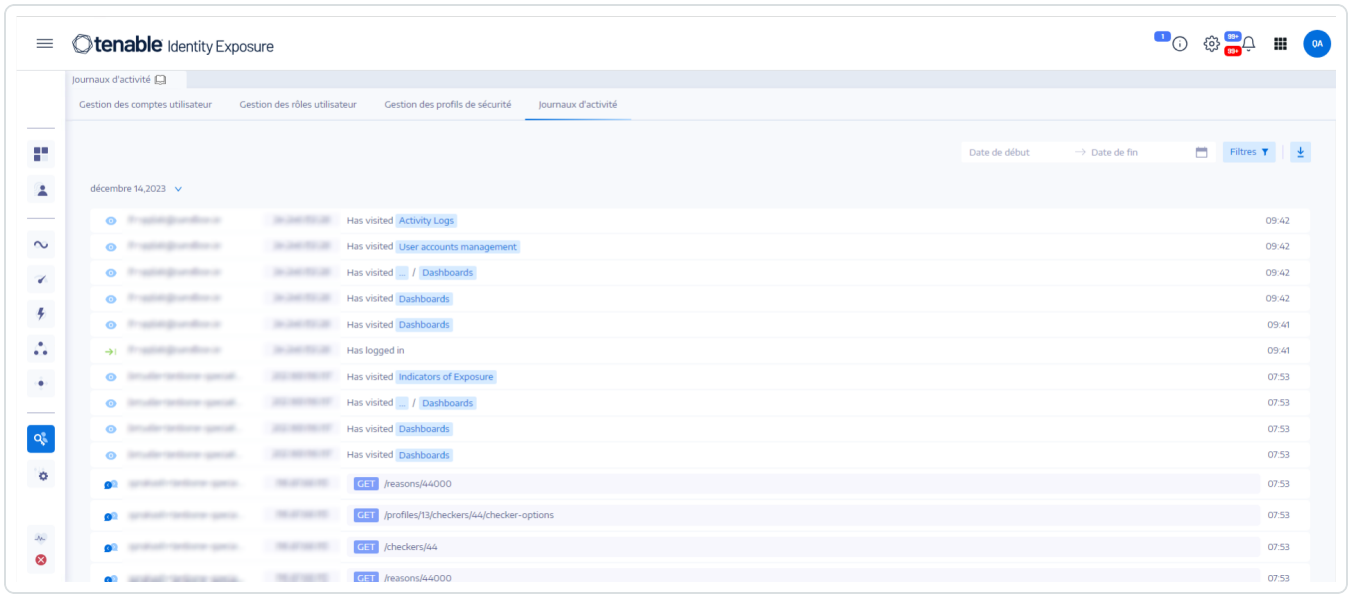
Pour afficher les journaux d'activités :

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 Filters.

   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.

Guide de l'administrateur Tenable Identity Exposure

Dernière mise à jour : 30 avril 2024

Le Guide de l'administrateur fournit des informations sur les tâches d'administration pour Tenable Identity Exposure (anciennement Tenable.ad).

Tenable recommande d'effectuer certaines des opérations suivantes pour démarrer en tant qu'administrateur dans Tenable Identity Exposure :

- Préparer et installer
- Configurer le profil et les utilisateurs
- Détecter et surveiller

Conseil : 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)

Préparer et installer

Pour préparer et réaliser l'installation de Tenable Identity Exposure :

- Installez Tenable Identity Exposure comme indiqué dans le *Guide d'installation de Tenable Identity Exposure*.
- Connectez-vous à Tenable Identity Exposure.

Configurer le profil et les utilisateurs

Nous recommandons ensuite d'effectuer les opérations suivantes pour configurer et parcourir l'interface de Tenable Identity Exposure :

- Définissez les préférences du profil : définissez votre langue par défaut, modifiez votre mot de passe et définissez les autres préférences de votre profil.
- Créez et ajoutez des utilisateurs à votre instance Tenable Identity Exposure.

- Configurez le contrôle d'accès basé sur le rôle (RBAC) pour sécuriser l'accès aux données et aux fonctions au sein de votre organisation.

Détecter et surveiller

Une fois que vous avez configuré et adapté Tenable Identity Exposure aux besoins de votre entreprise, vous pouvez commencer à travailler avec vos données :

- Déployez le module Indicateurs d'attaque.
- Gérez et recevez des informations pertinentes sur l'état de sécurité de l'infrastructure surveillée à l'aide du portail Tenable Identity Exposure.
- Définissez des scénarios d'attaque en sélectionnant les types d'attaques que Tenable Identity Exposure doit surveiller dans des domaines spécifiques.

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

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.

Pour plus d'informations, voir ce qui suit :

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 l'interface de ligne de commande du contrôleur de domaine, exécutez la commande suivante pour accorder l'accès aux objets ou conteneurs Active Directory :

  Remarque : vous devez exécuter cette commande sur chaque domaine surveillé par Tenable Identity Exposure.

```
dsacls "<__CONTAINER__>" /takeownership
dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
```

où :

- <__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 :

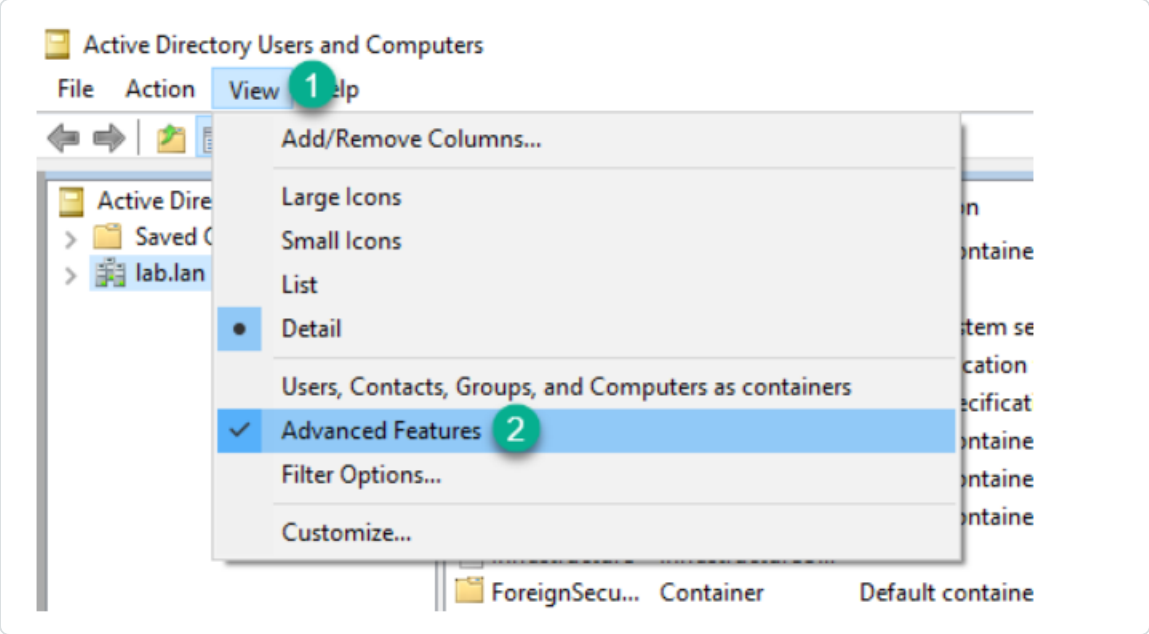
  ```
  dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
  SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
  ```

  Où :

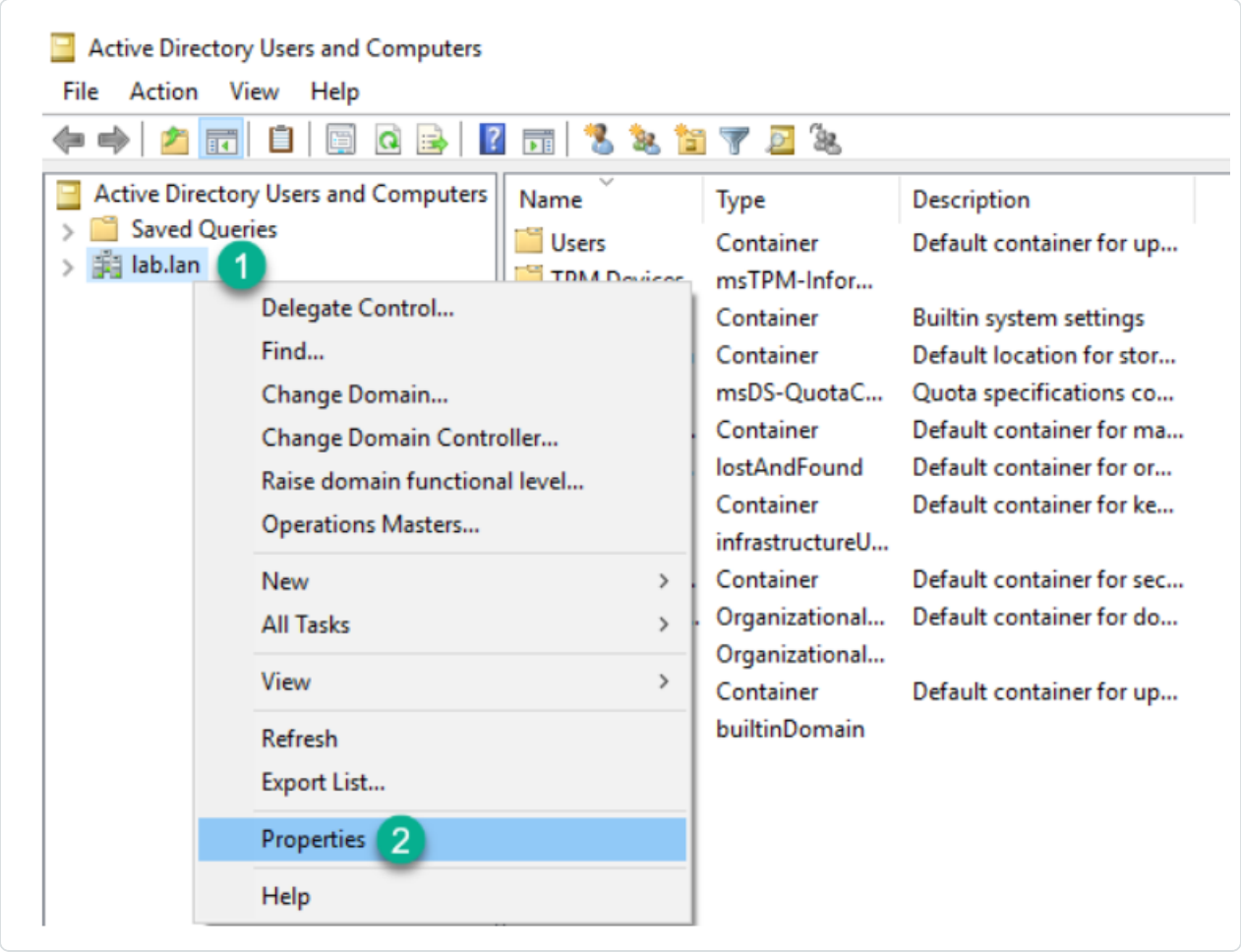
  - `<__DOMAIN_ROOT__>` fait référence au nom distinctif de la racine du domaine. Exemple : « `DC=<DOMAINE>,DC=<TLD>` «
  - `<__SERVICE_ACCOUNT__>` désigne le compte de service que Tenable Identity Exposure utilise. Exemple : « `DOMAIN\tenablead` ».

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 **Afficher**, sélectionnez **Fonctions avancées**.

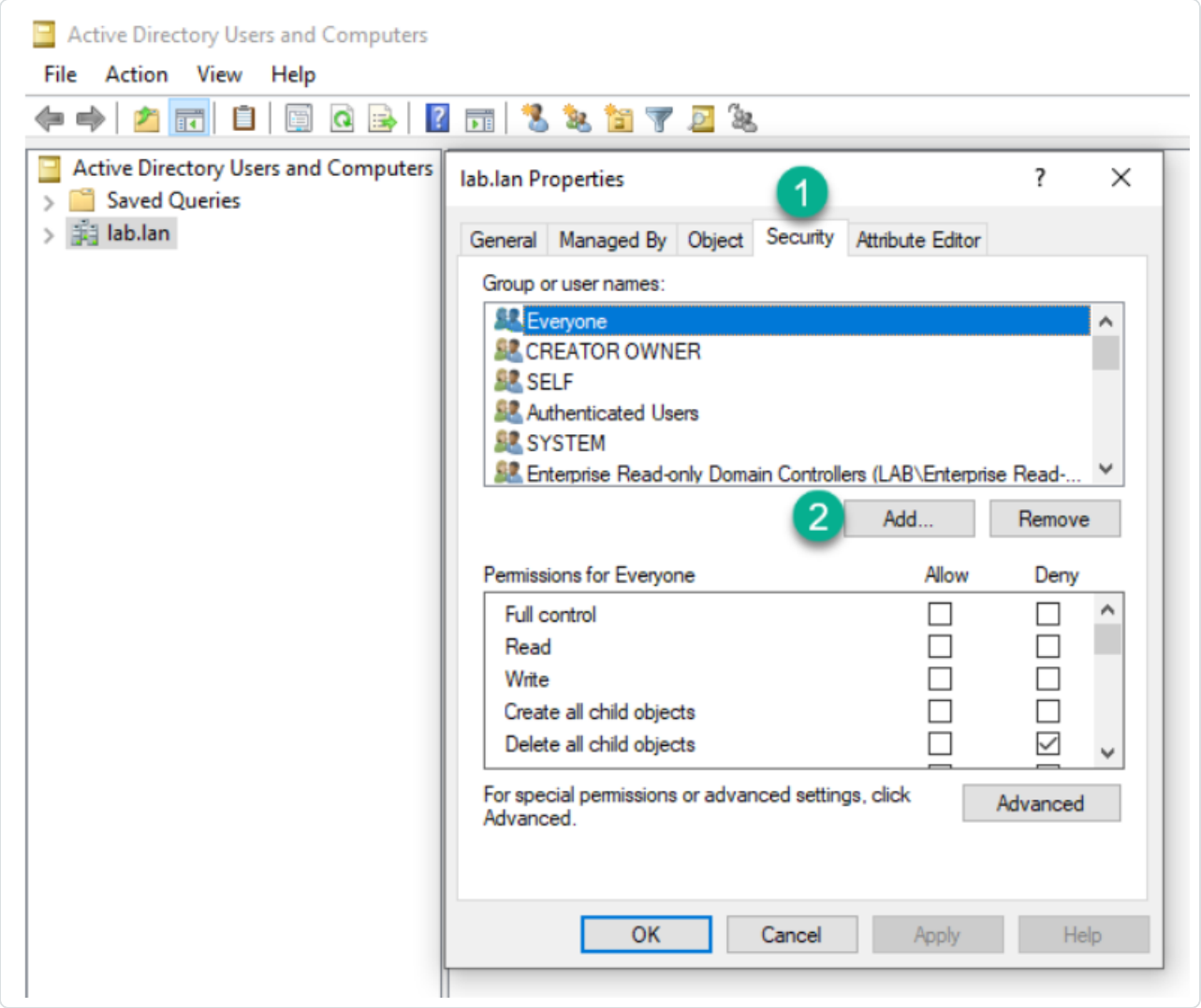


3. Cliquez avec le bouton droit sur la racine du domaine et sélectionnez **Propriétés**.



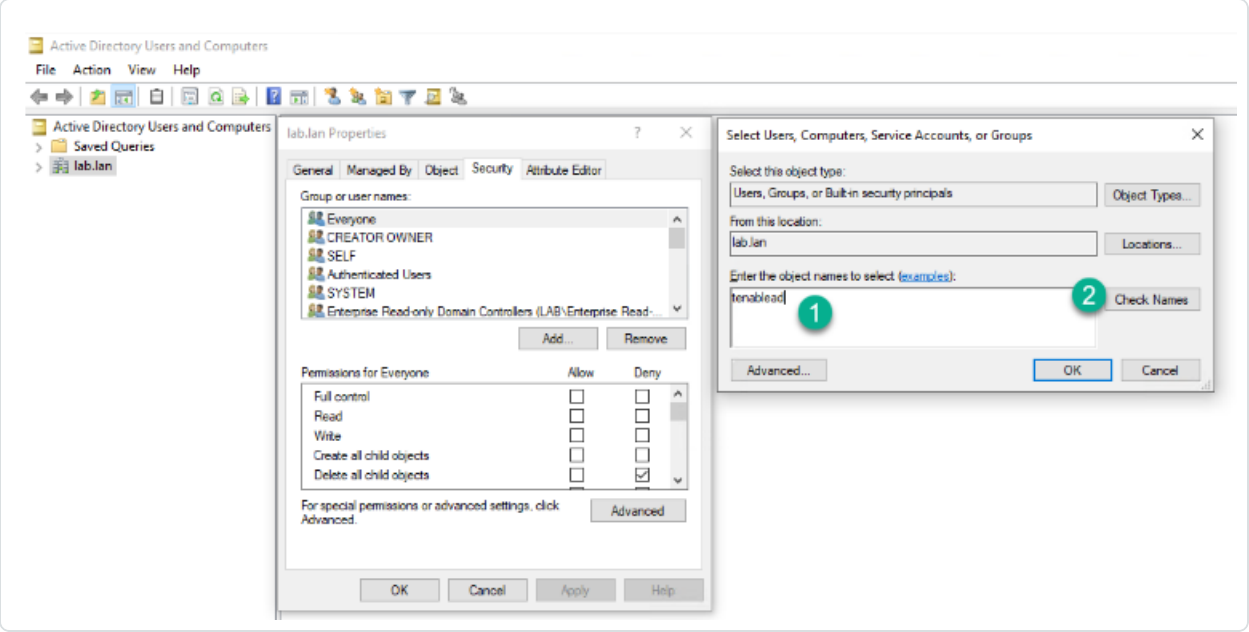
Le volet des propriétés de la racine du domaine apparaît.

4. Cliquez sur l'onglet **Sécurité** et sur **Ajouter**.



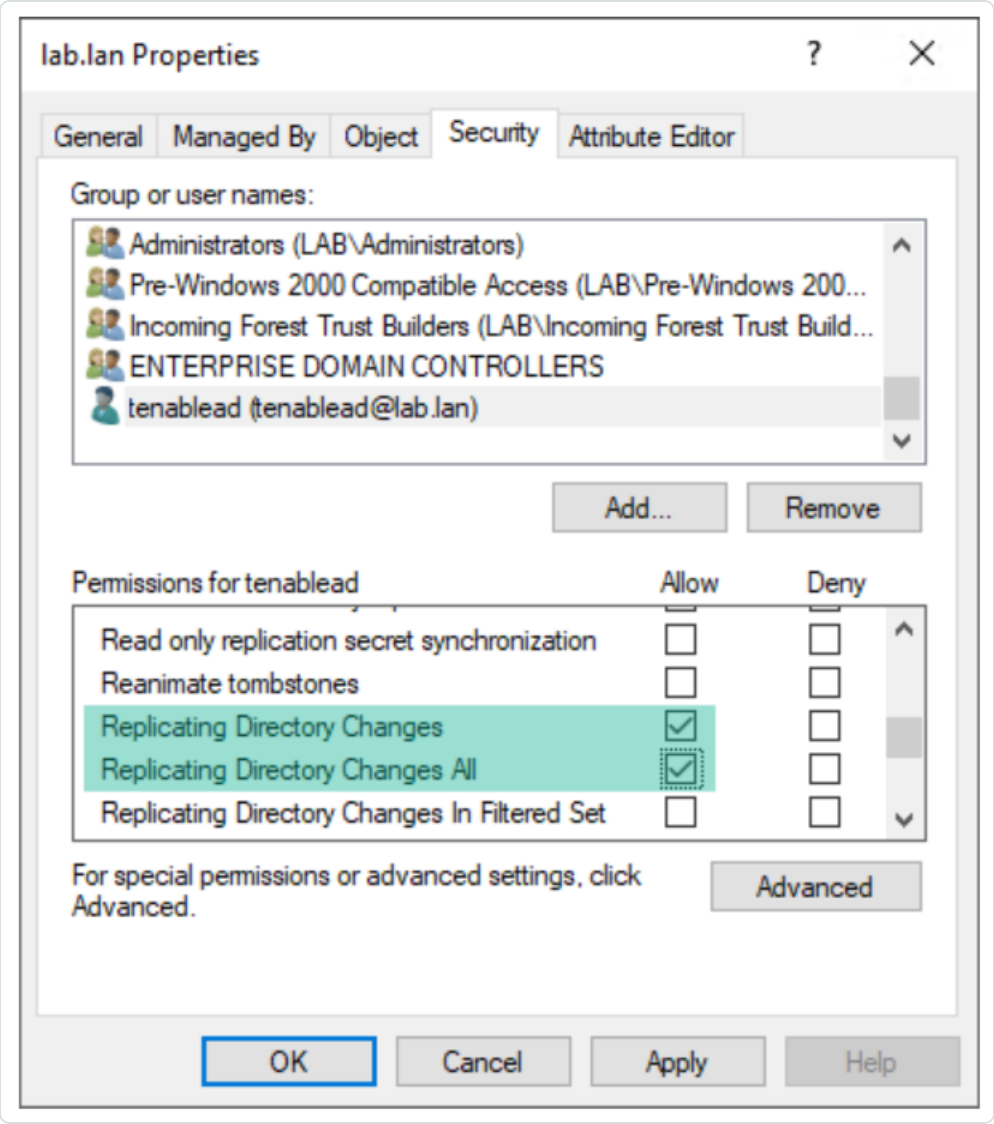
5. Localisez le compte de service Tenable Identity Exposure :

> **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**.

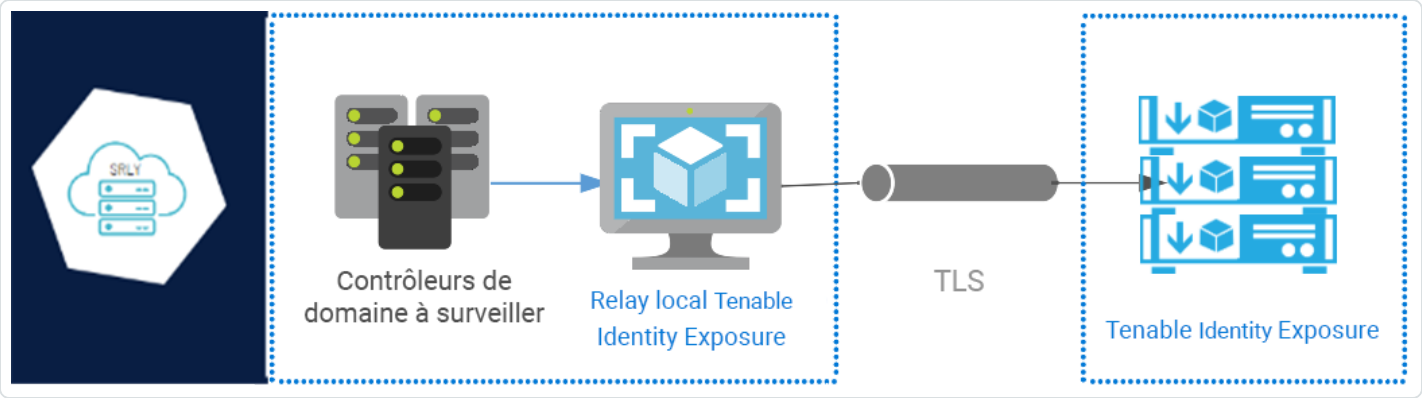
Vous devez attribuer des autorisations supplémentaires **au niveau de la racine du domaine**.
Active Directory ne prend pas en charge les autorisations attribuées à une unité d'organisation ou à un utilisateur spécifique (par exemple, pour limiter l'analyse privilégiée à l'UO ou à l'utilisateur) et celles-ci 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.

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.

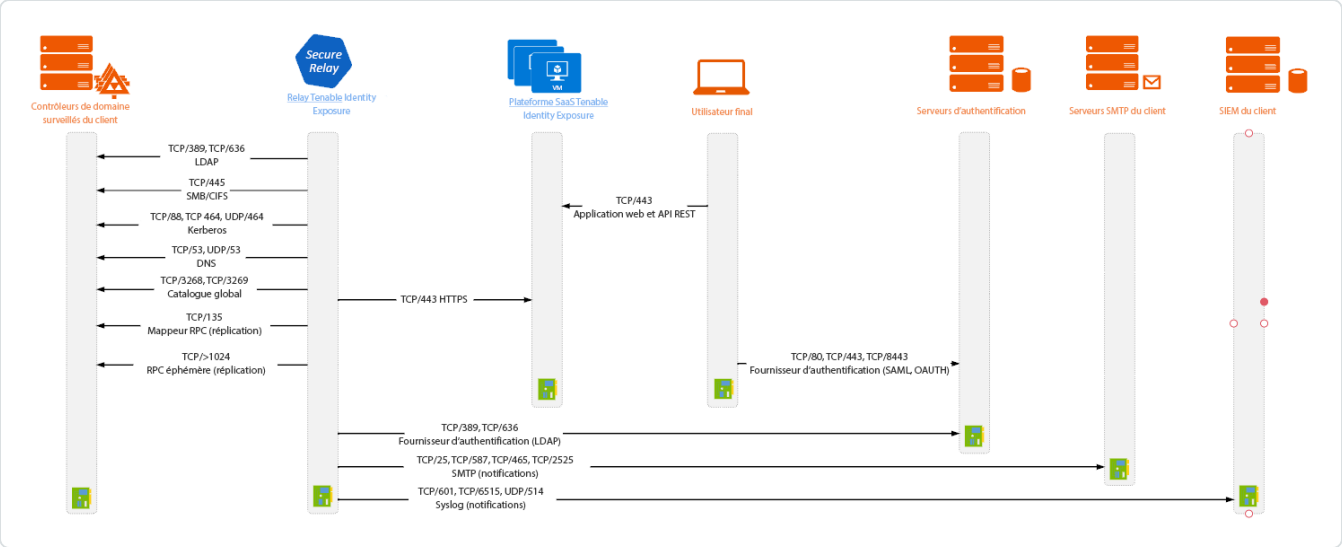


Remarque : la fonction Secure Relay ne s'applique actuellement que si Tenable Identity Exposure provisionne votre plateforme pour utiliser Secure Relay. Il n'est pas possible de passer manuellement d'un VPN à Secure Relay. Pour obtenir de l'aide sur la migration de votre plateforme d'un VPN vers Secure Relay, contactez votre représentant du service client Tenable Identity Exposure.

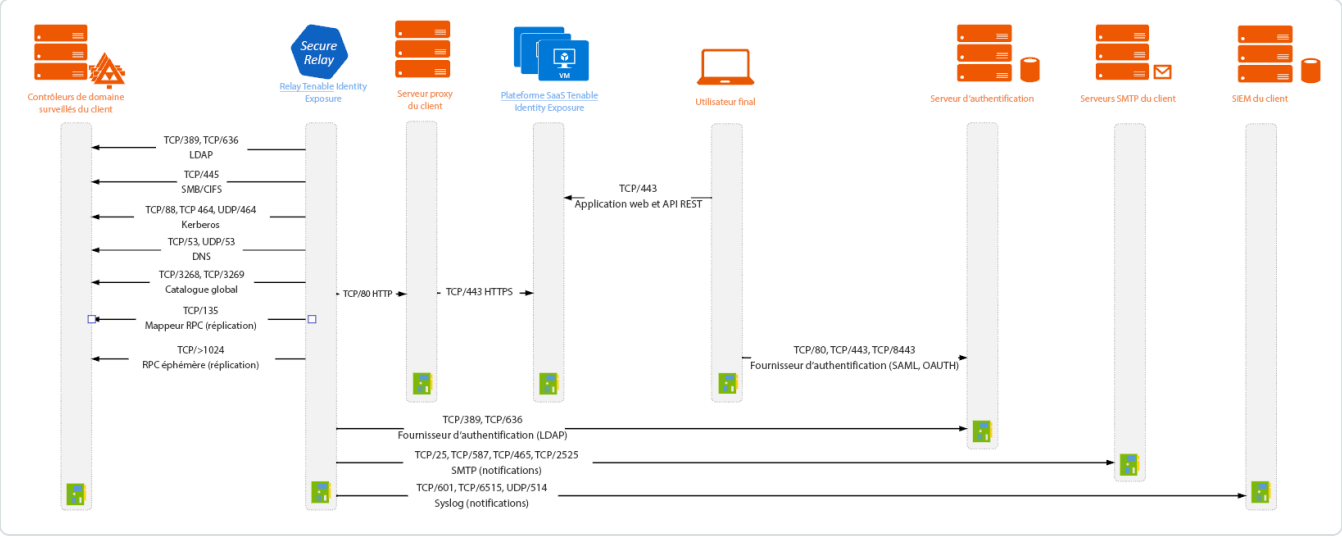
Flux réseau

Ports requis pour Secure Relay

- 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 :



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 :

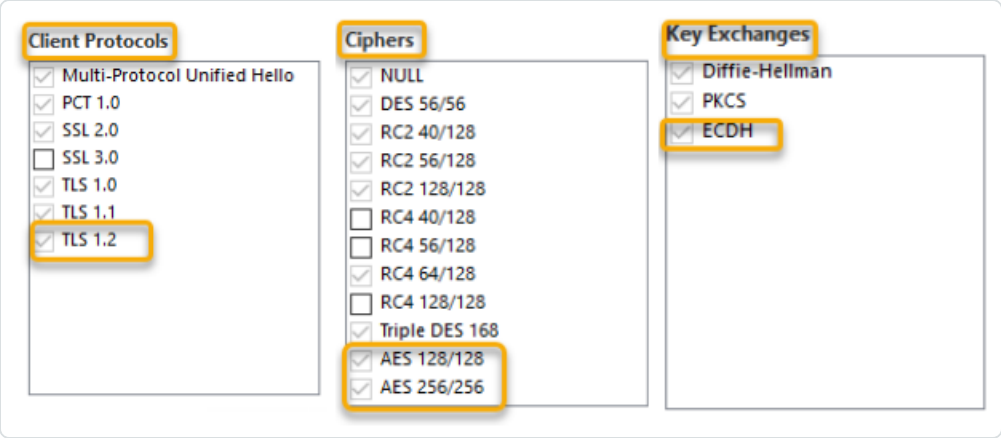
   ```
   Get-TlsEccCurve
   ```

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.

Avant de commencer

Conditions préalables

Machine virtuelle

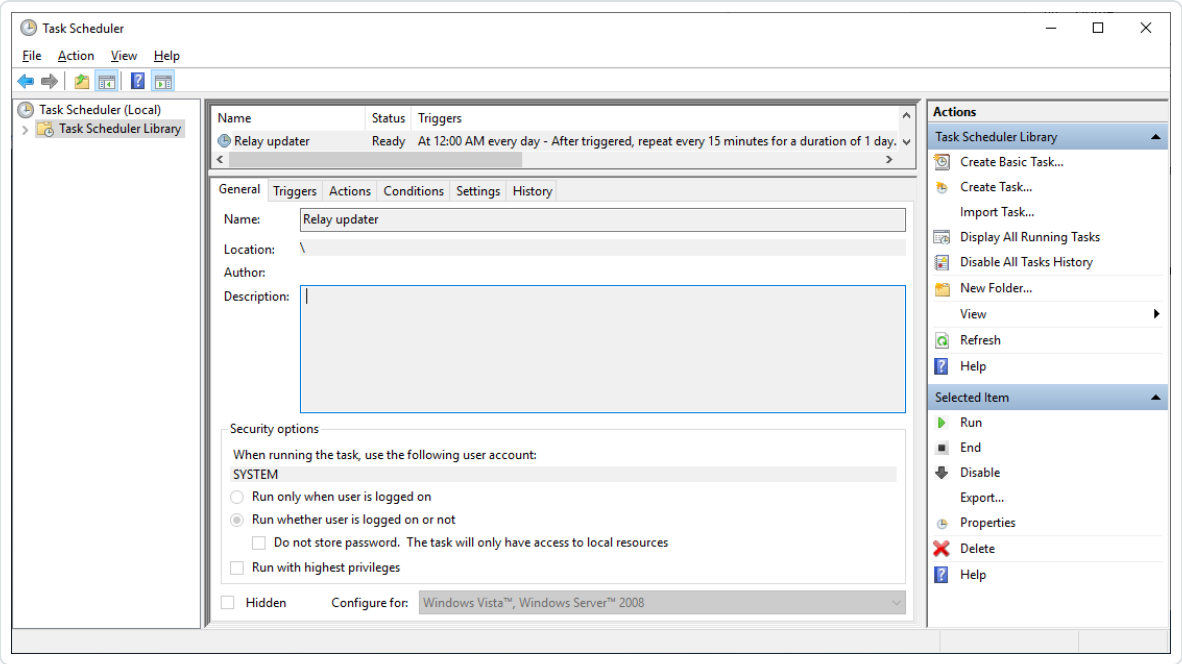
La machine virtuelle (VM) hébergeant le Secure Relay doit présenter les caractéristiques suivantes :

Taille du client	Services Tenable Identity Exposure	Instance requise	Mémoire (par instance)	vCPU (par instance)	Topologie de disque	Espace 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

La VM doit également avoir :

- 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 » :



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.

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).

Autorisez les fichiers et processus suivants :

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

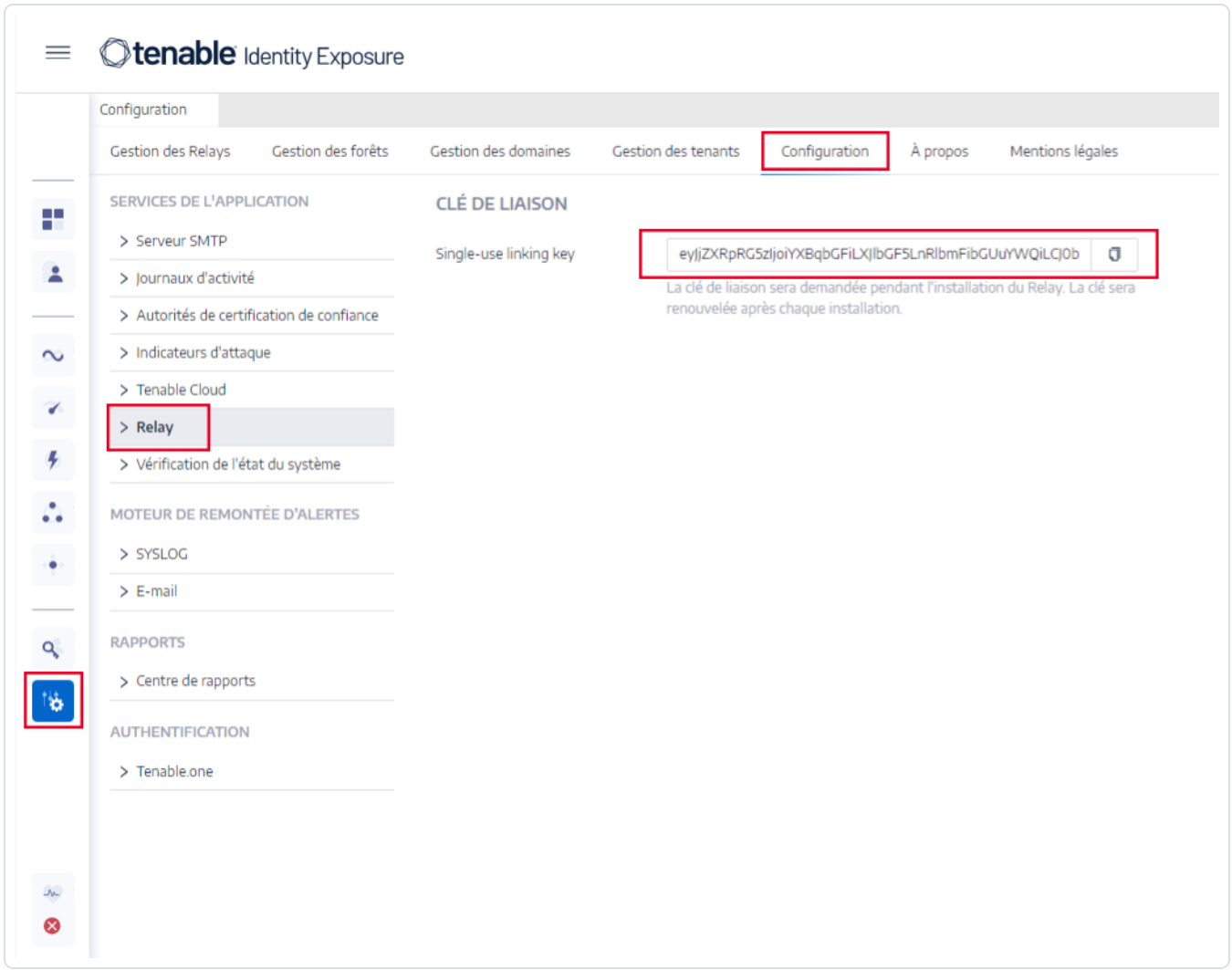
Clé de registre
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

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 de Secure Relay.

Pour récupérer la clé de liaison :

1. Dans 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.

Installation

Pour installer le Secure Relay :

- Choisissez une méthode d'installation :
    - Installer le Secure Relay (Interface graphique)
    - Installer le Secure Relay (Tenable Nessus Agent)

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.

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.

Voir aussi

Pour des informations complètes sur Secure Relay, voir Secure Relay dans le Guide de l'administrateur Tenable Identity Exposure.

Installer le Secure Relay (Interface graphique)

La procédure suivante installe le Secure Relay en utilisant un programme d'installation Windows. 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 installer le Secure Relay :

1. Téléchargez le programme d'installation depuis le portail des téléchargements Tenable Identity Exposure sur votre machine virtuelle.
2. Double-cliquez sur le fichier `tenable.ad_SecureRelay_v3.xx.x` pour lancer l'assistant d'installation.

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

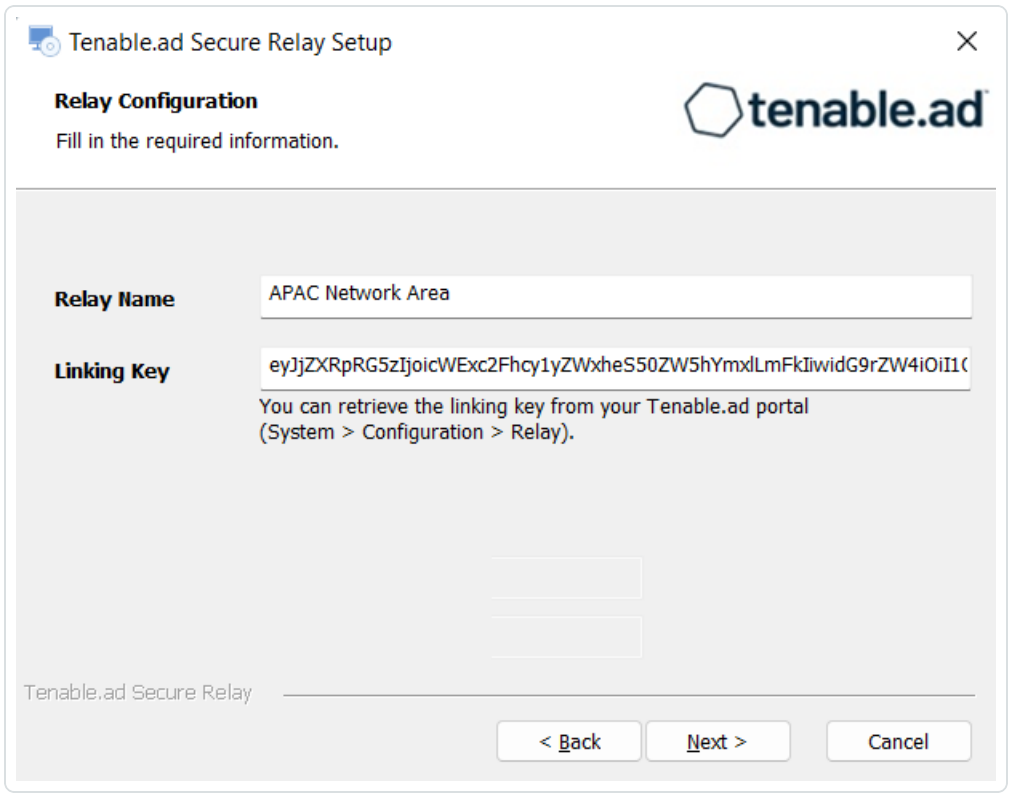
   

3. Cliquez sur **Next** (Suivant).

   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 :

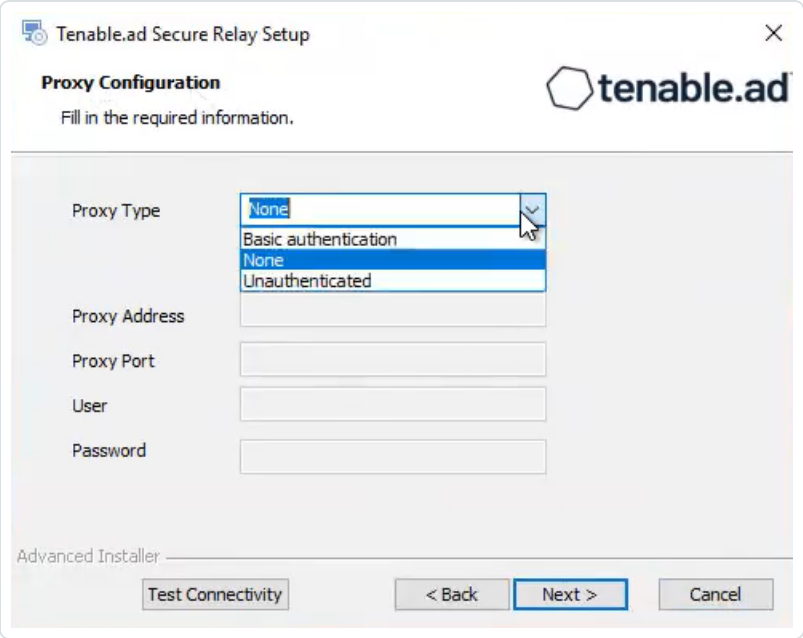
    a. Dans la zone **Relay Name** (Nom du Relay), saisissez le nom de votre Secure Relay.

    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).

Que faire ensuite

- Vérifications post-installation

Voir aussi

- Secure Relay
- Installer le Secure Relay (Tenable Nessus Agent)
- Vérifications post-installation
- Configurer le Relay

Installer le Secure Relay (Tenable Nessus Agent)

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

Avant de commencer

- Vérifiez que vous avez téléchargé et installé Tenable Nessus Agent.

  Remarque : le programme d'installation Tenable Nessus Agent 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 :

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

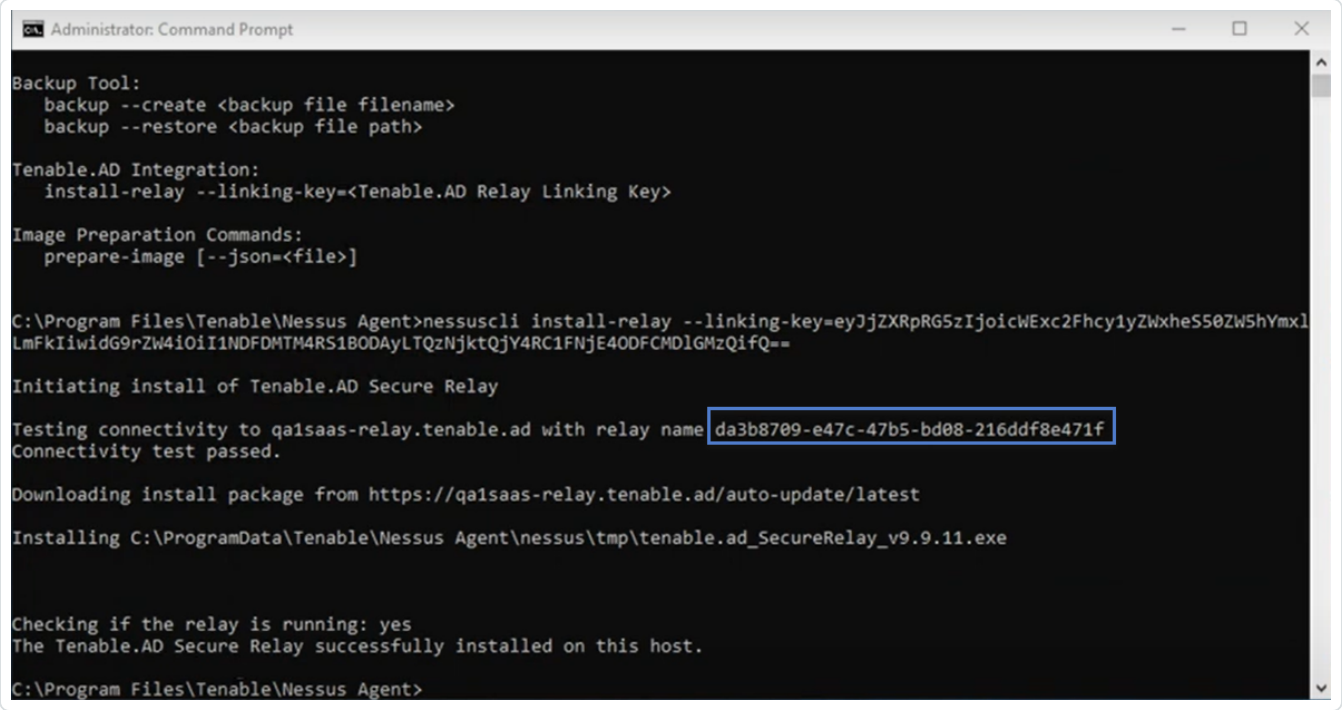
   Installation de Secure Relay

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

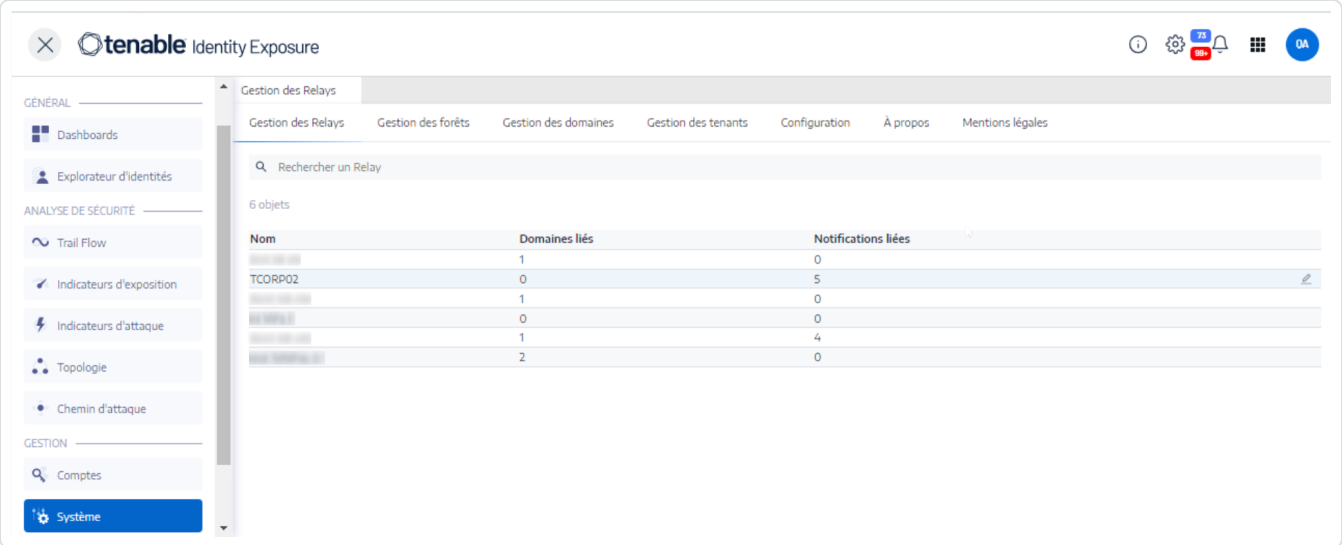
2. Remplacez <Tenable Identity Exposure Relay Linking Key> par la valeur que vous avez copiée précédemment à partir de votre instance Tenable Identity Exposure et fournissez une adresse et un numéro de port de proxy si vous utilisez un serveur proxy.

   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.



Que faire ensuite

- Vérifications post-installation

Voir aussi

- Secure Relay
- Installer le Secure Relay (Interface graphique)
- Vérifications post-installation
- Configurer le Relay

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 4 nouvelles variables d'environnement liées à Secure Relay dont les noms commencent par « ALSID ». Si vous avez choisi d'utiliser un serveur proxy, il existe 2 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.

Que faire ensuite

- Configurer le Relay

Voir aussi

- Secure Relay
- Installer le Secure Relay (Interface graphique)
- Installer le Secure Relay (Tenable Nessus Agent)

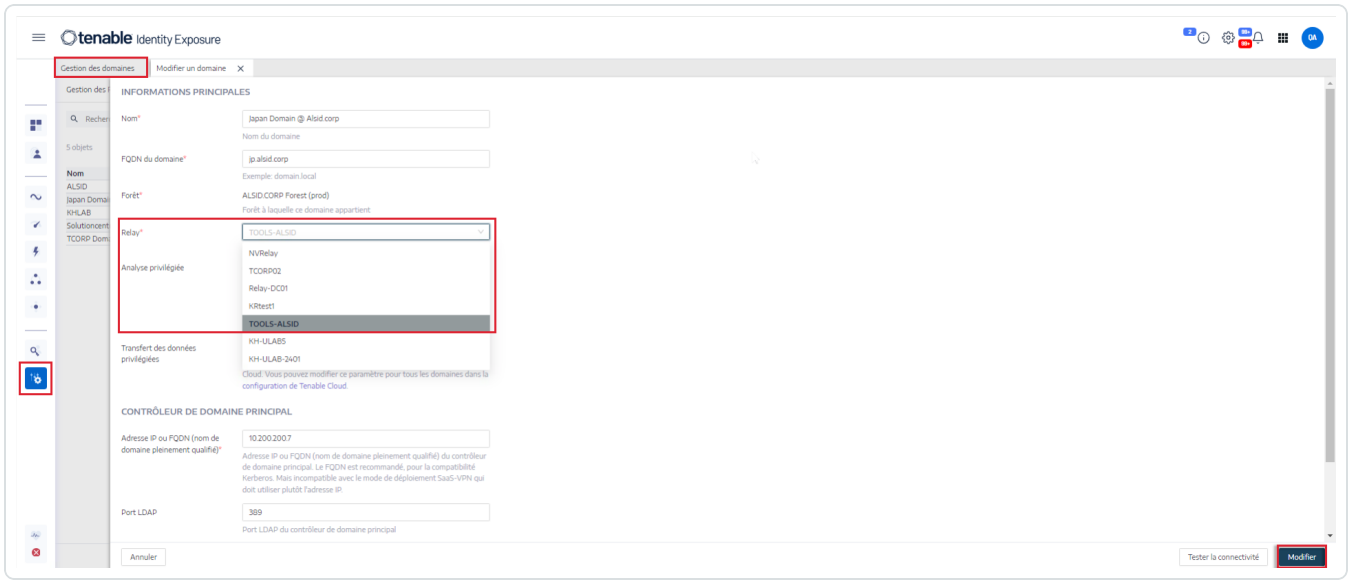
Configurer le Relay

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.

Pour lier 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.



4. 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.

Voir aussi

- Secure Relay
- Installer le Secure Relay (Interface graphique)
- Installer le Secure Relay (Tenable Nessus Agent)
- Vérifications post-installation

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.

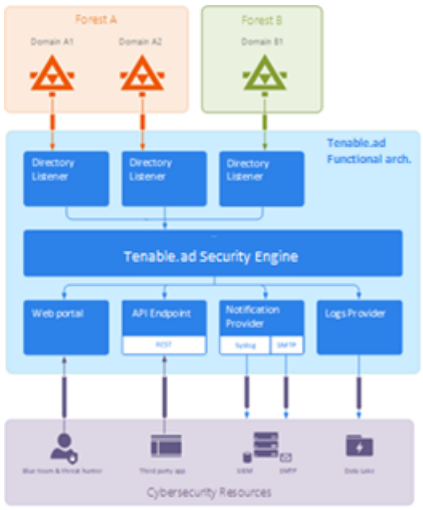
Tenable Identity Exposure utilise un compte utilisateur standard sans autorisations administratives pour se connecter aux API standard et exécuter sa fonction de surveillance de la sécurité.

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.
- 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.

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.

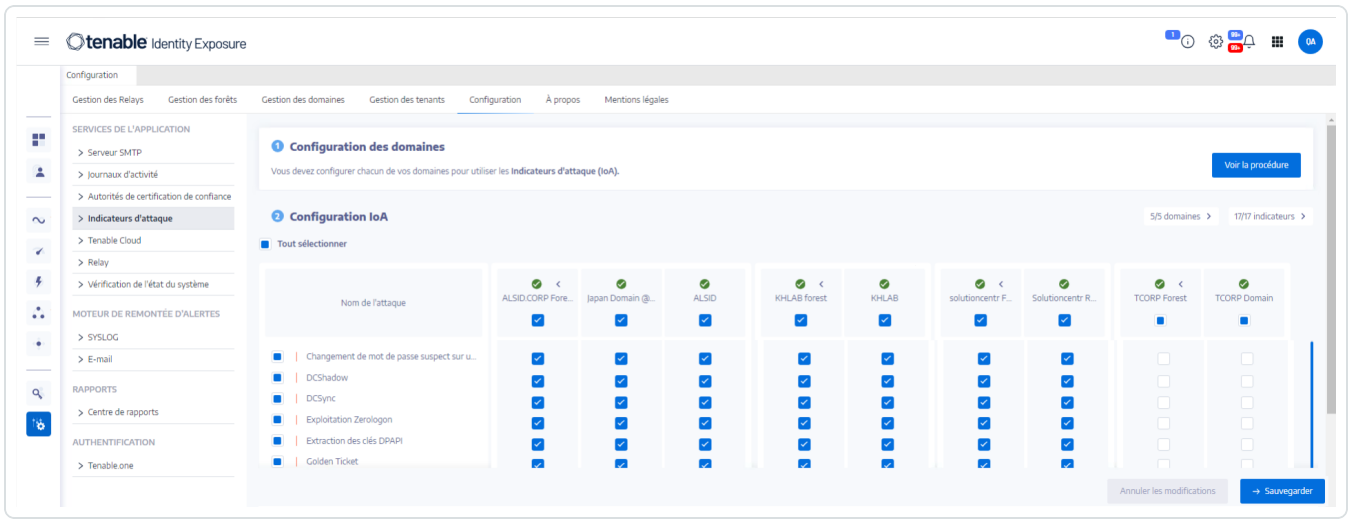
Pour configurer des domaines pour les IoA :

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

   Le volet **Configuration** apparaît.

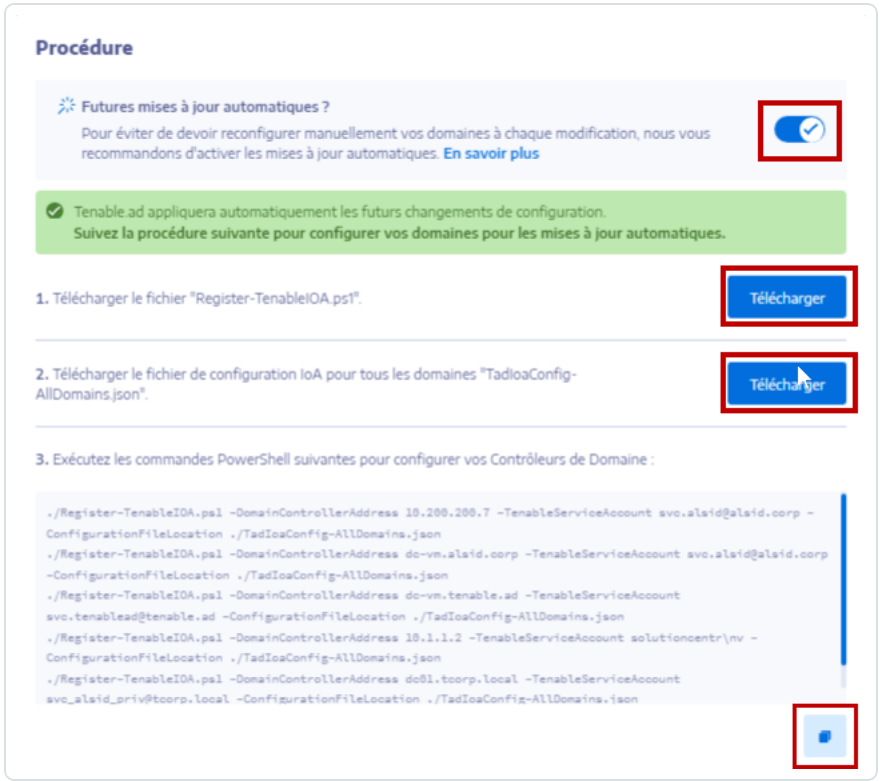
2. Cliquez sur **Indicateurs d'attaque**.

   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 ?** :

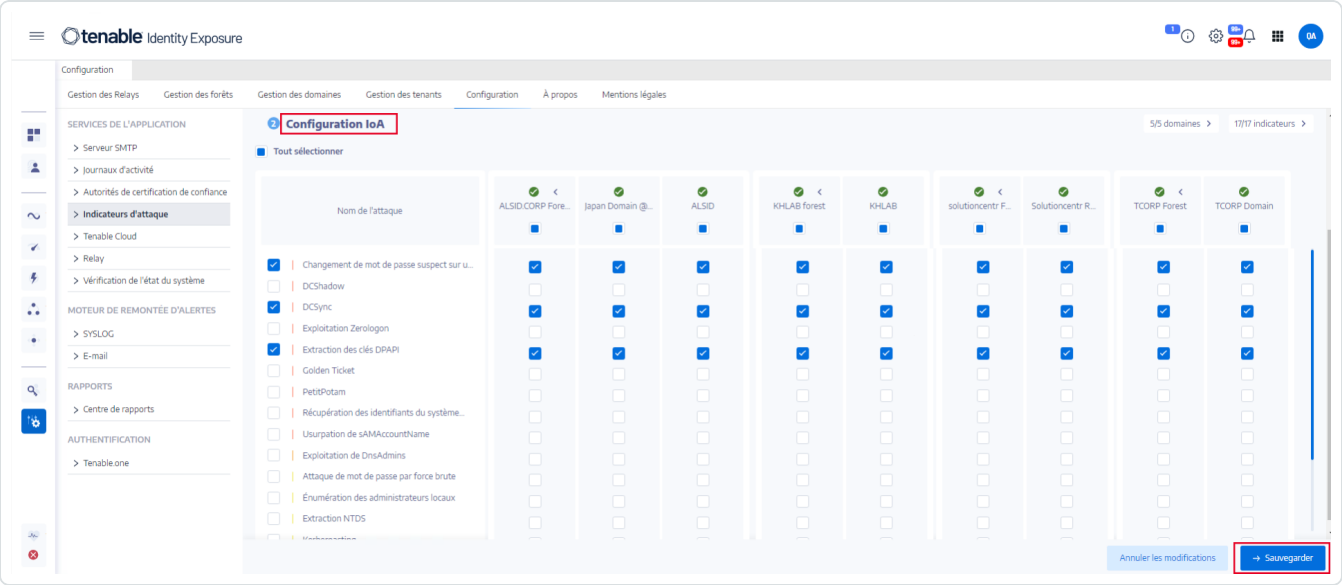
- L'option par défaut **Activer** permet à Tenable Identity Exposure de mettre automatiquement à jour votre configuration IoA chaque fois que vous la modifiez dans Tenable Identity Exposure à l'avenir. Cela permet également d'analyser la sécurité en continu.
- Si vous désactivez cette option, un message 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.

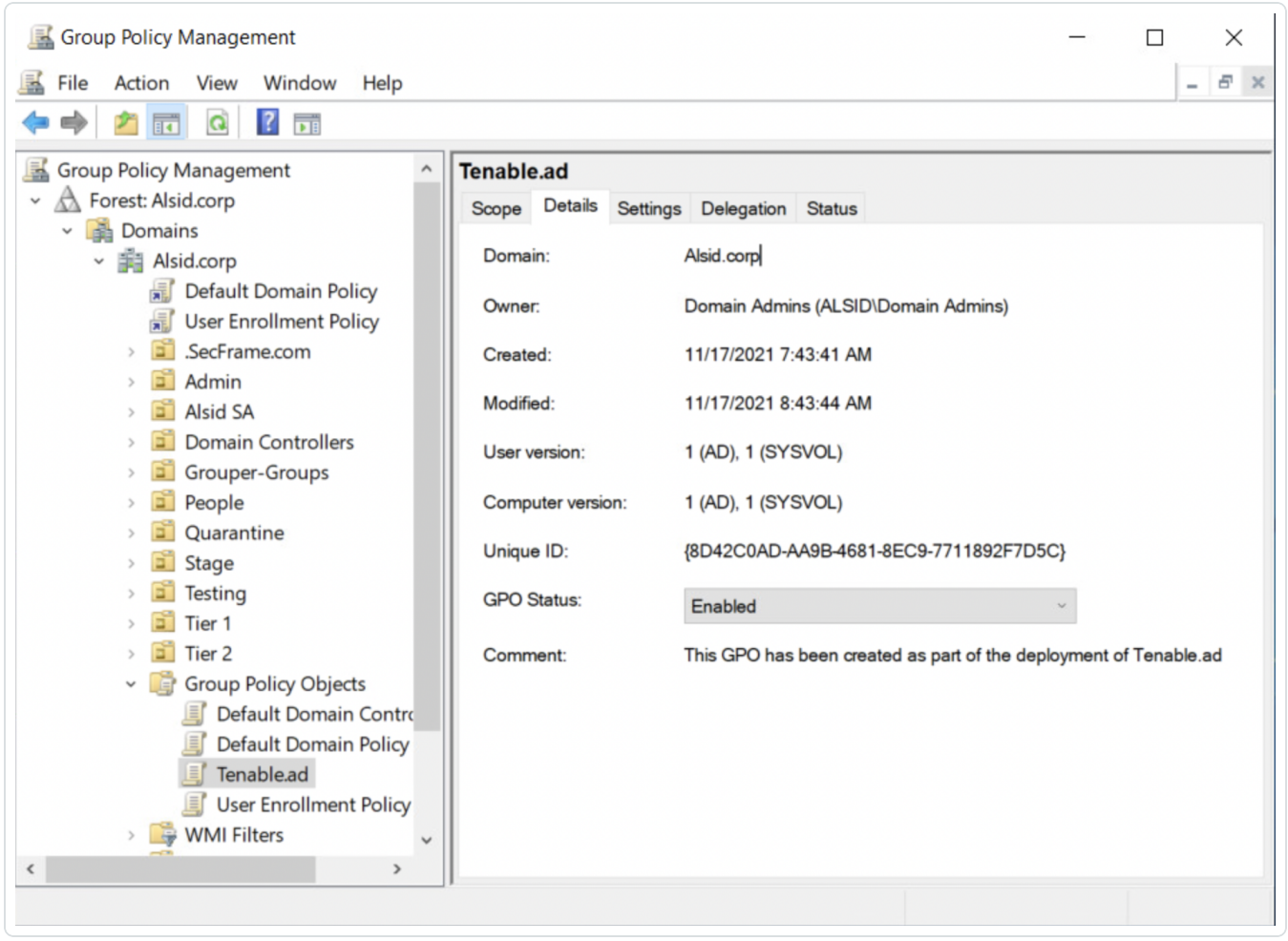


Conseil : l'indicateur d'attaque (IoA) Zerologon **Exploitation** date de 2020. Si tous vos contrôleurs de domaine (DC) ont reçu des mises à jour au cours des trois dernières années, ils sont protégés contre cette vulnérabilité. Pour déterminer les correctifs requis pour sécuriser vos DC contre cette 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.

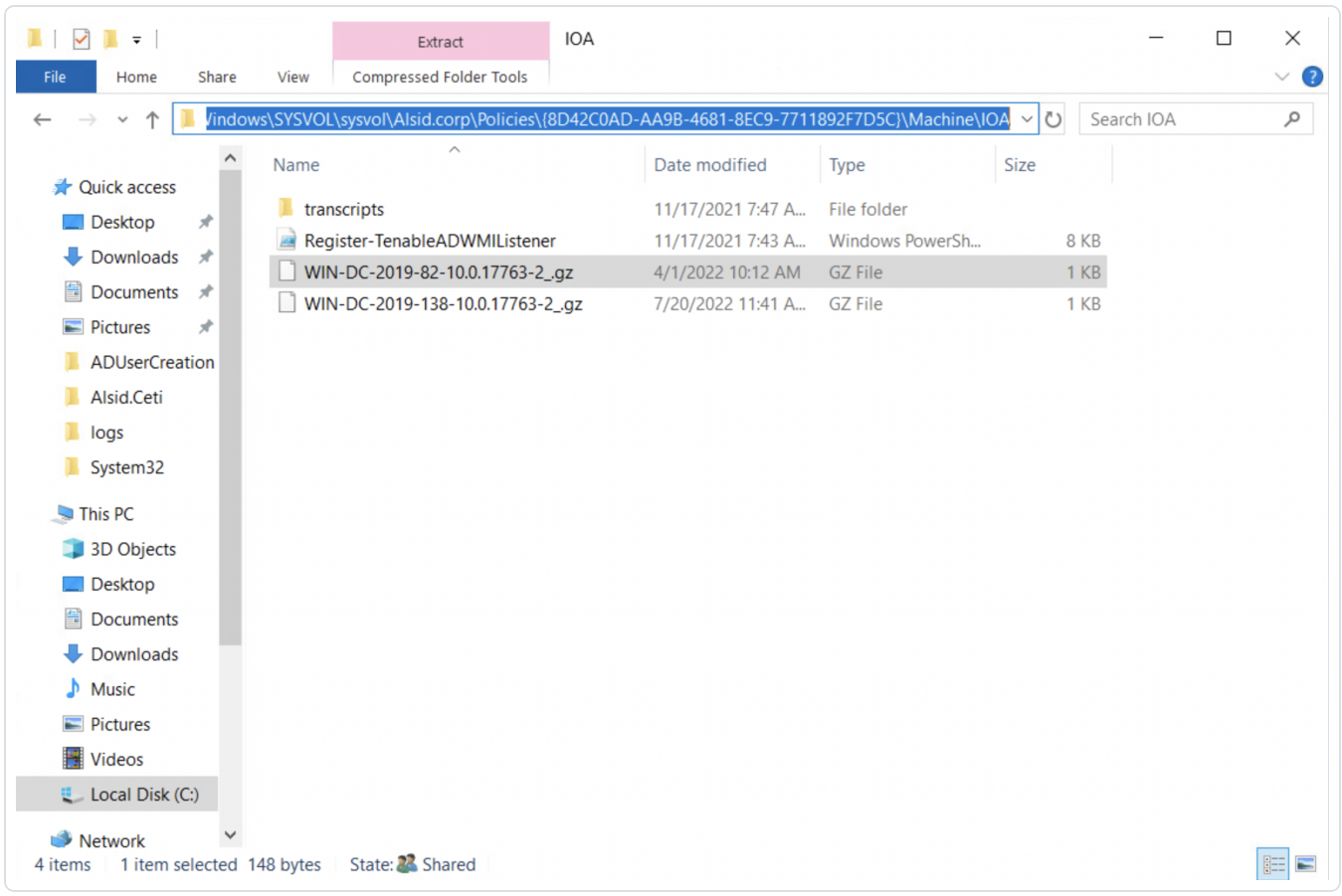
2. Cliquez sur **Enregistrer**.
    - Si vous avez activé les **mises à jour automatiques futures**, Tenable Identity Exposure enregistre et met automatiquement à jour votre nouvelle configuration. Attendez quelques minutes pour que cette mise à jour prenne effet.
    - Si vous n'avez pas activé les **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. Cliquez avec le bouton droit sur le dossier « IOA » 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 activée.

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	• Vérifiez qu'aucun autre processus que le module IoA

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.)	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.

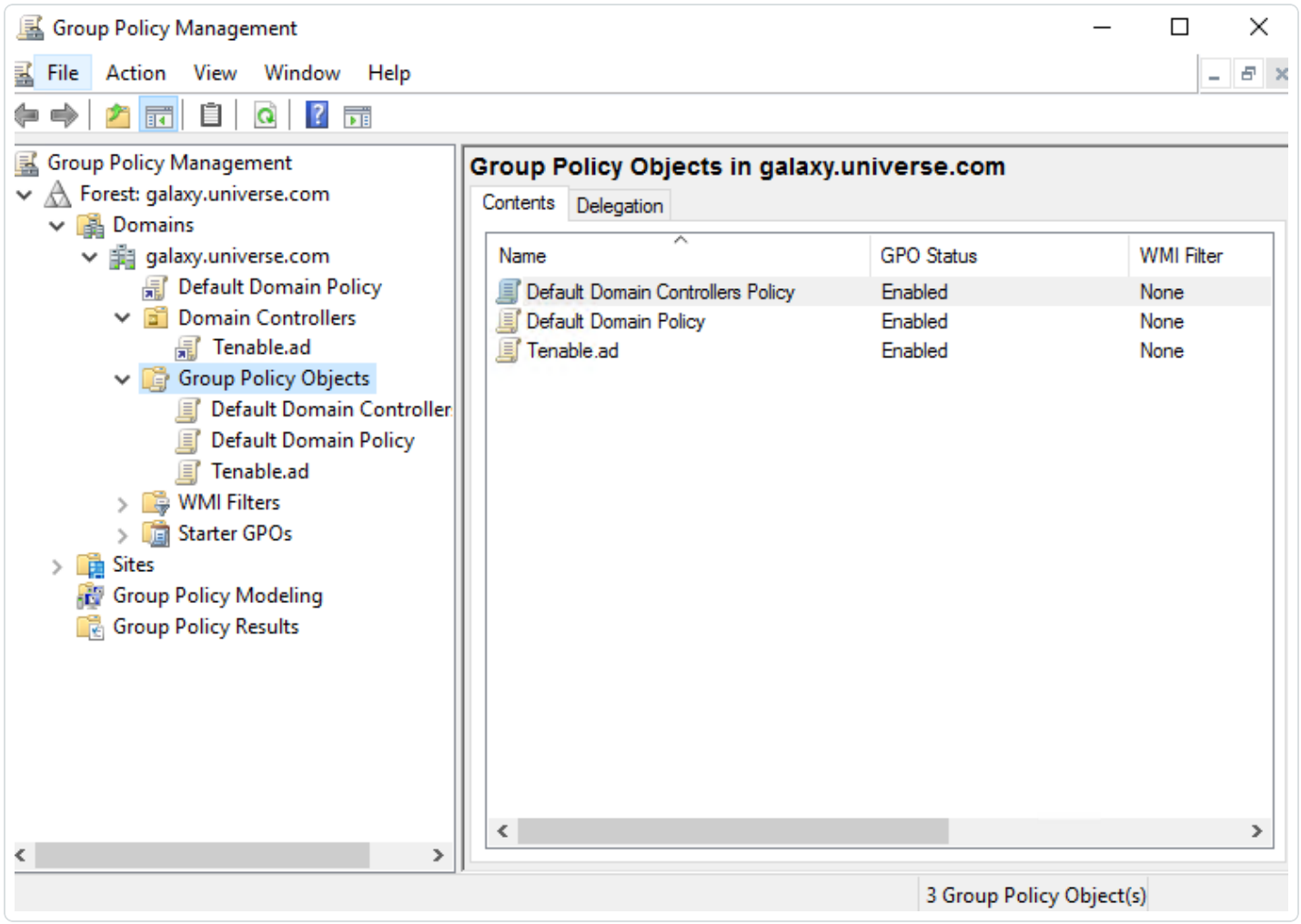
Pour plus d'informations, voir :

- 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)

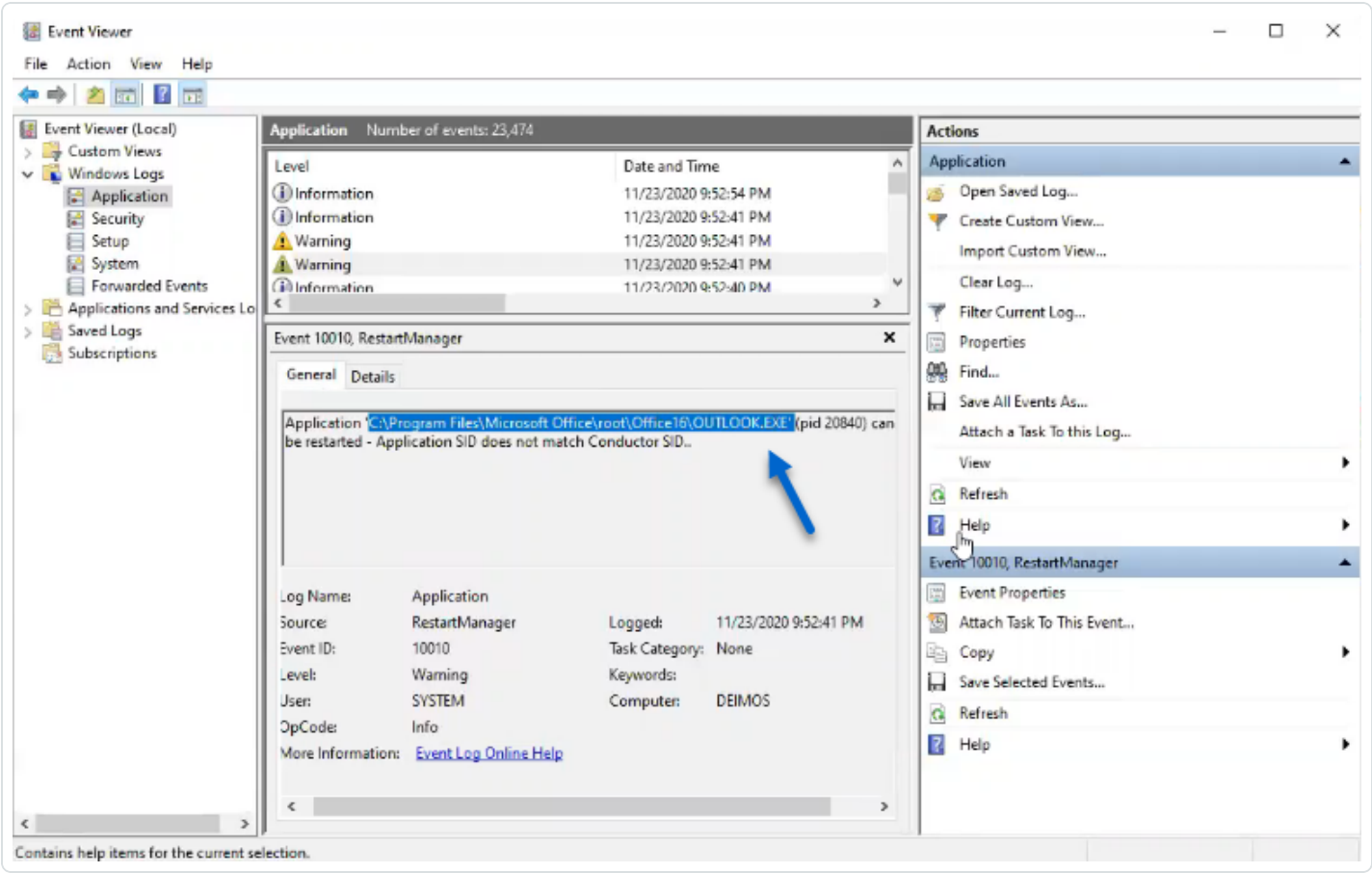
La GPO contient des scripts PowerShell que tous les DC exécutent localement pour collecter des données d'intérêt, comme suit :

- 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	Système	Chaque DC détecte la nouvelle GPO à appliquer, en

	déploiement de l'IoA de Tenable Identity Exposure sur le DC	local du DC	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<nom_DC>`).
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

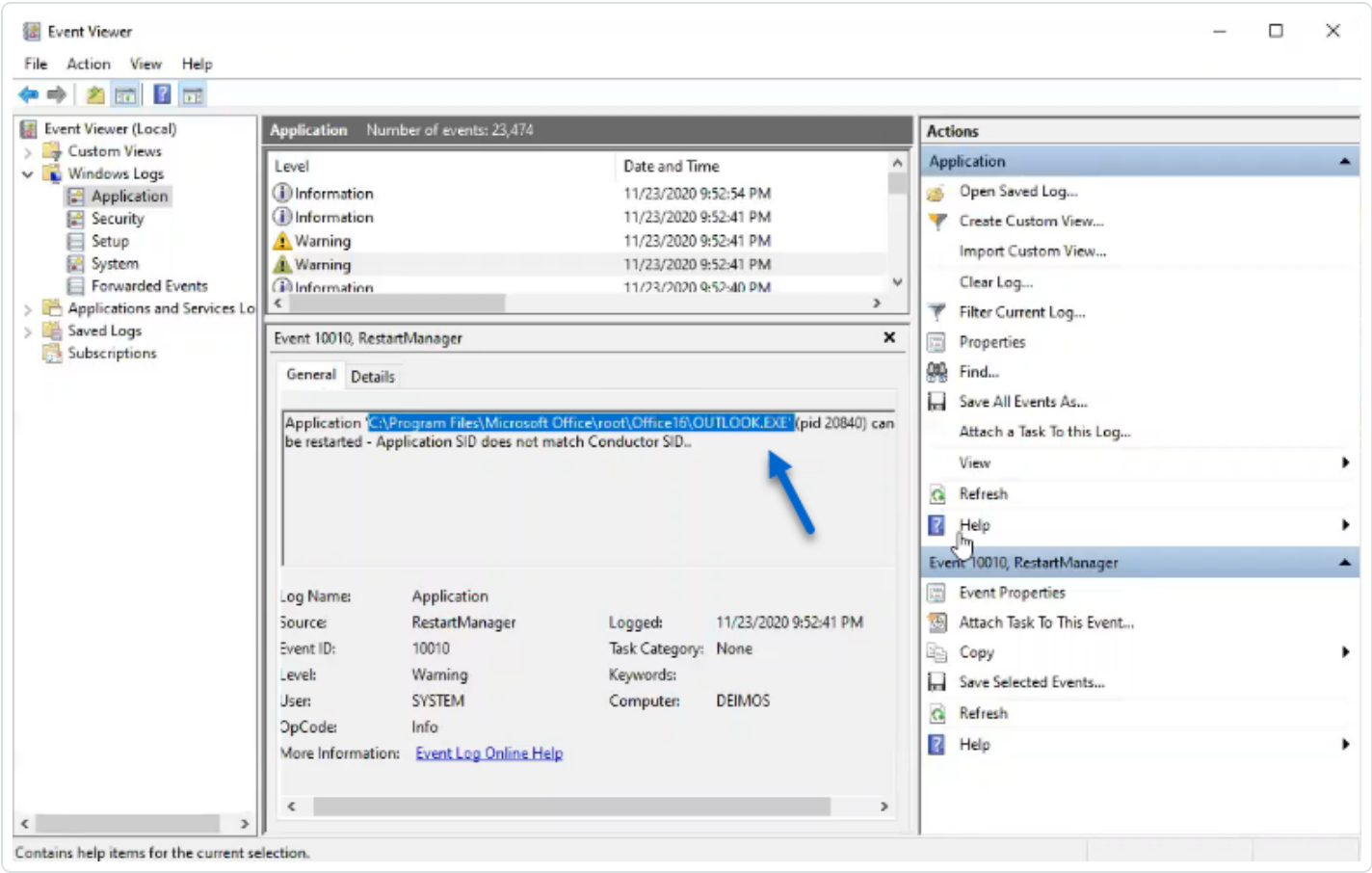
l'observateur d'événements.

- 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<nom_DC>`).

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

- Indicators of Attack and the Active Directory
- 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.

Limitation 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 :

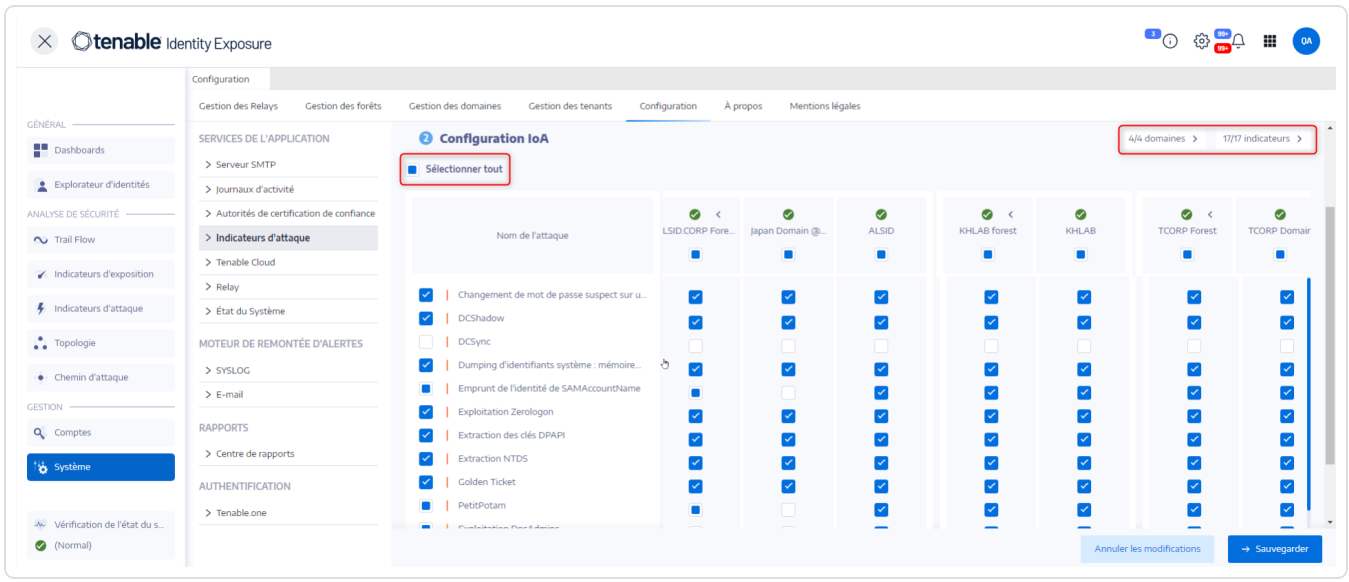
- Dans **Entités de type Données**, accès « Lecture » à :
  - Tous les indicateurs d'attaque
  - Tous les domaines
- Dans **Entités de type Interface**, accès à :
  - Gestion > Système > Configuration
  - Gestion > Système > Configuration > Services de l'application > Indicateurs d'attaque
  - Gestion > 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.

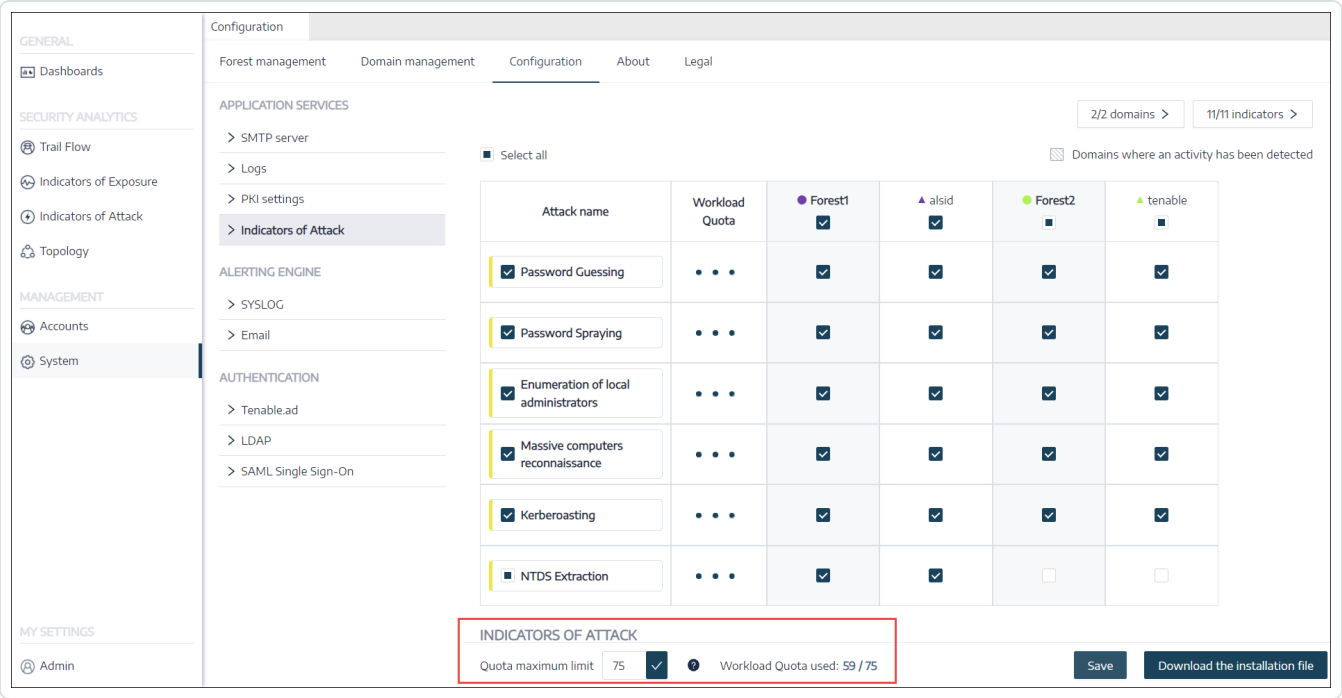
Pour modifier la limite de quota de charge de travail :

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
   ```

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

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 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
```

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
```

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

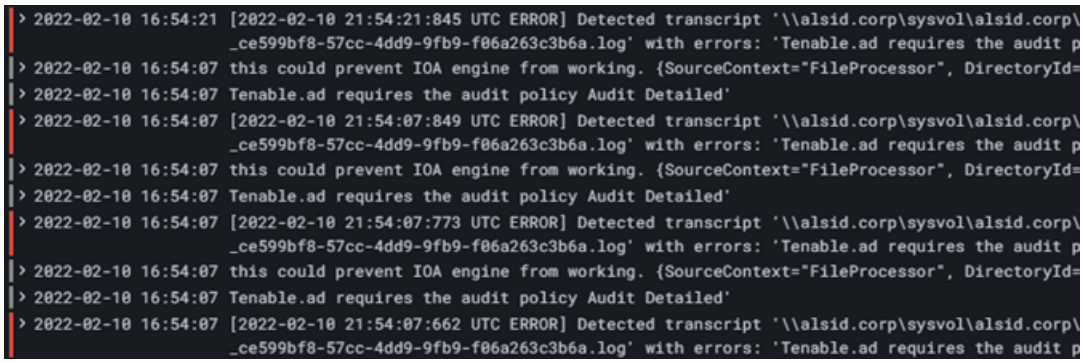
- Vérifiez le message d'erreur suivant dans le journal CETI :

```
[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"}
```

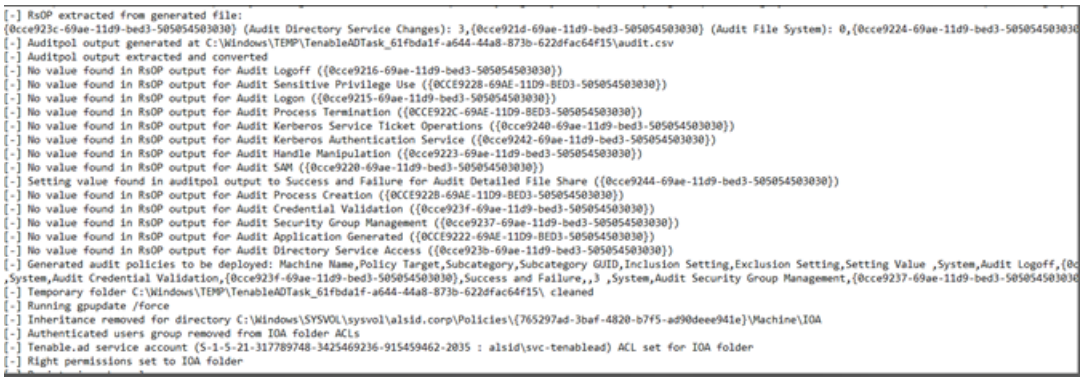
- Si vous voyez ce message, vérifiez que les paramètres GPO et le consommateur WMI sont exécutés sur le contrôleur de domaine (DC) indiqué dans le message d'erreur ci-dessus.

Paramètres d'audit

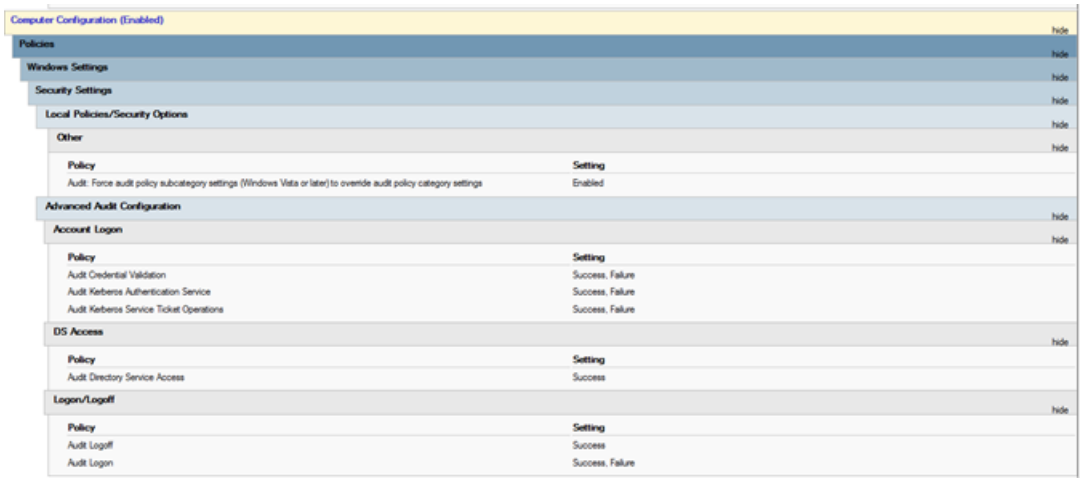
- Si vous constatez une erreur similaire à : « Tenable Identity Exposure requires the Audit Policy... » (Tenable.ad nécessite la stratégie d'audit...), vérifiez vos GPO existantes pour vous assurer que vous n'avez pas défini les stratégies d'audit requises sur « No Auditing » (Pas d'audit).



- 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

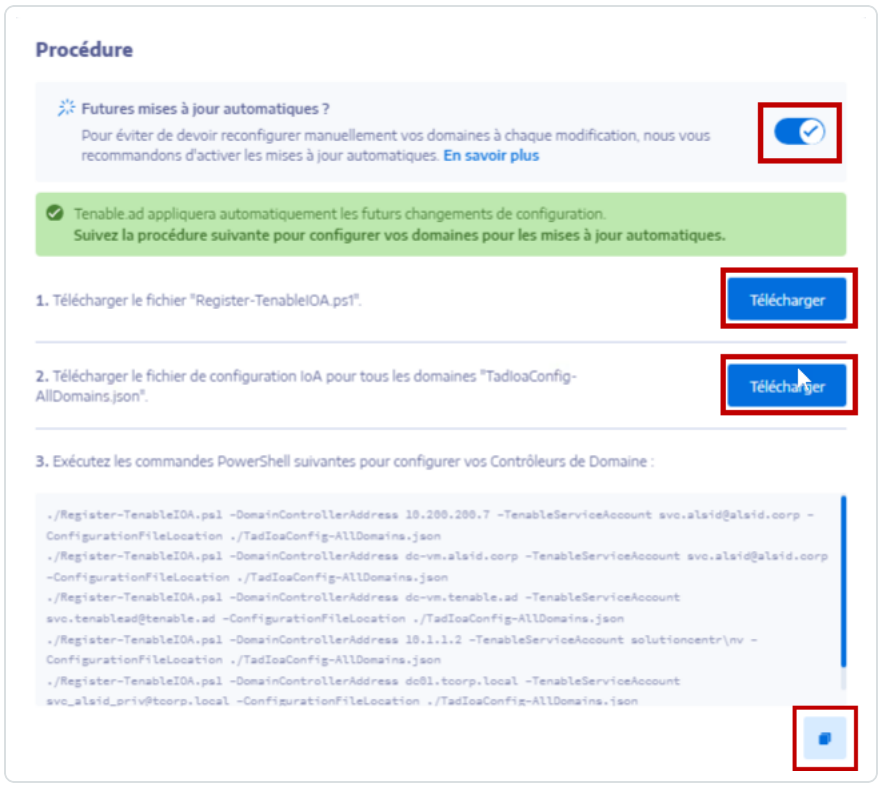
La valeur `[X]` du paramètre `-EventLogsFileWriteFrequency X` désigne l'intervalle auquel l'écouteur Tenable Identity Exposure génère un fichier de journaux d'événements sur les contrôleurs de domaine (DC) non-PDCe. La valeur par défaut et recommandée, utilisée par l'écouteur Tenable Identity Exposure, 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.

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 verrouille pas le compte après des tentatives de connexion infructueuses.	Activé
Durée de verrouillage	Durée pendant laquelle Tenable Identity Exposure empêche le compte de se connecter. Tenable Identity Exposure	300 secondes

	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.	
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 : 1. Cliquez sur le curseur pour définir une période. 2. Sélectionnez « Infinie » si vous ne souhaitez pas définir de période de	900 secondes

	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. Voir la procédure Pour ajouter un certificat d'autorités de certification (CA) de confiance pour LDAPS : 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.
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 ajouter un certificat d'autorités de certification (CA) de confiance 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**.

Pour plus d'informations sur les profils et les rôles de sécurité, voir :

- Profils de sécurité
- Rôles d'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 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 :

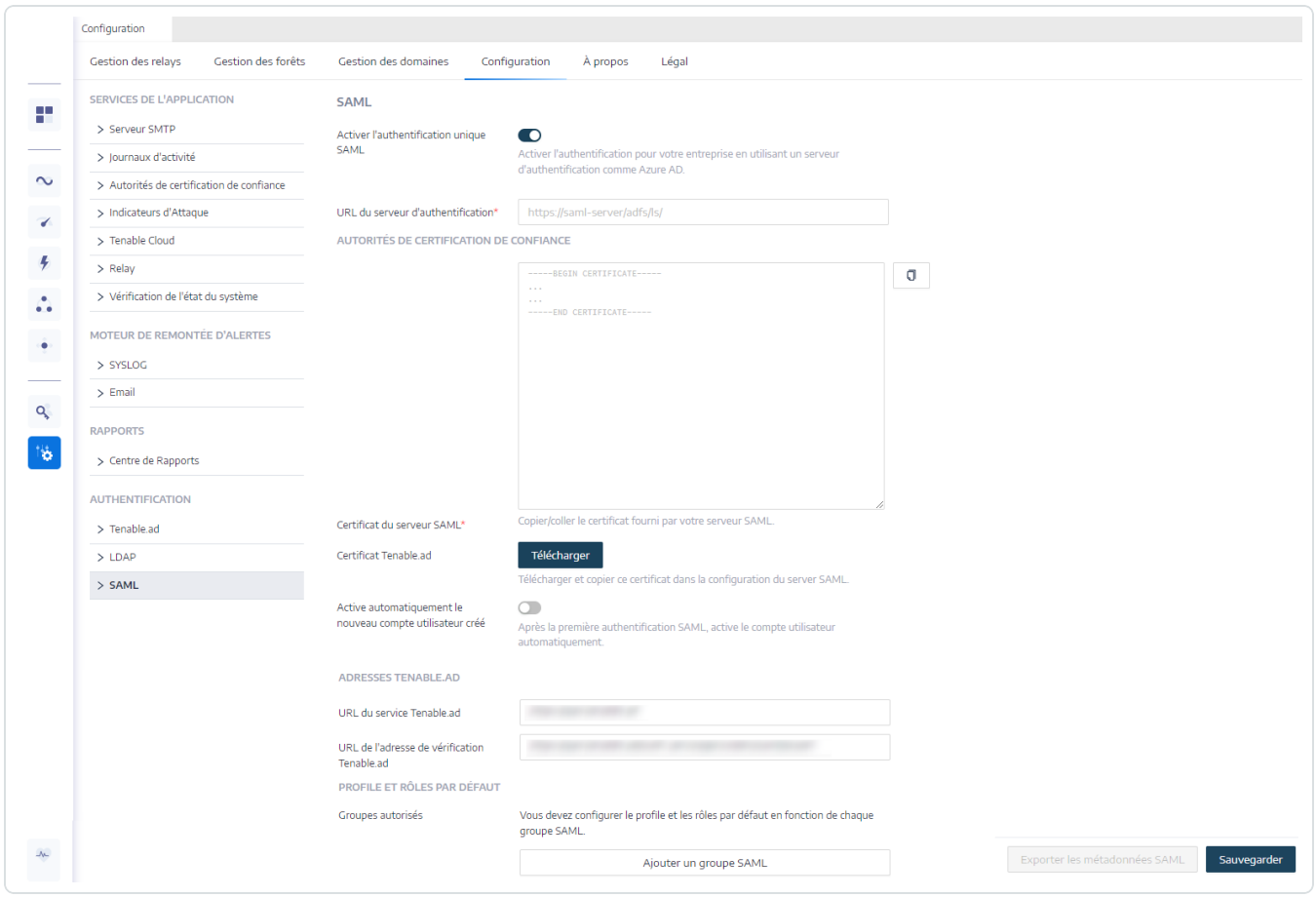
1. Dans Tenable Identity Exposure, cliquez sur **Systèmes** > **Configuration**.

   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 d'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.

Pour plus d'informations, voir :

- Créer un utilisateur
- Modifier un utilisateur
- Désactiver un utilisateur
- Supprimer un utilisateur

Créer un utilisateur

Rôle utilisateur requis : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

Remarque : les instructions suivantes s'appliquent aux instances autonomes de Tenable Identity Exposure. Pour les instances liées à Tenable Vulnerability Management, vous créez des utilisateurs dans Tenable Vulnerability Management, puis ils sont propagés à Tenable Identity Exposure.

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 **Créer**.

   Un message confirme que Tenable Identity Exposure a créé l'utilisateur avec le rôle sélectionné.

Voir aussi

- Modifier un utilisateur
- Désactiver un utilisateur
- Supprimer un utilisateur

Modifier un utilisateur

Rôle utilisateur requis : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

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.

Voir aussi

- Créer un utilisateur
- Désactiver un utilisateur
- Supprimer un utilisateur

Désactiver un utilisateur

Rôle utilisateur requis : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

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.

Voir aussi

- Créer un utilisateur
- Modifier un utilisateur
- Supprimer un utilisateur

Supprimer un utilisateur

Rôle utilisateur requis : administrateur ou utilisateur d'organisation disposant des autorisations appropriées.

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.

Voir aussi

- Créer un utilisateur
- Modifier un utilisateur
- Désactiver un 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. Personnalisez l'indicateur de manière appropriée.

Remarque : certaines options d'indicateur nécessitent d'utiliser des expressions régulières (regex). Une regex applique une correspondance de type « contient » et non pas « égale ». Par exemple : si vous donnez « `admin` » comme option d'entrée, vous pouvez mettre sur liste blanche un utilisateur répondant à « `samAccountName=admin` », mais aussi à « `samAccountName=admintoto` ».
- 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 d'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.

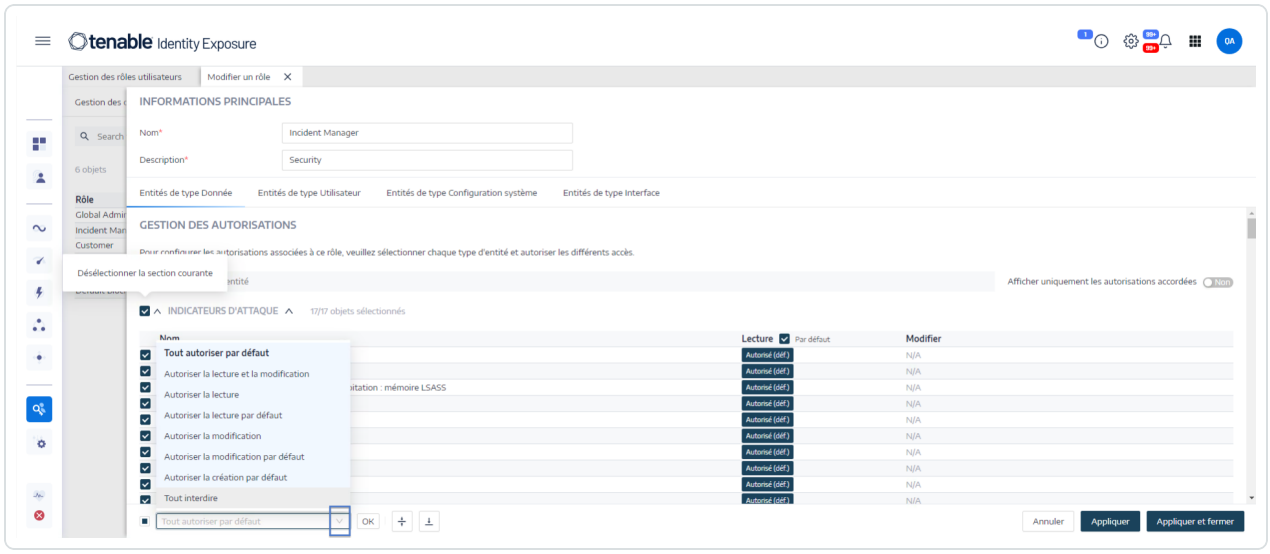
Un message confirme que Tenable Identity Exposure a mis à jour le rôle.

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 dans Tenable Identity Exposure.	• Indicateurs d'attaque • Indicateurs d'exposition • Forêts • Domaines • Profils • Utilisateurs • Alertes par e-mail • Alertes par Syslog • Rôles • Entité Relay • Rapports	Lire, Modifier, Créer
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 • 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	Lire, Modifier

	• Service Tenable Cloud (Collecte de données via Tenable Cloud) • Support 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 d'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 :

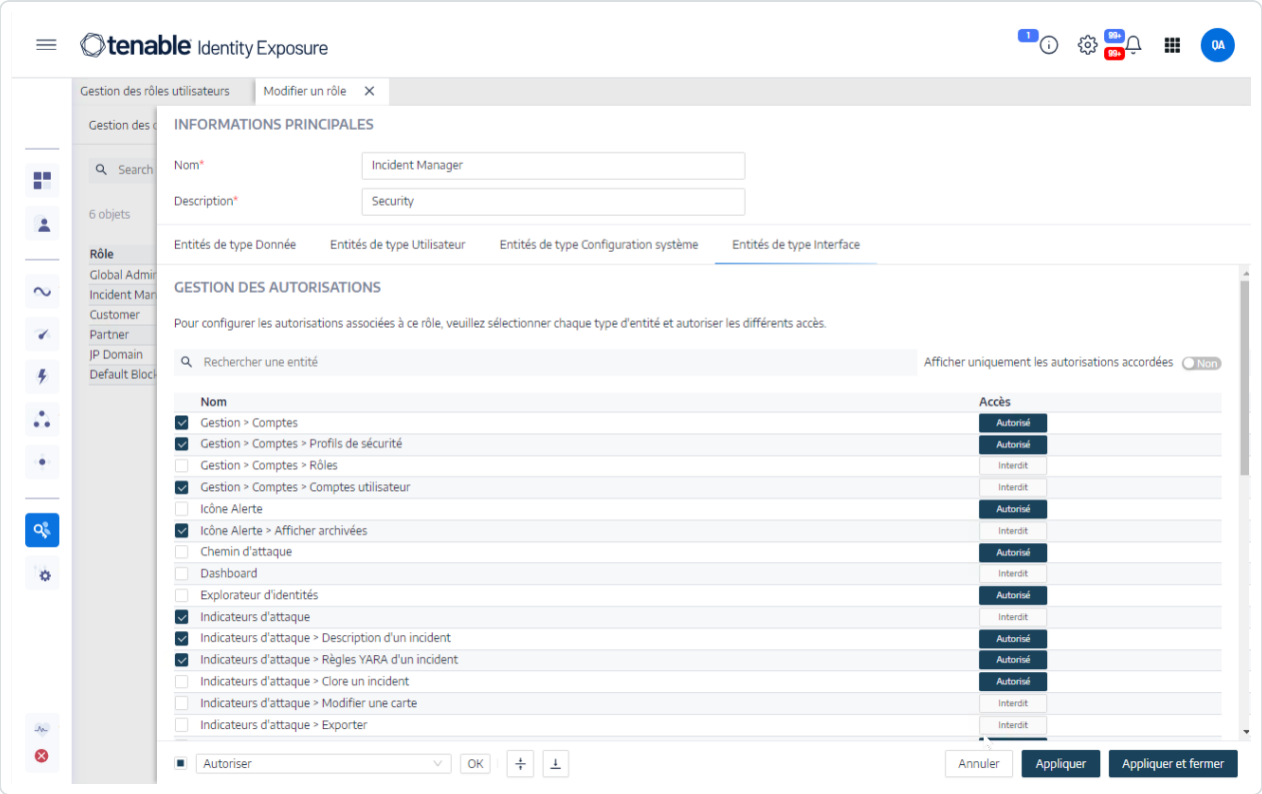
- Configuration système : **Gestion** > **Système**
- Paramètres de configuration : **Gestion** > **Système** > **Configuration**
- Alertes Syslog : **Gestion** > **Système** > **Configuration** > **Moteur de remontée d'alertes** > **SYSLOG**

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**.

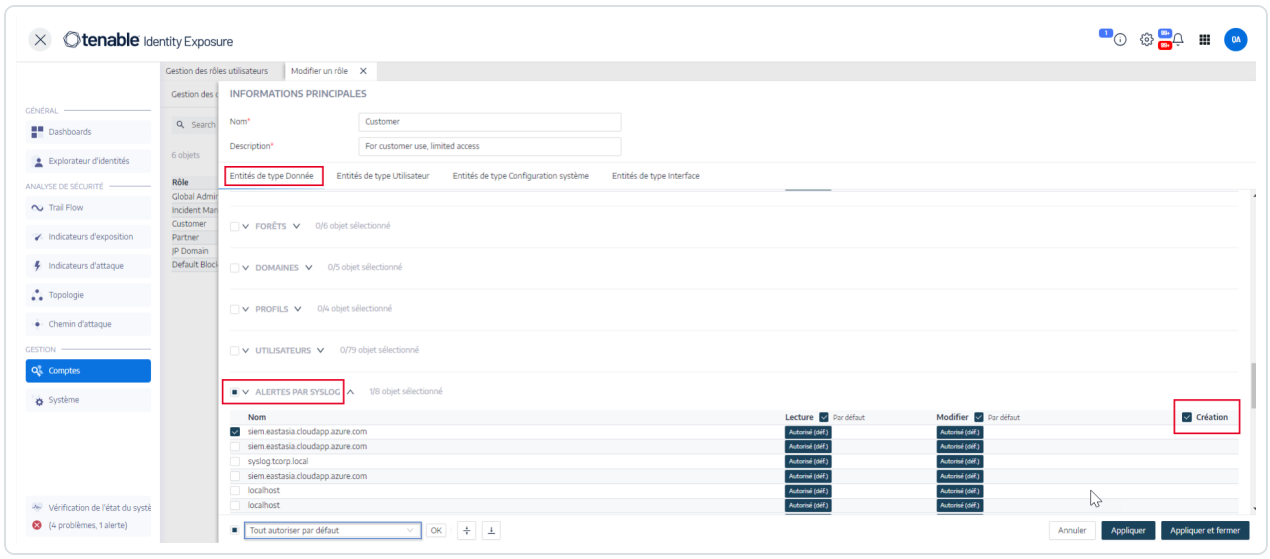
   Un message confirme que Tenable Identity Exposure a mis à jour les autorisations sur les entités.



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.


tenable Identity Exposure
Gestion des rôles utilisateurs
Modifier un rôle
INFORMATIONS PRINCIPALES
Nom*
Customer
Description*
For customer use, limited access
Entités de type Donnée
Entités de type Utilisateur
Entités de type Configuration système
Entités de type Interface
FORÊTS
DOMAINES
PROFILS
UTILISATEURS
ALERTES PAR SYSLOG
Nom
Lecture
Modifier
Création
siem.eastasia.cloudapp.azure.com
syslog.tcorp.local
localhost
Tout autoriser par défaut
Annuler
Appliquer
Appliquer et fermer

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 : échec de la pré-authentification Kerberos »* : 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
```

Où `<AD_ACCOUNT>` est le nom du compte Active Directory à modifier.

Domaines

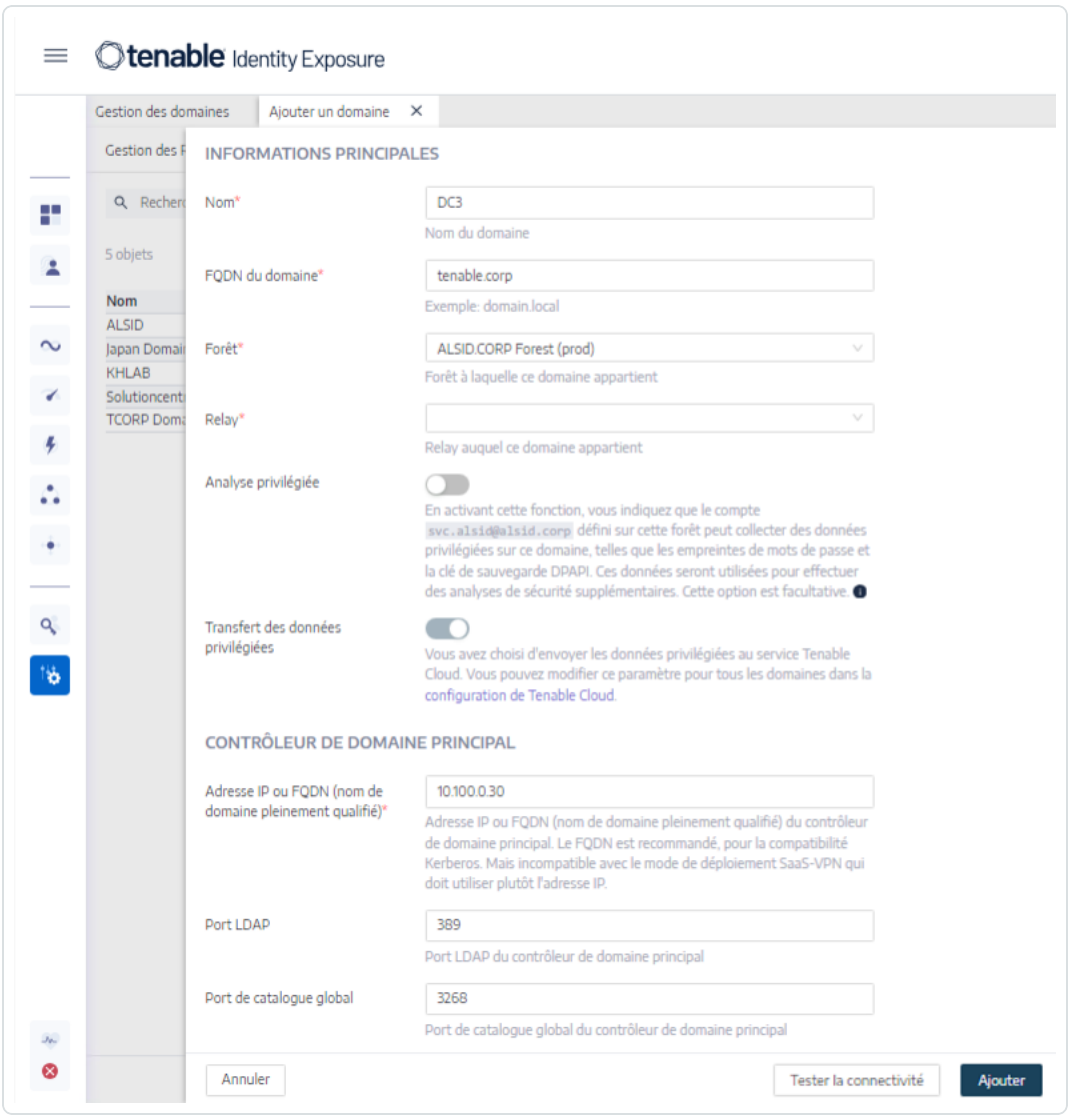
Tenable Identity Exposure surveille les domaines qui regroupent les objets partageant des paramètres communs de manière logique pour une gestion centralisée.

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 :

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.
5. Cliquez sur **Supprimer**.

   Un message confirme que Tenable Identity Exposure a supprimé le domaine.

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.

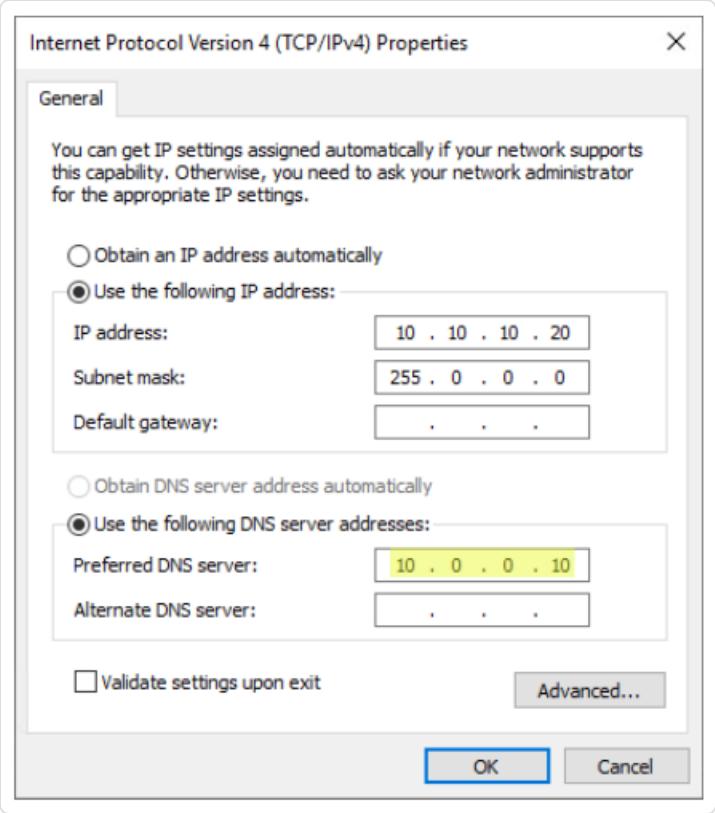
L'utilisation de NTLM au lieu de Kerberos est également la raison pour laquelle le durcissement SYSVOL interfère avec Tenable Identity Exposure. Pour plus d'informations, voir Interférence du durcissement SYSVOL avec Tenable Identity Exposure.

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	Oui
SaaS avec VPN	Non — Vous devez faire passer l'installation en mode de déploiement Secure Relay.

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.

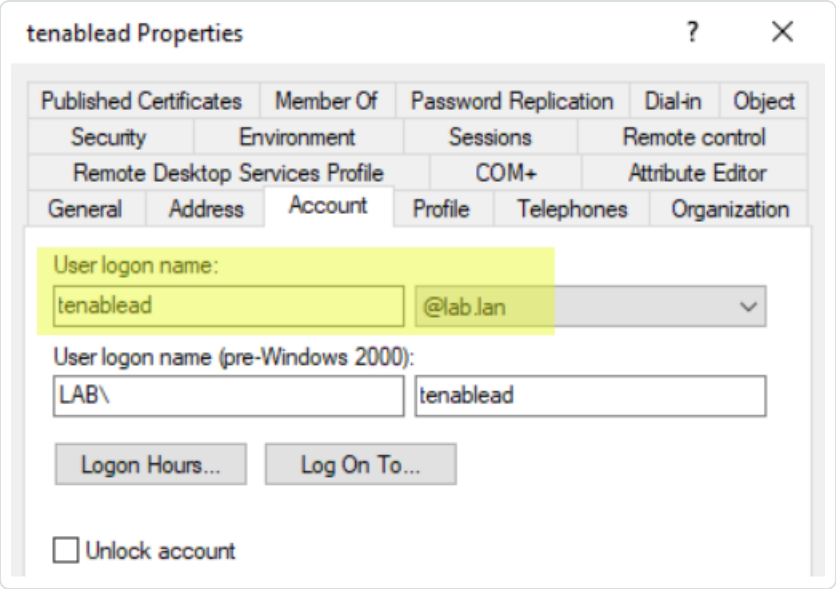
Pour plus d'informations sur les exigences, voir Matrice de flux réseau et Matrice réseau TLS.

> **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 :



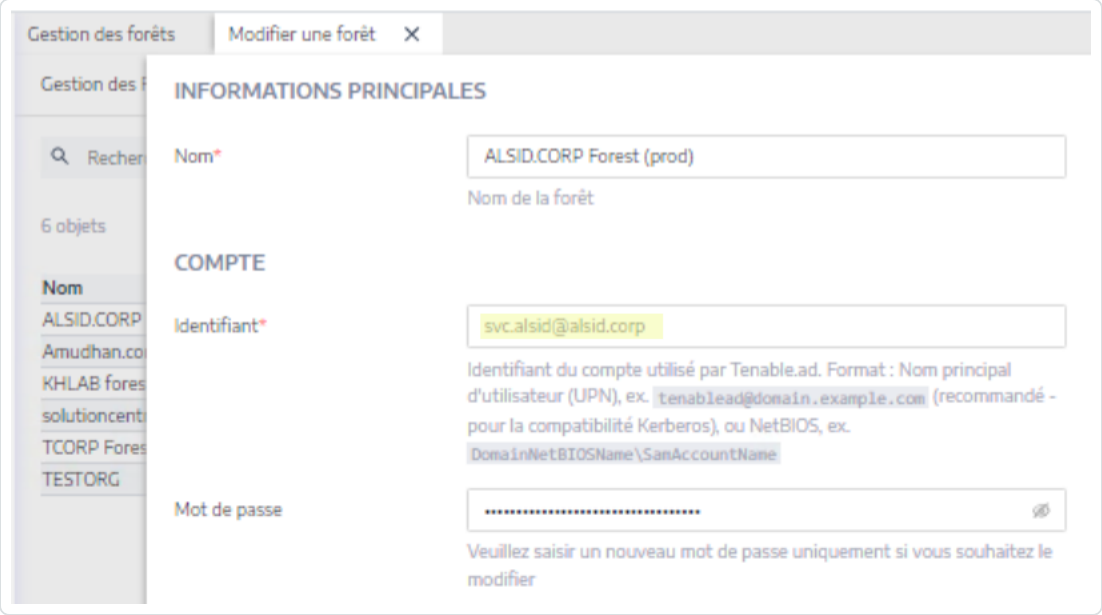

```
PS C:\Users\admin> Get-ADUser tenablead


DistinguishedName : CN=tenablead,CN=Users,DC=lab,DC=lan
Enabled           : True
GivenName         : tenablead
Name              : tenablead
ObjectClass       : user
ObjectGUID        : 70020328-b176-40d0-8a79-7948c1d4cb74
SamAccountName    : tenablead
SID               : S-1-5-21-1891480667-311803191-3341389180-22602
Surname           :
UserPrincipalName : tenablead@lab.lan
```

> **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.

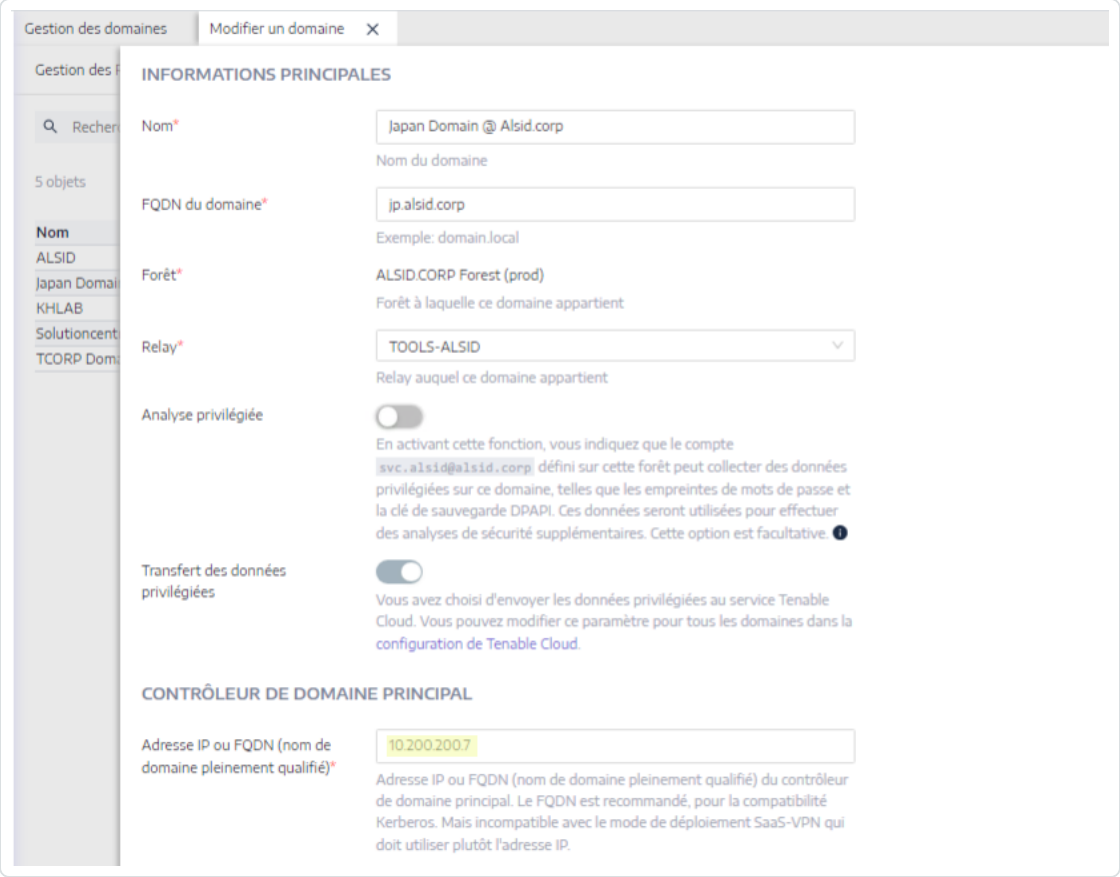
b. Dans la section de configuration de la forêt de Tenable Identity Exposure, définissez cet UPN au lieu du format court « `nom d'utilisateur` » ou du format NetBIOS

« `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.

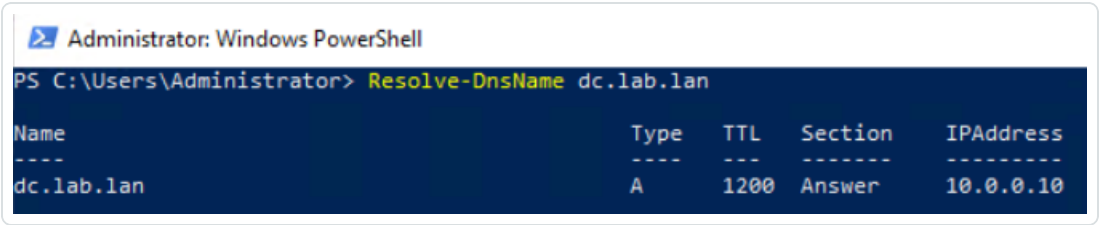


Résolution des problèmes

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

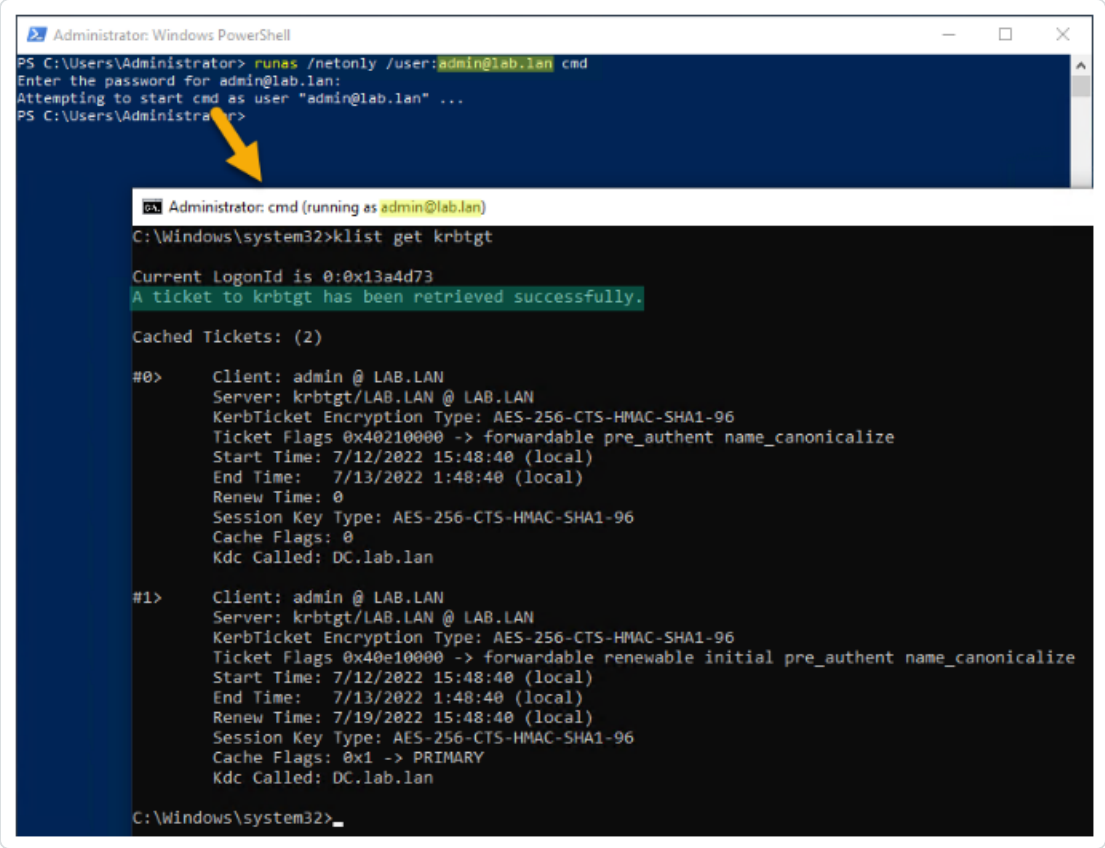
Pour vérifier que Kerberos fonctionne avec les commandes que vous exécutez sur le Directory Listener ou la machine Relay :

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 :

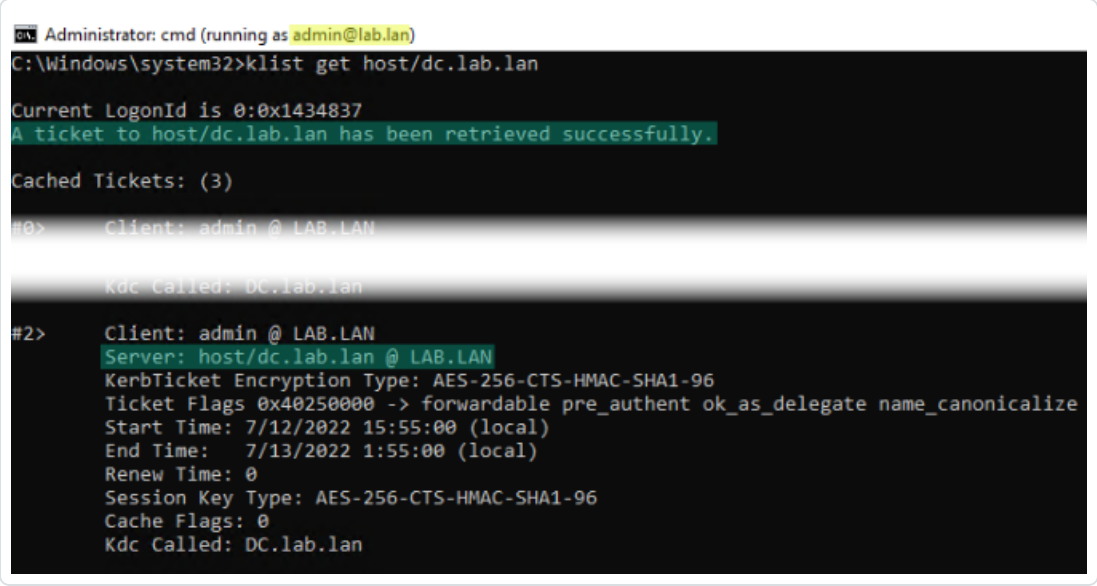


    Voici les codes d'erreur potentiels :

- `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

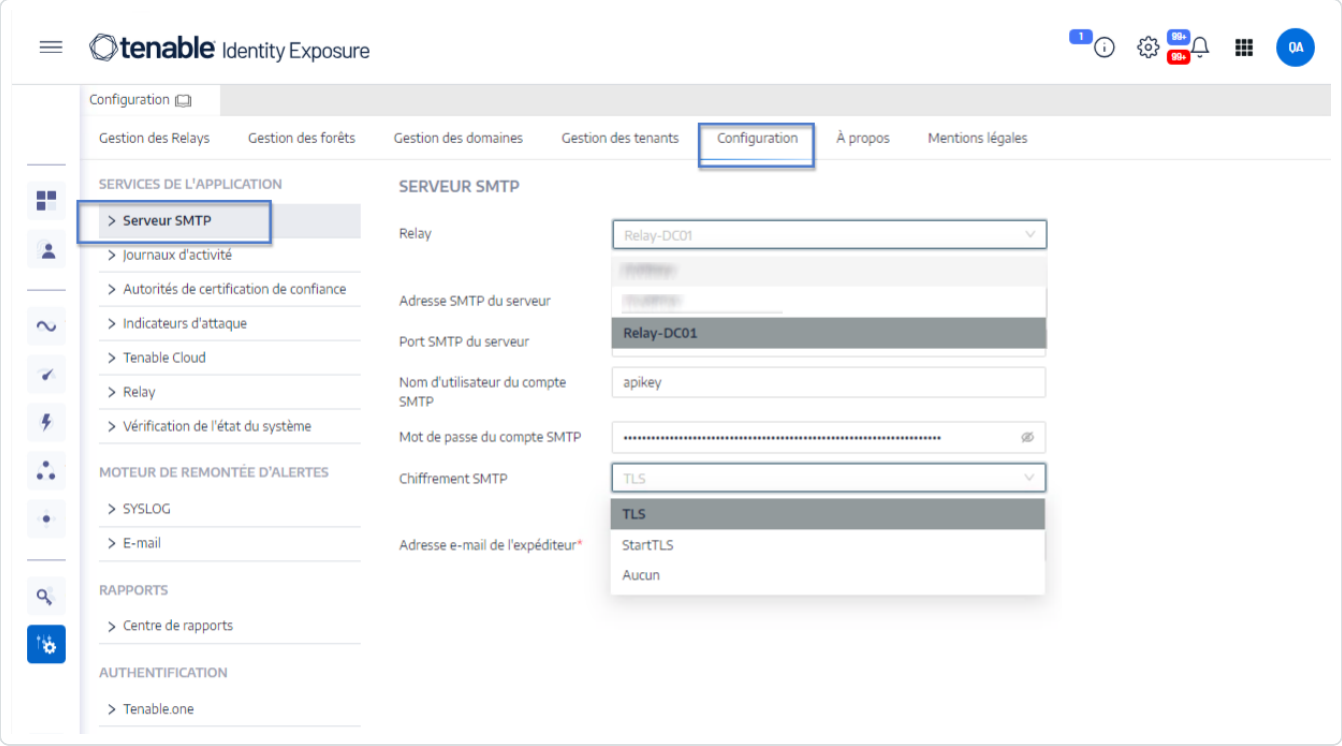
Configuration de serveur SMTP

Tenable Identity Exposure nécessite de configurer le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des notifications d'alerte.

Pour configurer le serveur SMTP :

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

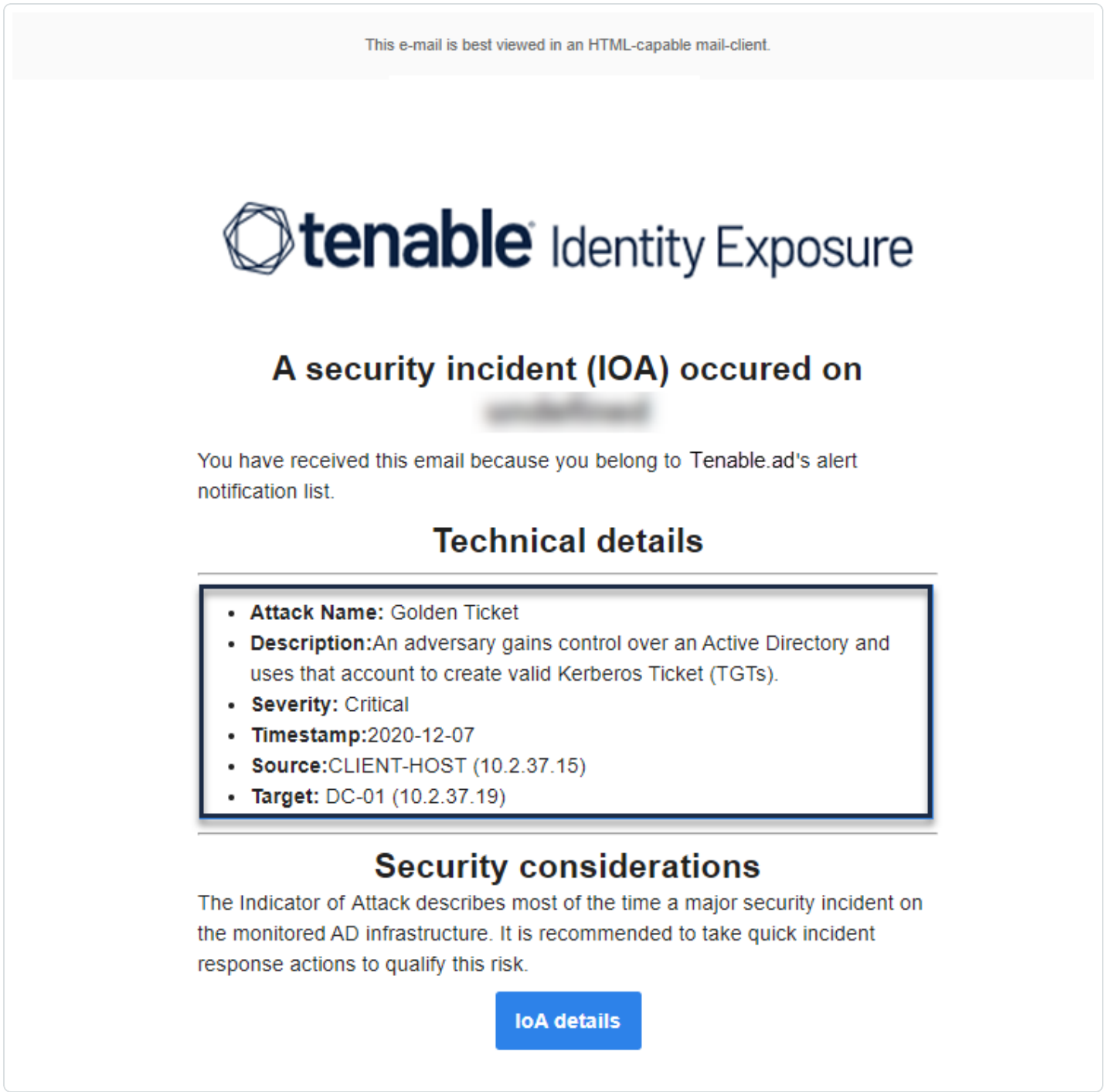
- Nom d'utilisateur du compte SMTP
- Mot de passe du compte SMTP

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.

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 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

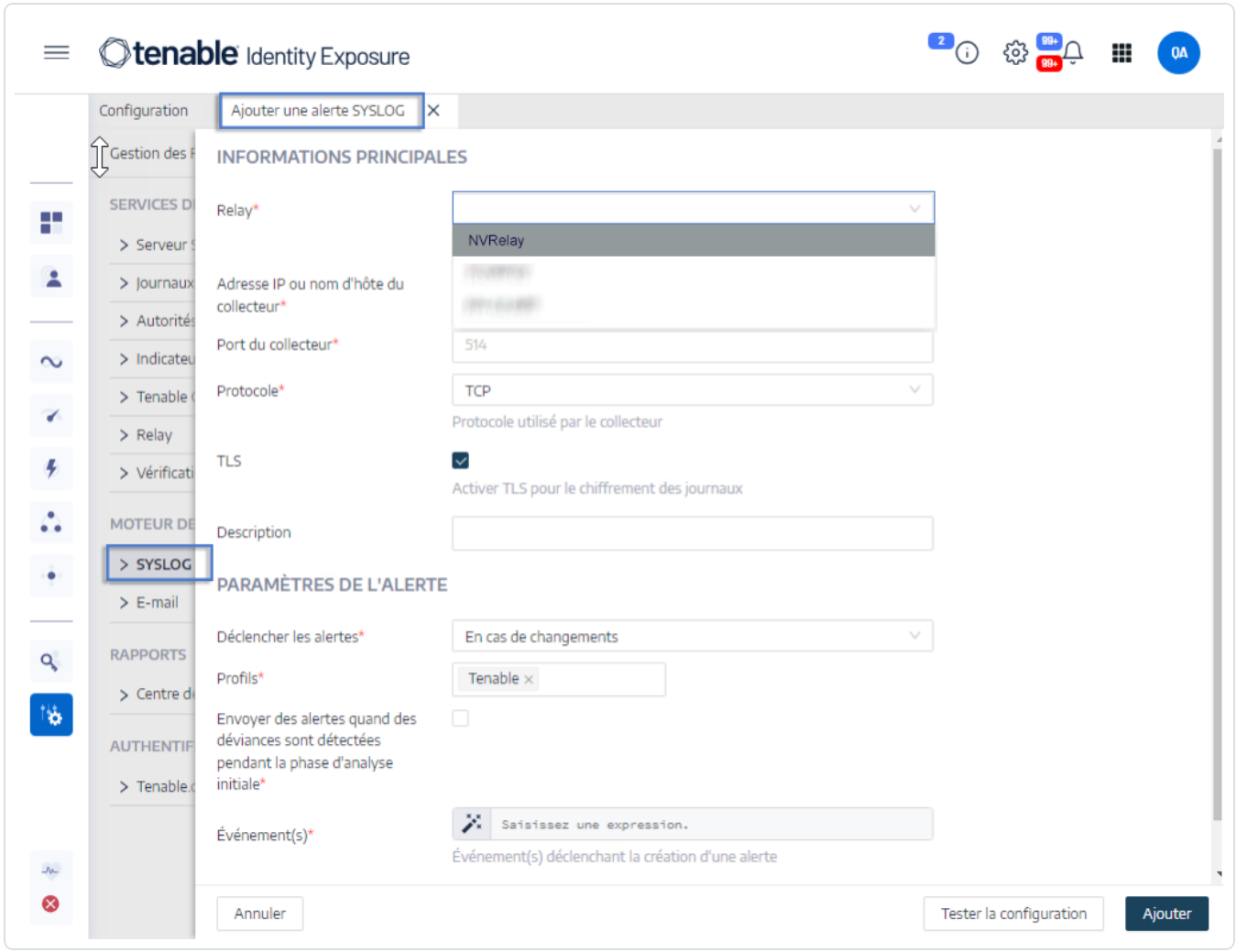
Alertes Syslog

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 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 :
    - **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.
    - **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 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.

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"
```

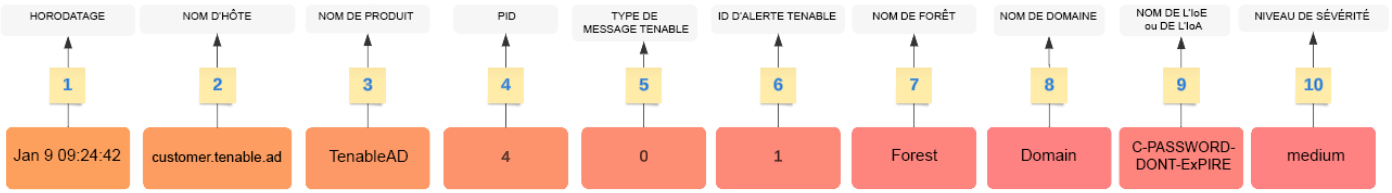
Exemple d'alerte pour un indicateur d'attaque (IoA)

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

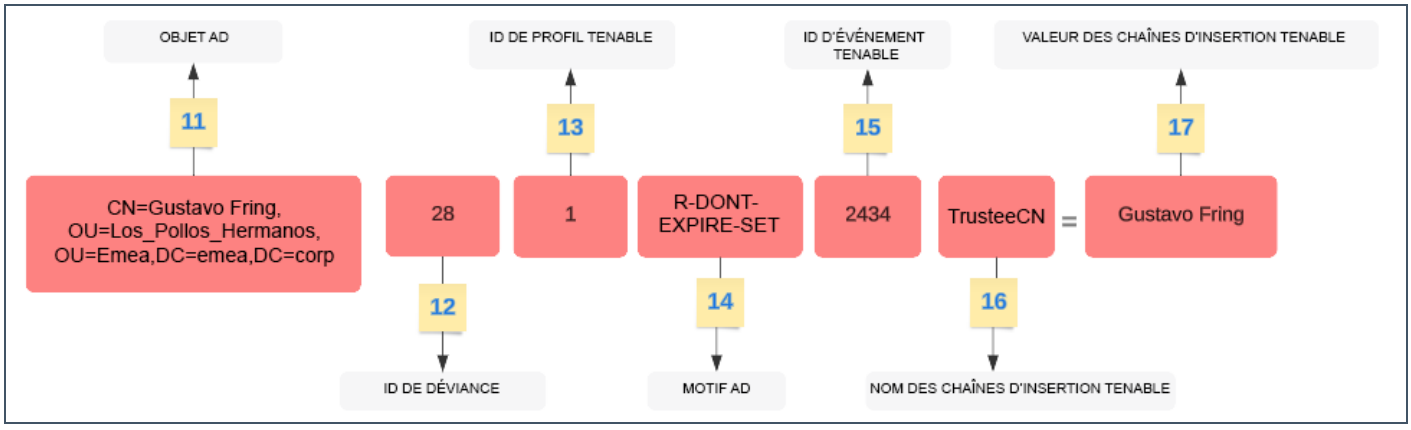


La structure d'en-tête comprend les éléments suivants, comme décrit dans le tableau.

Élément	Description

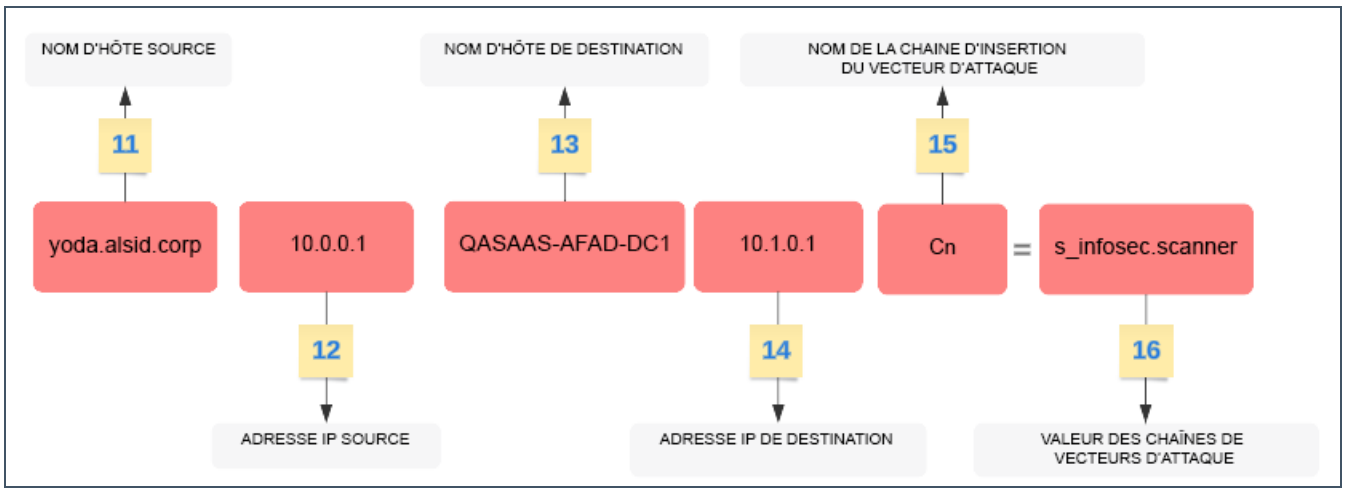
1	**Horodatage** — Date de la détection. Exemple : « 7 juin 05:37:03 »
2	**Nom d'hôte** — Nom d'hôte de votre application. Exemple : « customer.tenable.ad »
3	**Nom du produit** — Nom du produit qui a déclenché la déviance. Exemple : « TenableAD », « AutreProduitTenableAD »
4	**PID** — ID (Tenable Identity 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)
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

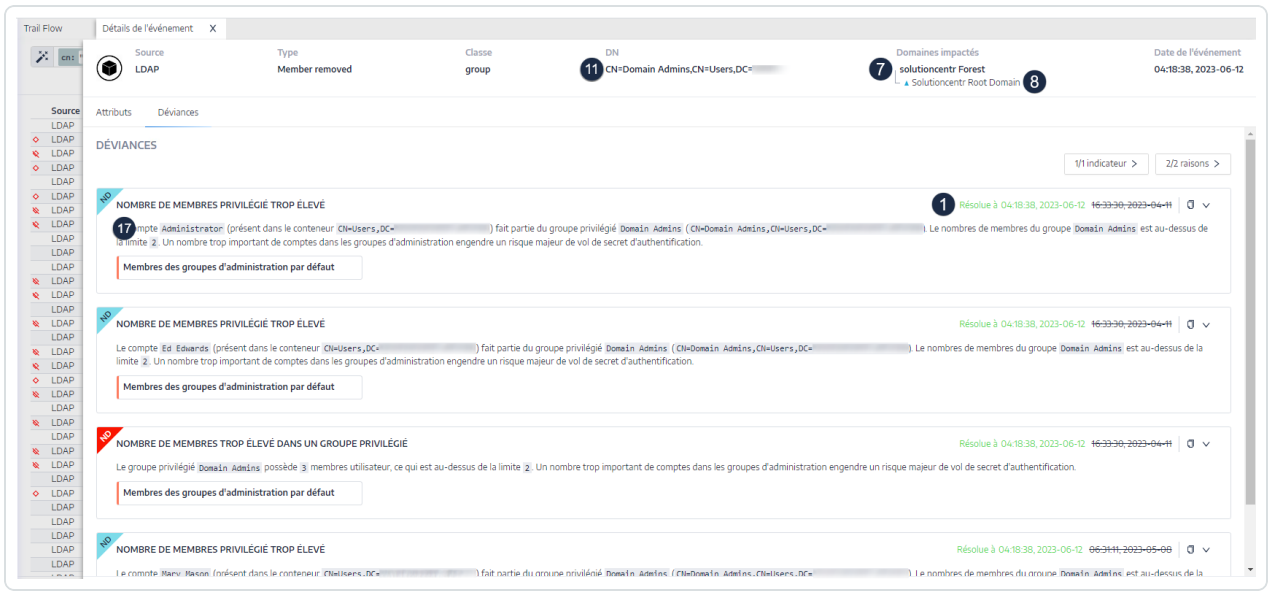
11	**Nom d'hôte source** — Nom de l'hôte attaquant. La valeur peut également être « Inconnue ».
12	**Adresse IP source** — Adresse IP de l'hôte attaquant. Les valeurs peuvent être IPv4 ou IPv6.
13	**Nom d'hôte de destination** — Nom de l'hôte attaqué.
14	**Adresse IP de destination** — Adresse IP de 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.

Examples

Détails de l'événement Trail Flow

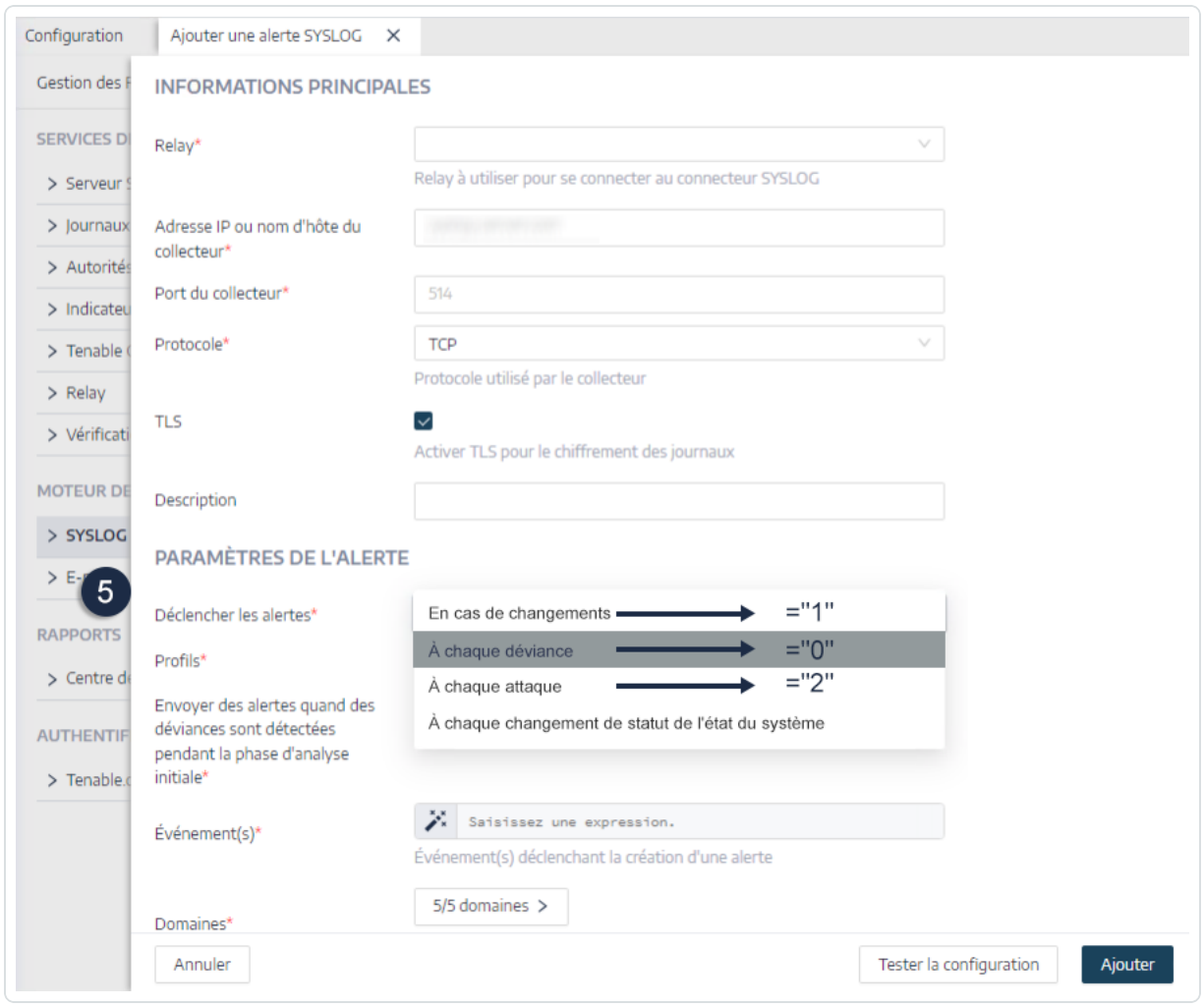
L'exemple suivant montre les détails d'un événement dans le Trail Flow contenant les éléments suivants :

- 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

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 fonctionnelle au port RPC dynamique, 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.

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.

Nom de la vérification de l'état du système	Type	Description de la vérification	Raisons
Accessibilité du domaine	Domaine	Possibilité d'établir une connexion avec le domaine AD.	• `IP-UNREACHABLE` • `R-LDAP-GLOBAL-CATALOG-UNREACHABLE` • `LDAP-SERVER-UNREACHABLE` • `SMB-SERVER-UNREACHABLE` • `DYNAMIC-RPC-CONNECTION-NOT-WORKING` • `RPC-CONNECTION-NOT-WORKING`
Authentification au	Domaine	Possibilité de	• `INCORRECT-`

domaine AD		s'authentifier au domaine AD	CREDENTIALS • LDAP-SERVER-BUSY • LDAP-SERVER-UNAVAILABLE • LDAP-SERVER-ACCESS-DENIED • SMB-SERVER-ACCESS-DENIED
Autorisations de collecter les données du domaine	Domaine	Possibilité de collecter les données du domaine AD	• MISSING-PERMISSIONS-PRIVILEGED-DATA
Autorisations d'accéder aux conteneurs AD	Domaine	Possibilité d'accéder aux conteneurs AD	• MISSING-PERMISSIONS-DELETED-OBJECTS-ACCESS • MISSING-PERMISSIONS-PASSWORD-SETTINGS-ACCESS
Domaine AD lié à un Relay	Domaine	Le domaine est lié à un Relay.	• LINKED-TO-RELAY-DOWN
Fonctionnement du Service Relay	Plateforme	Le Relay fonctionne comme prévu	• RELAY-DOWN
Version du	Plateforme	La version du	• VERSION-

Service Relay		Relay est alignée avec celle du produit.	`MISMATCH`
Fonctionnement du collecteur de données AD	Plateforme	Le collecteur de données AD fonctionne comme prévu	• `DATA-COLLECTOR-SERVICE-DOWN` • `DATA-COLLECTOR-BRIDGE-DOWN` • `BROKER-DOWN`

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**.

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.

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.

Pour créer un rapport :

1. Dans le volet **Centre de rapports**, cliquez sur **Créer un rapport**.

   Le volet **Configuration du rapport** apparaît.
2. Sous **Type de rapport**, saisissez les informations suivantes :

a. Dans **Type de rapport**, sélectionnez **Déviances** ou **Attaques**.

b. Dans **Indicateurs**, cliquez sur **n/n indicateurs** pour sélectionner **Indicateurs d'exposition** (pour les déviances) ou **Indicateurs d'attaque** (pour les attaques) et cliquez sur **Filtrer sur la sélection**.

c. Dans **Domaines**, cliquez sur **n/n domaines** pour sélectionner les forêts ou les domaines du rapport et cliquez sur **Filtrer sur la sélection**.

d. Dans **Profils**, cliquez sur la flèche pour sélectionner un profil dans le menu déroulant.

3. Dans **Nom du rapport**, saisissez le nom du rapport.
4. Sous **Paramètres de génération**, sélectionnez les paramètres suivants :

   a. **Période des données** — Le rapport couvre la période qui précède la période actuelle, à savoir le jour, la semaine, le mois ou le trimestre précédents.

   b. **Récurrence** — Tenable Identity Exposure génère un nouveau rapport pour chaque période que vous définissez : cliquez sur la flèche pour sélectionner les valeurs correspondantes dans le menu déroulant.

   c. **Fuseau horaire** — Fuseau horaire du rapport.

5. Sous **Destinataires**, cliquez sur **Ajouter des adresses e-mails** et saisissez l'adresse e-mail des destinataires. Vous pouvez ajouter autant de destinataires que nécessaire.

   Pour plus d'informations sur la configuration des adresses e-mails des destinataires des rapports, voir Configuration de serveur SMTP

6. Cliquez sur **Créer un rapport**.

Pour autoriser les utilisateurs à télécharger un rapport :

- En haut du volet **Centre de rapports**, sous **Clé d'accès aux rapports**, cliquez sur pour copier la clé. Cette clé d'accès est requise pour télécharger le rapport à partir du lien figurant dans l'e-mail envoyé au destinataire. Elle est unique pour tous les utilisateurs et tous les rapports.
- Si nécessaire, cliquez sur pour générer une nouvelle clé d'accès.

  Attention : la génération d'une nouvelle clé d'accès rend la clé d'accès précédente inutilisable. Seule la nouvelle clé d'accès peut donner accès aux rapports existants.

Pour modifier la configuration d'un rapport :

1. Dans la liste des rapports, sélectionnez un rapport et cliquez sur à la fin de la ligne pour ouvrir le volet **Configuration du rapport**.
2. Modifiez selon vos besoins.
3. Cliquez sur **Enregistrer**.

Pour supprimer un rapport :

1. Dans la liste des rapports, sélectionnez un rapport et cliquez sur à la fin de la ligne pour le supprimer.

   Un message demande de confirmer la suppression.
2. Cliquez sur **Supprimer**.

   Le dernier rapport généré associé à cette configuration de rapport n'est plus disponible au téléchargement.

Pour accorder des autorisations à des rôles :

- Dans **Gestion des autorisations**, sous **Entités de données** > **Rapports**, les administrateurs peuvent accorder des autorisations à des rôles utilisateur pour créer, lire ou modifier toutes les configurations de rapports ou des configurations spécifiques.

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

Voir aussi

- Widgets

Support 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 devez disposer d'un **compte Tenable Vulnerability Management** pour utiliser la fonctionnalité de support Microsoft Entra ID. Ce compte vous permet de configurer des scans Tenable pour votre Microsoft Entra ID et de collecter les résultats de ces scans.

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. Elle collecte ces données en utilisant l'API Microsoft Graph et des identifiants des principaux de service en suivant les 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.

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) ».

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.

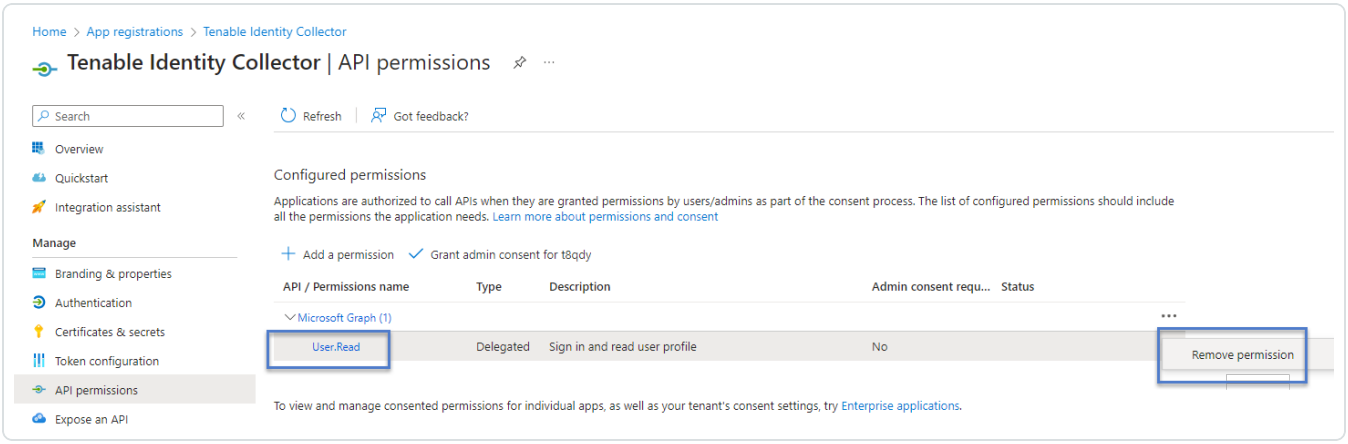
3. **Attribuer des autorisations à l'application :**

a. Dans le portail d'administration Azure, ouvrez la page **Inscriptions d'application**.

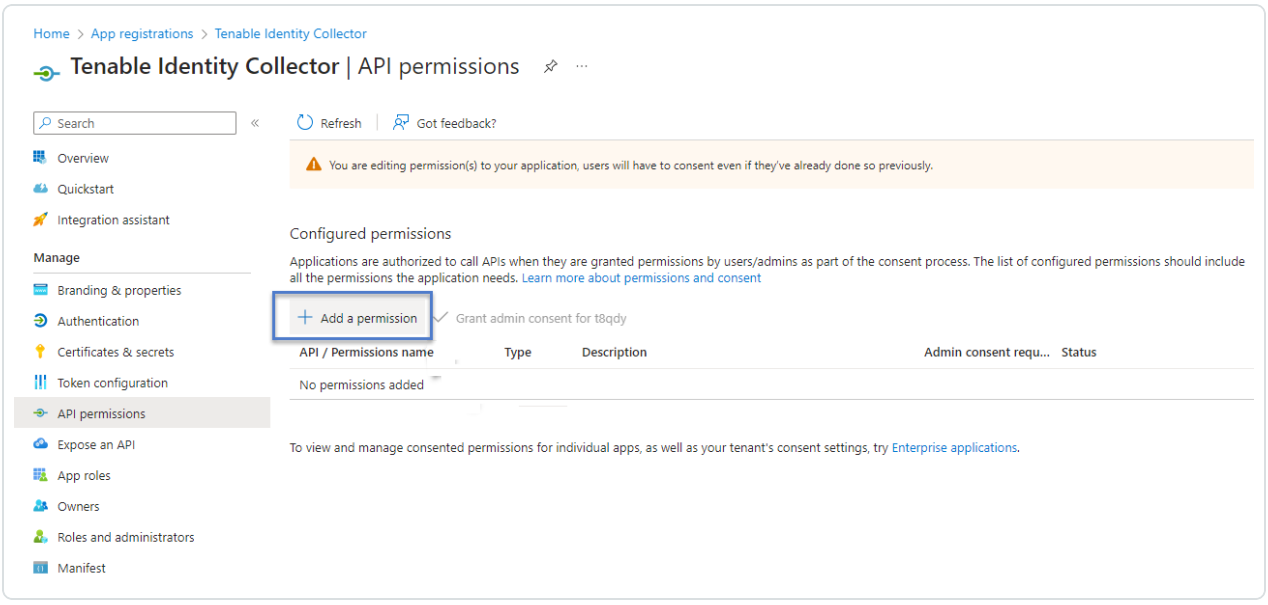
b. Cliquez sur l'application que vous avez créée.

c. Dans le menu de gauche, cliquez sur **Autorisations des API**

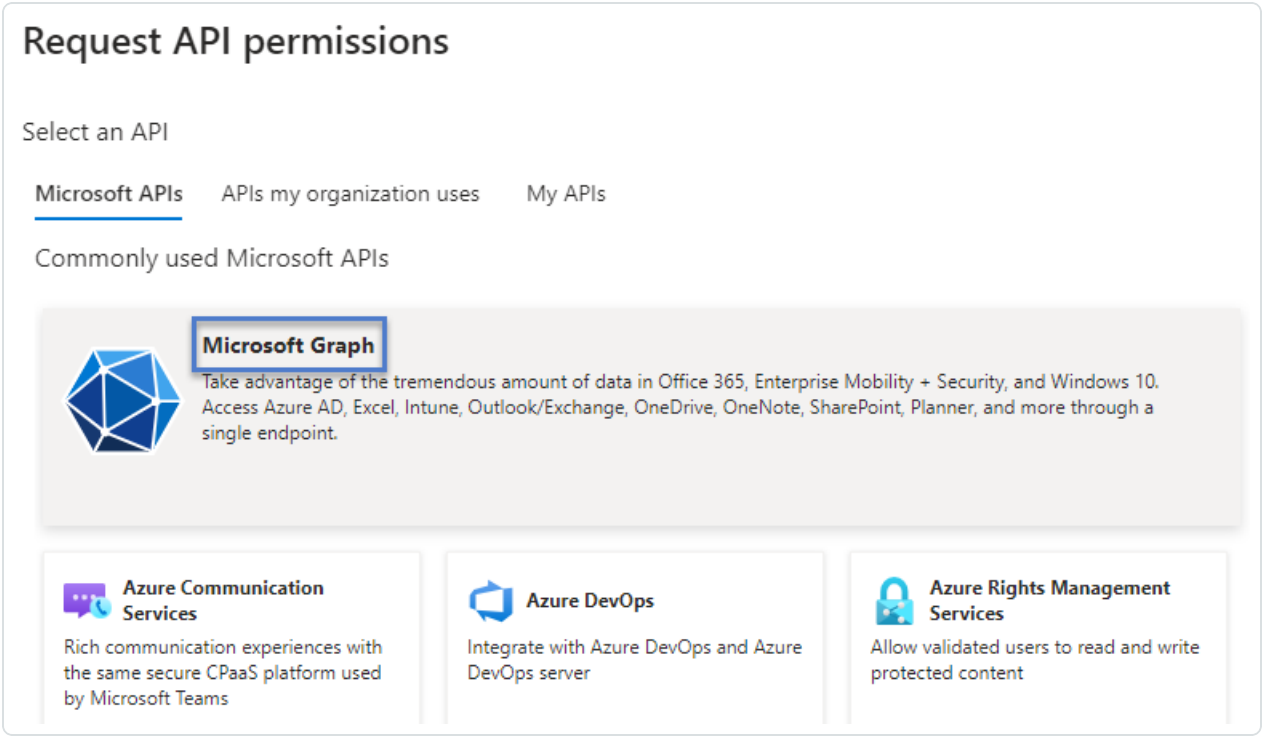
d. Supprimer l'autorisation existante `User.Read` :



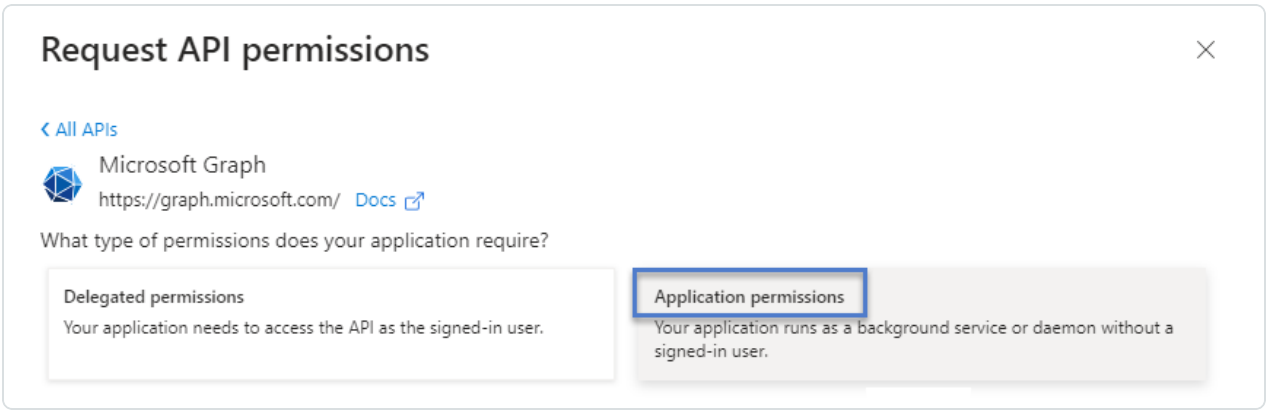
e. Cliquez sur **Ajouter une autorisation** :



f. Sélectionnez **Microsoft Graph** :



g. Sélectionnez **Autorisations de l'application** et non pas « Autorisations déléguées ».



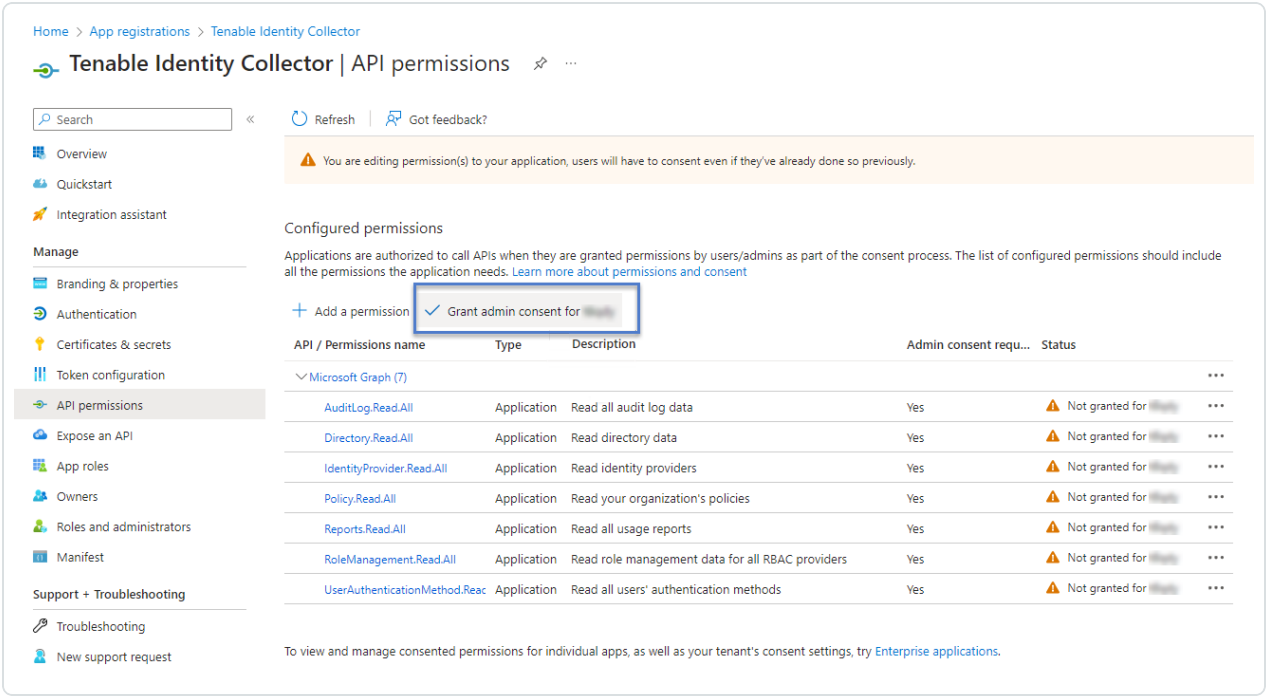
h. Utilisez la liste ou la barre de recherche pour rechercher et sélectionner toutes les autorisations suivantes :

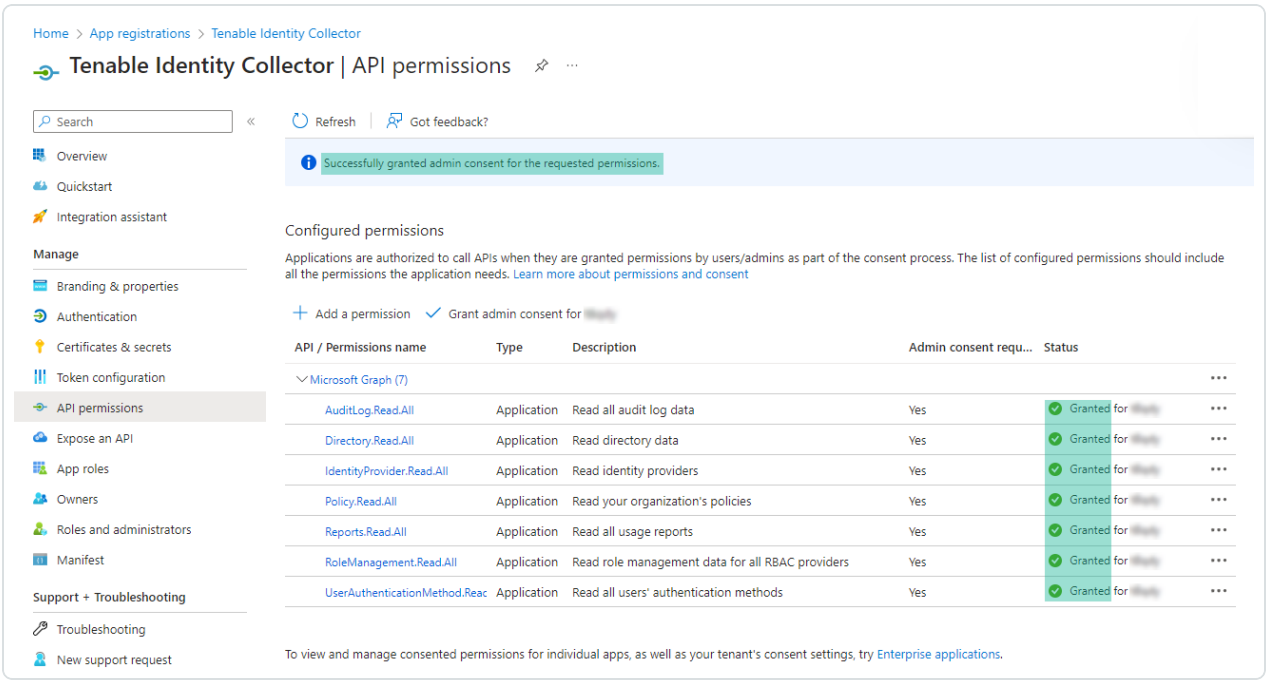
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `IdentityProvider.Read.All`
   - `Policy.Read.All`

- `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 activer la prise en charge de :

Remarque : pour activer cette fonctionnalité, 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 Microsoft Entra ID**, cliquez sur le curseur pour l'activer.
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**.

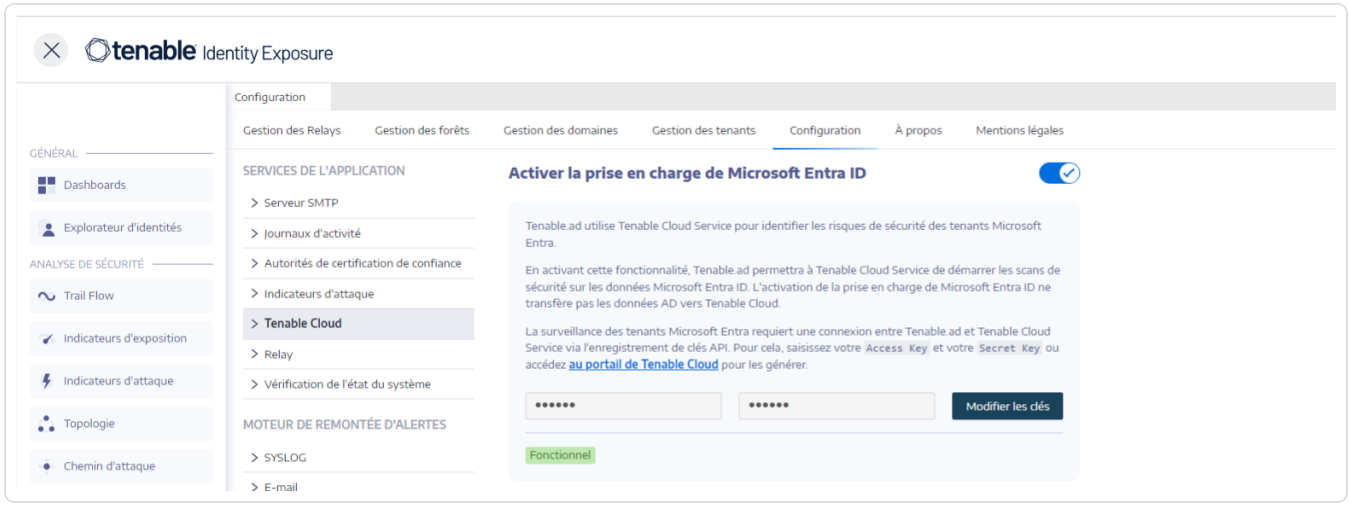
      Tenable envoie un e-mail à cette adresse avec un lien pour réinitialiser votre mot de passe.

      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.

Activer les scans de tenant

Pour ajouter un nouveau tenant :

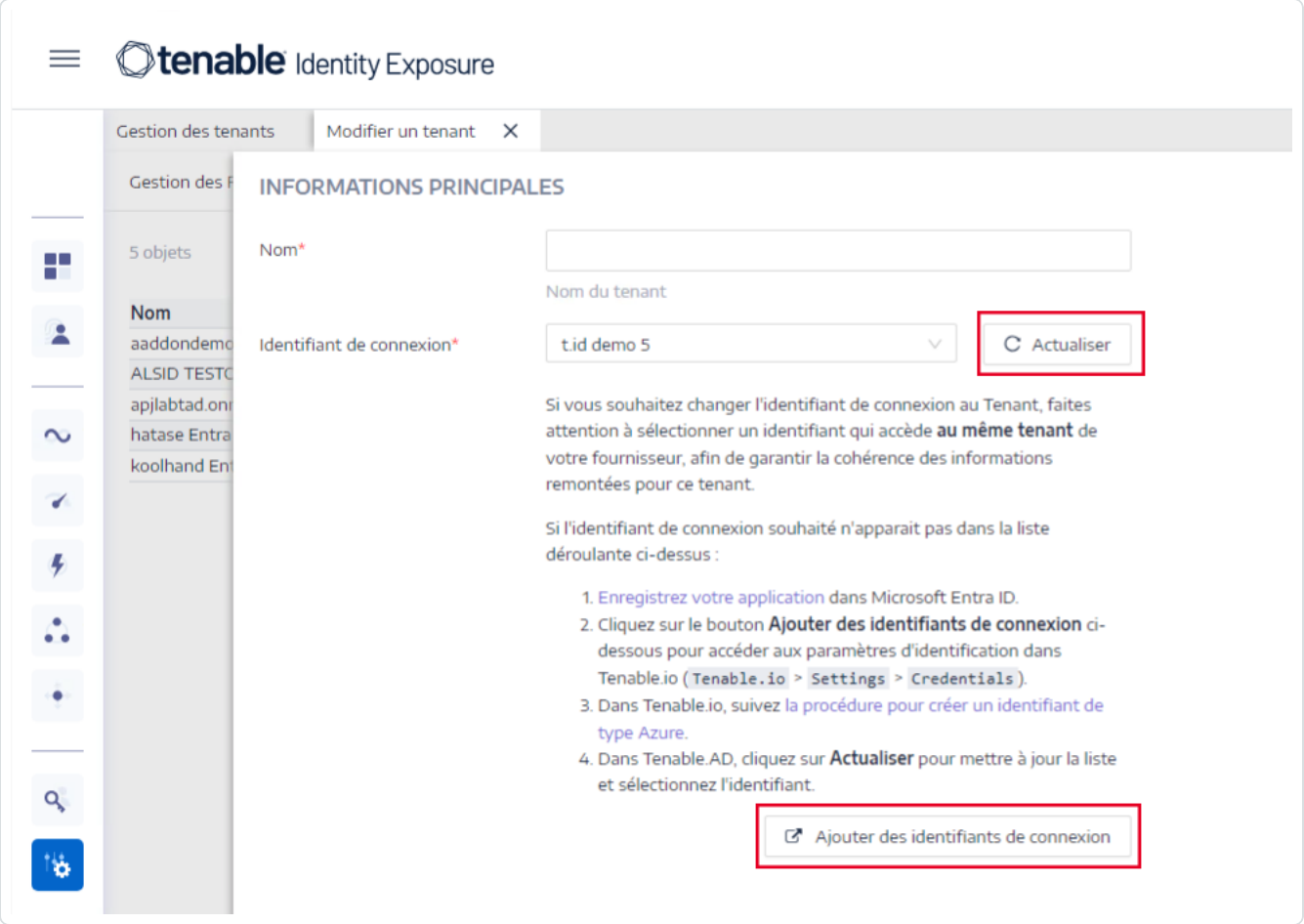
L'ajout d'un tenant lie Tenable Identity Exposure au tenant Microsoft Entra ID pour effectuer des scans sur le tenant.

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.

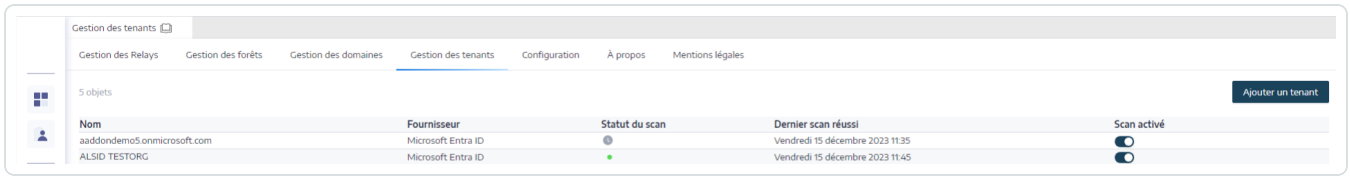
6. Cliquez sur **Actualiser** pour mettre à jour la liste déroulante des identifiants.
7. Sélectionnez l'identifiant que vous avez créé.
8. Cliquez sur **Ajouter**.

   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 :

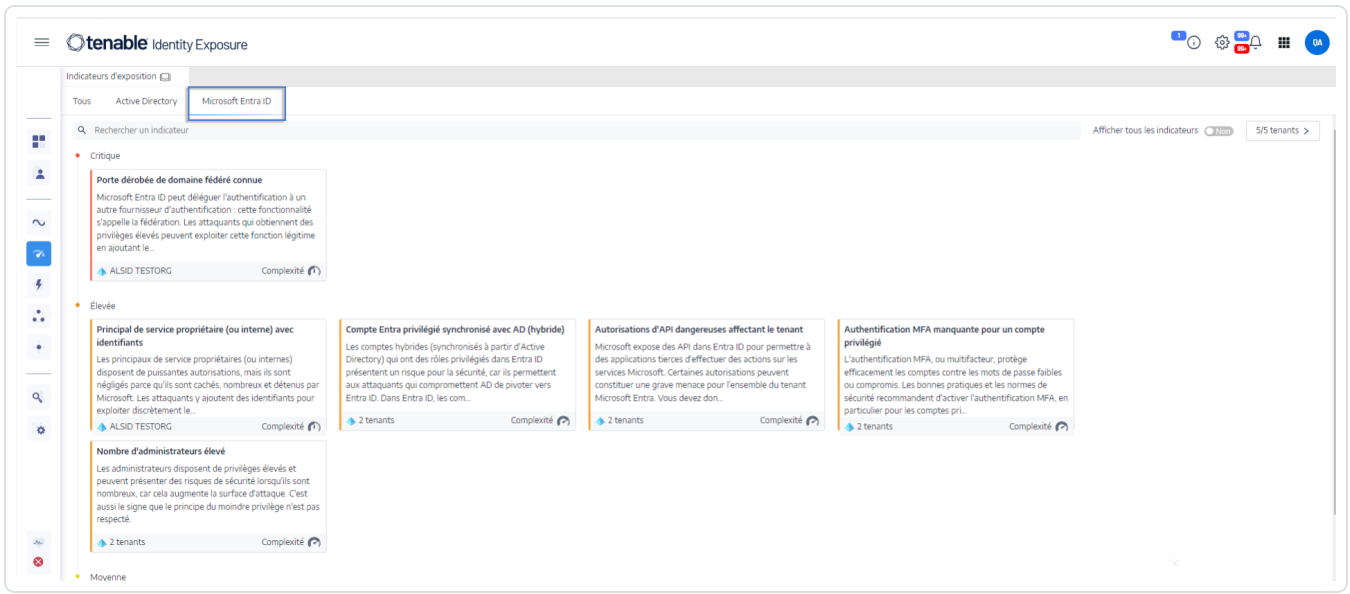
> **Remarque** : les scans de tenant ne sont pas exécutés en temps réel et il faut compter au moins 45 minutes avant que les données Microsoft Entra ID soient visibles dans l'Explorateur d'identités.

- 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**.



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.

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 mots de passe ne quittent jamais l'infrastructure du client, car seul le Relay les gère. Le Relay ne stocke pas les mots de passe, mais récupère le mot de passe de l'utilisateur chaque fois qu'il est nécessaire à des fins d'analyse, ne le conservant 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**.

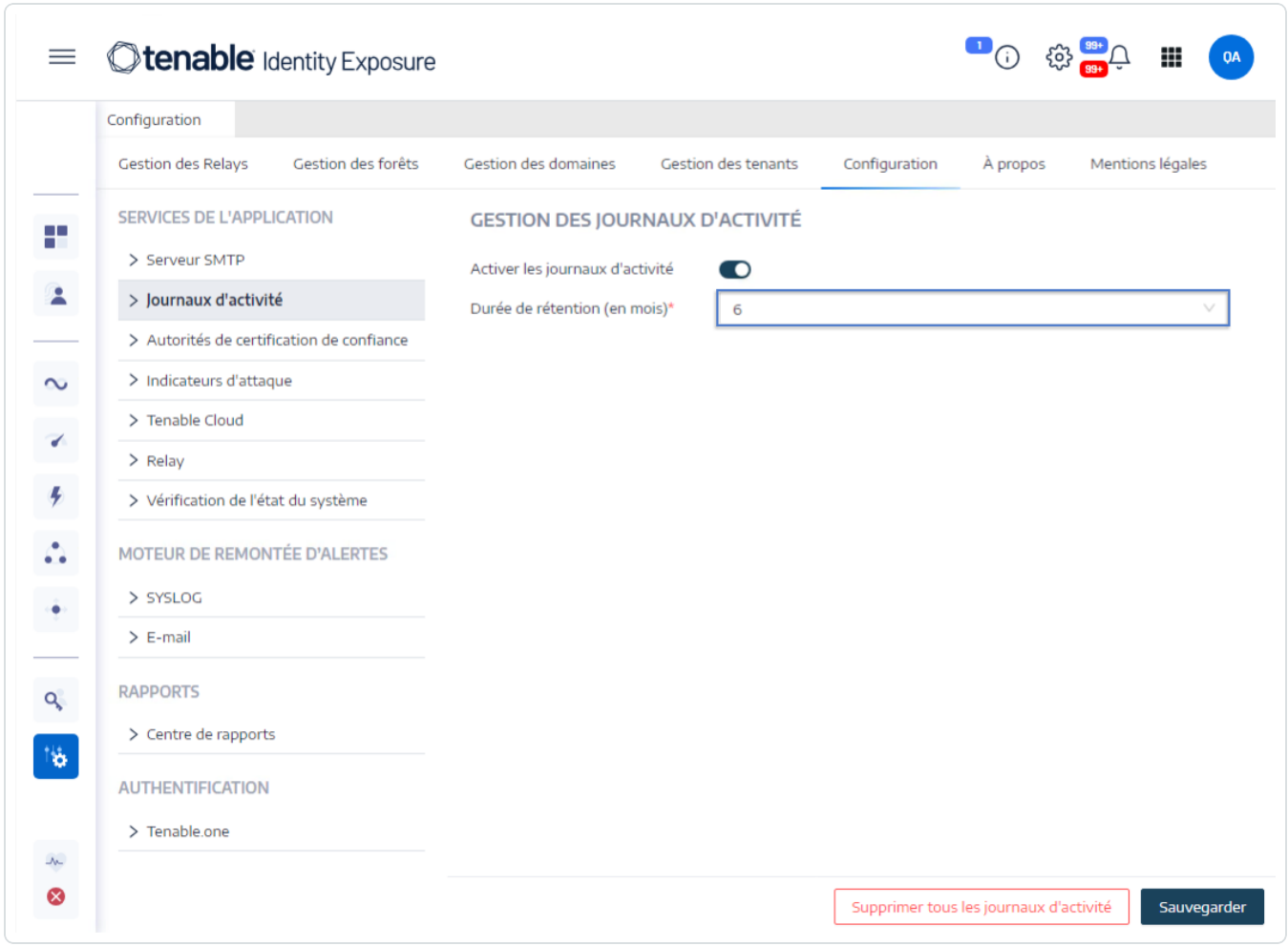
   Le volet **Gestion des journaux d'activité** apparaît.

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.

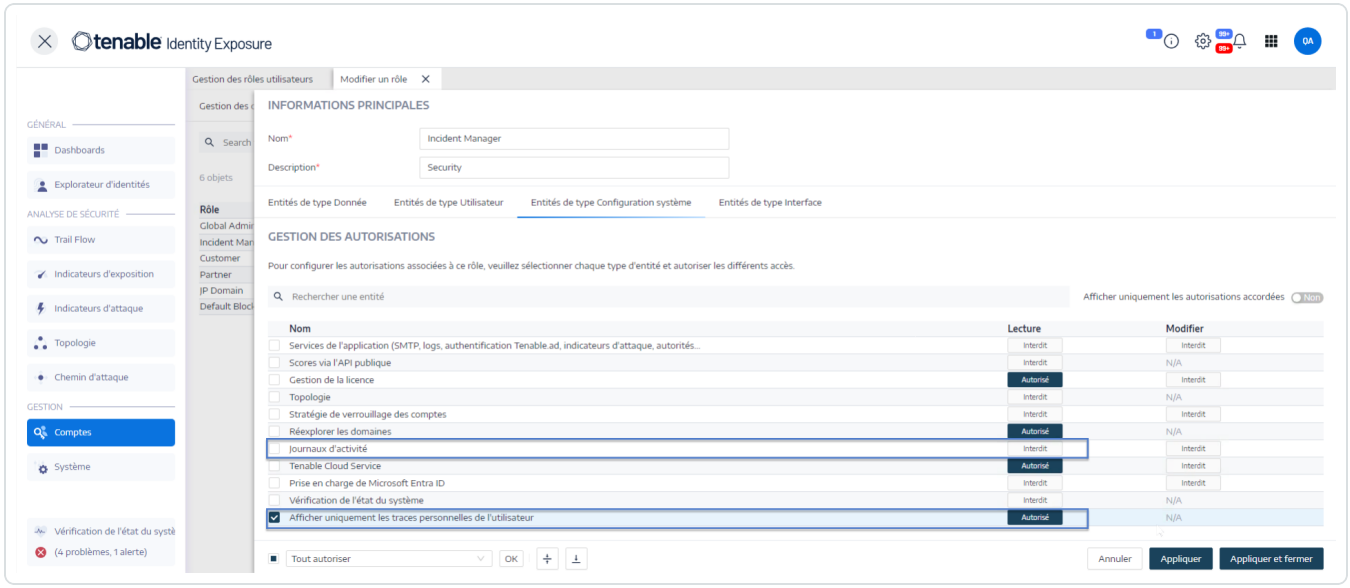
2. Cliquez sur l'onglet **Gestion des rôles**.
3. Dans la liste des rôles, survolez celui qui nécessite cette autorisation et cliquez sur l'icône ✎ en fin de ligne.

   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.



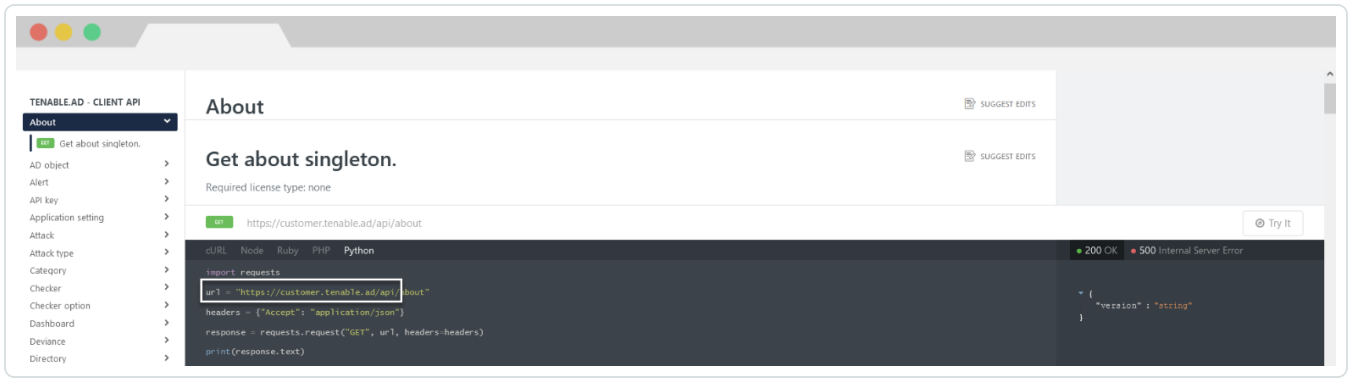
API publique Tenable Identity Exposure

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.

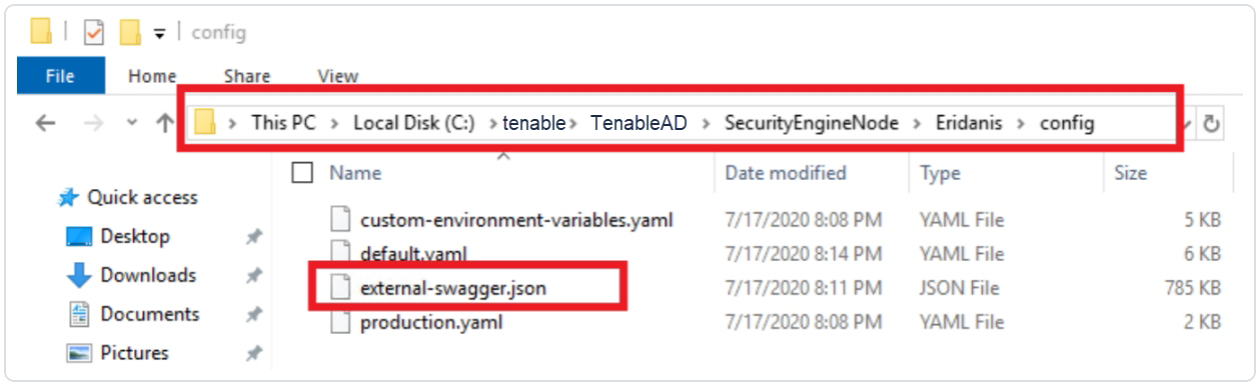
Pour accéder à l'API de votre instance Tenable Identity Exposure :

- Dans votre navigateur, ouvrez cette URL :



Pour télécharger le fichier OpenAPI :

- Pour les installations sur site, suivez ce chemin vers le 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 l'icône 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 pendant six mois. Cette période de gestion des données n'est pas configurable.

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. Pour apprendre à utiliser Tenable Identity Exposure, consultez le Guide de l'utilisateur Tenable Identity Exposure.

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.

Composants Tenable Identity Exposure

Les deux versions de Tenable Identity Exposure sont livrées avec les composants suivants :

- Vue Trail Flow
- Vue Topologie
- Indicateurs d'exposition
- Indicateurs d'attaque
- Chemins d'attaque
- Explorateur d'identités
- 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. Cependant, lorsque vous scannez plus d'assets que ne le permet votre licence, Tenable communique clairement le dépassement et réduit ensuite les fonctionnalités en trois étapes.

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 pendant plus de 45 jours.	Un message apparaît dans Tenable Identity Exposure ; les fonctionnalités d'exportation sont désactivées.

Licences expirées

Les licences Tenable Identity Exposure que vous achetez sont valables pendant toute la durée de votre contrat. 30 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.

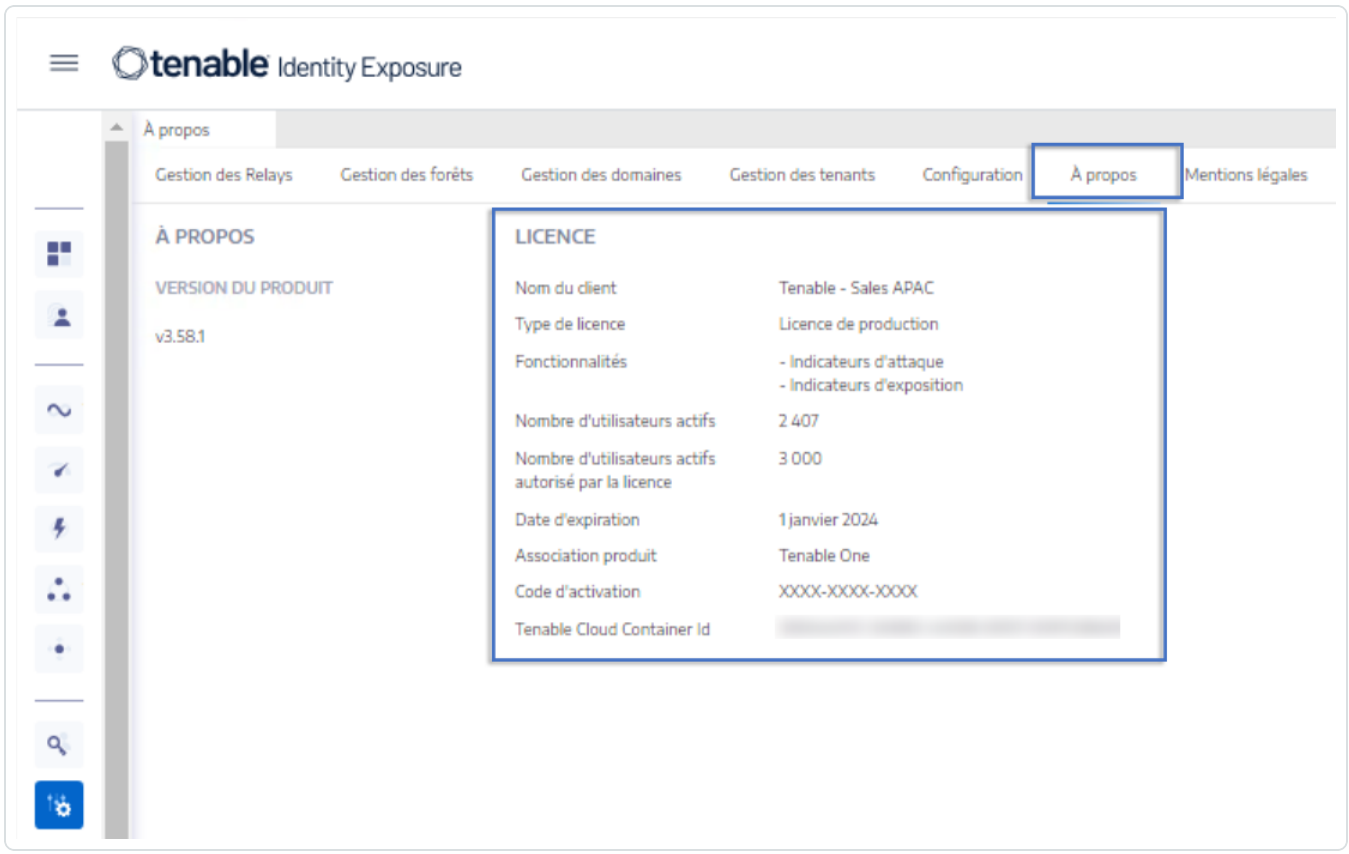
Les licences Tenable Identity Exposure peuvent inclure :

- 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

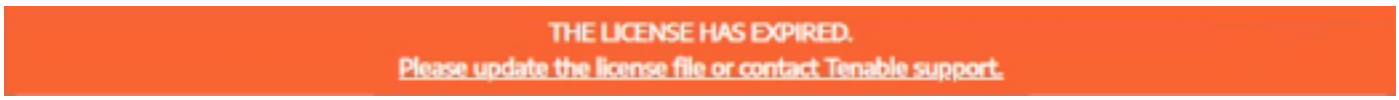
Pour les installations sur site, Tenable Identity Exposure suit la consommation de licence si une connexion Internet est disponible.

Validité de la licence

La licence Tenable Identity Exposure reste valide tant que vous répondez aux critères suivants :

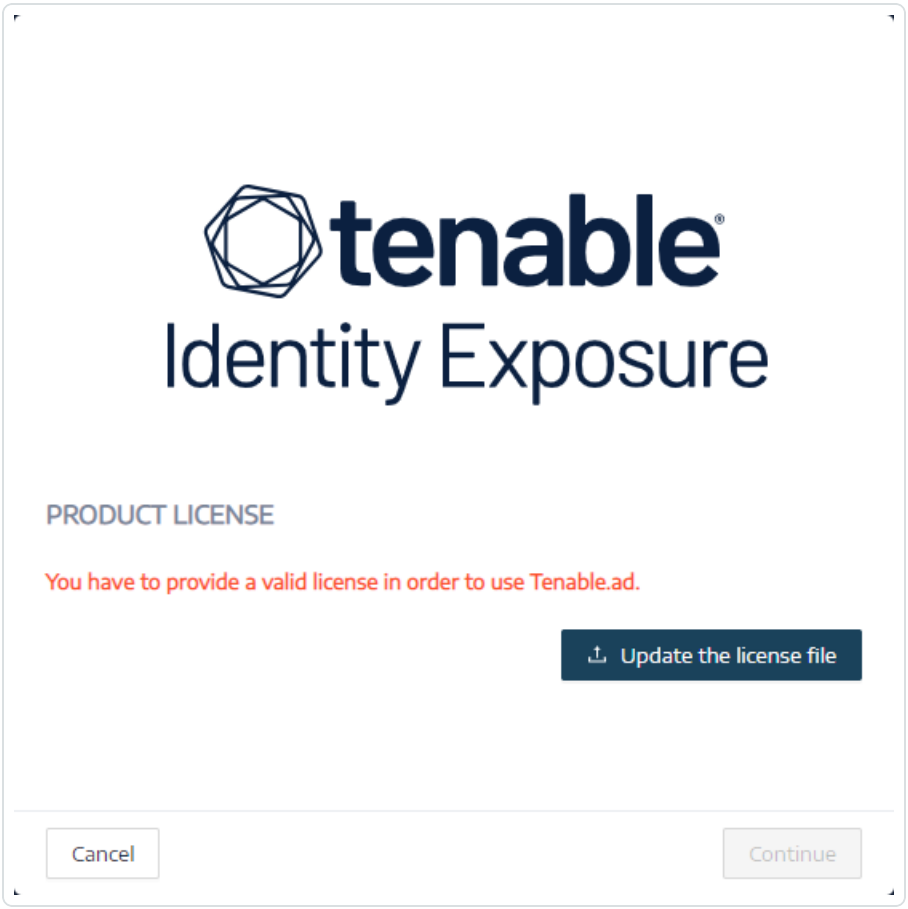
- Le nombre d'utilisateurs ne dépasse pas le nombre accordé dans la licence.
- La date d'expiration n'est pas passée.

Si vous ne respectez aucun des critères ci-dessus, Tenable Identity Exposure affiche un avertissement pour vous inviter à mettre à jour votre licence :



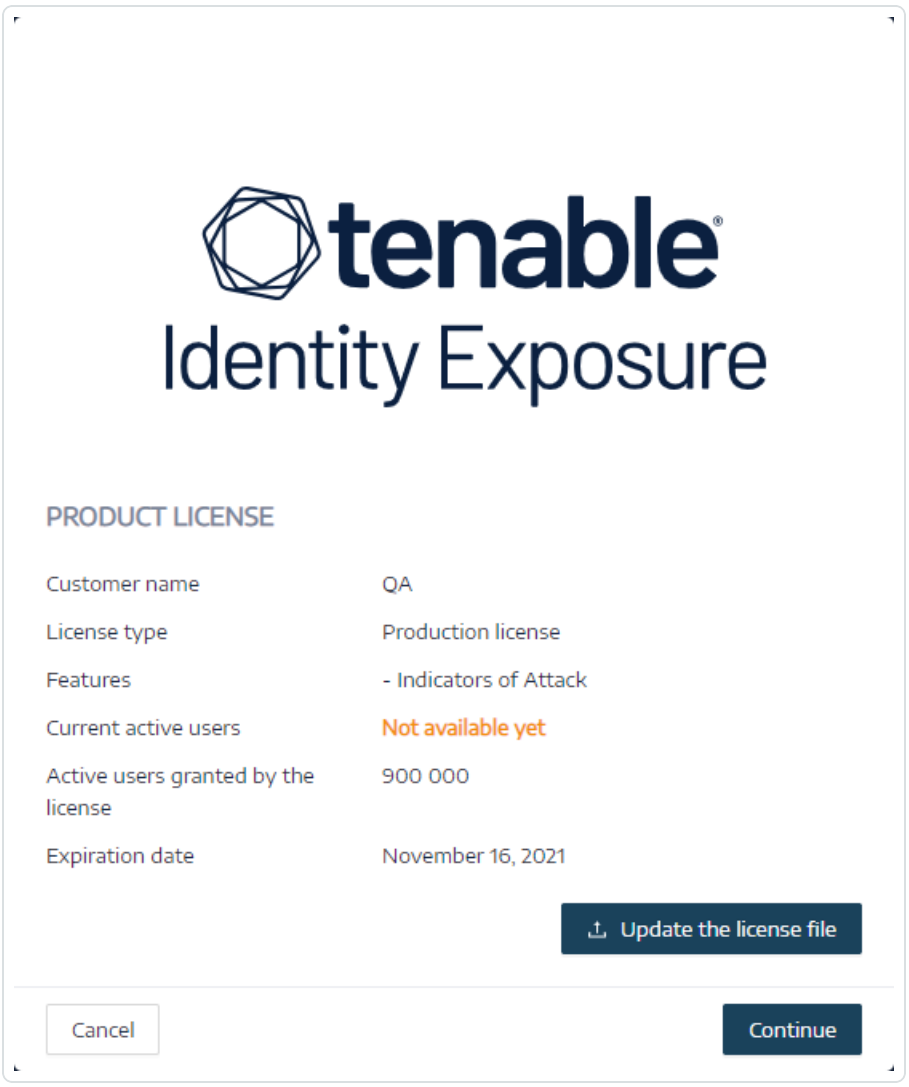
Pour charger un fichier de licence :

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.

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) :

- Outil de diagnostic Tenable Identity Exposure
- Interférence du durcissement SYSVOL avec Tenable Identity Exposure

Outil de diagnostic Tenable Identity Exposure

Tenable Identity Exposure fournit un outil de diagnostic qui vous permet de récupérer des informations de journal liées à votre installation Tenable Identity Exposure, afin que le support client puisse effectuer une analyse et vous aider en cas de problème.

Vous pouvez télécharger cet outil de diagnostic à partir du portail de téléchargements Tenable.

> **Remarque** : cet outil de diagnostic ne fonctionne que pour les **installations sur site** de Tenable Identity Exposure.

L'outil de diagnostic peut effectuer les opérations suivantes :

- Déterminer si la machine actuelle (sur laquelle vous avez lancé le fichier exécutable) héberge le Storage Manager (SM), Security Engine Node (SEN) ou Directory Listener (DL).
- Scanner l'environnement pour trouver d'autres installations Tenable Identity Exposure disponibles sur votre réseau.
- Détecter une liste des sources de journaux liées à vos installations Tenable Identity Exposure pour les tester et récupérer des informations à leur sujet en conséquence.
- Récupérer les journaux MSI sur les tentatives d'installation infructueuses de Tenable Identity Exposure.

Quelques conseils pour optimiser les résultats

- Exécutez l'outil de diagnostics sur le SEN.
- Exécutez l'outil de diagnostic en tant qu'utilisateur disposant de privilèges élevés pour activer la plupart ou l'intégralité des sources de journaux.
- Pour détecter l'installation de SM ou d'une autre installation, vérifiez ce qui suit :
    - La configuration permet à la commande à distance de s'exécuter sur l'ordinateur distant (cmdlet Invoke-Command).
    - La configuration permet l'accès à distance aux disques.
    - WMI est activé et autorisé pour le compte utilisateur actuel.

Pour exécuter l'outil de diagnostic :

1. Téléchargez le fichier `TenableAdDiagnosticTool.OnPrem.Console.exe` à partir du portail des téléchargements Tenable.
2. Exécutez le fichier exécutable en tant qu'administrateur sur une machine Tenable Identity Exposure, de préférence celle qui héberge le SEN.
3. À l'invite, saisissez l'une des options suivantes :
    - `E` — Tous les journaux (option par défaut)
    - `Msi` — Journaux liés aux installations Tenable Identity Exposure
    - `Tenable` — Journaux liés à Tenable Identity Exposure
4. Appuyez sur Entrée.

    L'outil de diagnostic scanne votre installation. Une fois le scan terminé, la sortie résultante est un fichier compressé situé dans votre répertoire actuel.
5. Envoyez ce fichier compressé au service client Tenable Identity Exposure. Veillez à ne modifier le contenu en aucune manière.

Pour exécuter l'outil de diagnostics à l'aide de la ligne de commande :

1. Dans la ligne de commande, exécutez le fichier exécutable `TenableAdDiagnosticTool.OnPrem.Console.exe` en tant qu'administrateur sur la machine Tenable Identity Exposure, de préférence celle qui héberge le SEN.

    L'outil de diagnostic scanne votre installation. Une fois le scan terminé, la sortie résultante est un fichier compressé situé dans votre répertoire actuel.
2. Envoyez ce fichier compressé au service client Tenable Identity Exposure. Veillez à ne modifier le contenu en aucune manière.

Autres options

L'outil de diagnostic propose également les options suivantes dans la ligne de commande :

- `--help` — Brève description de l'utilisation de l'outil de diagnostic.
- `--commands` — Liste de requêtes Powershell/WMI pour tester les fonctionnalités de la machine et scanner d'autres installations.

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 :

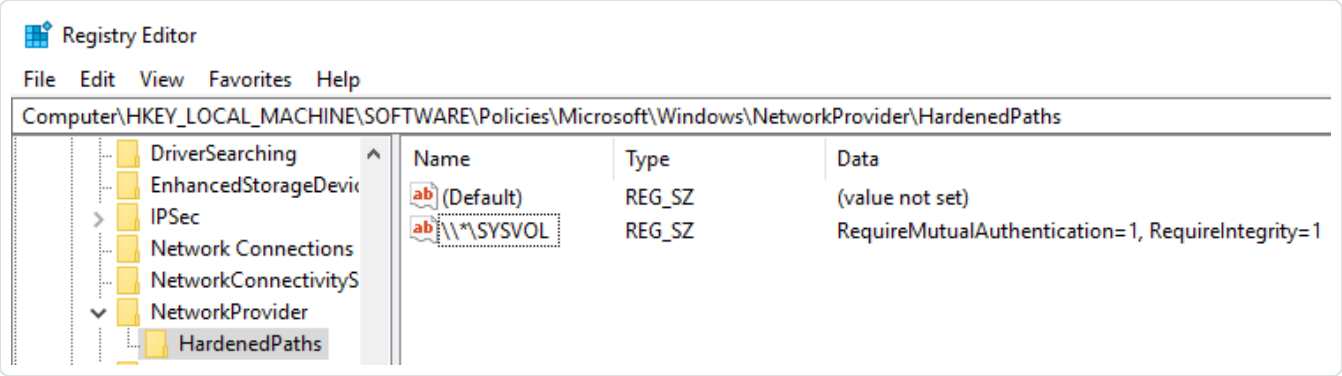
- SaaS avec VPN

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.

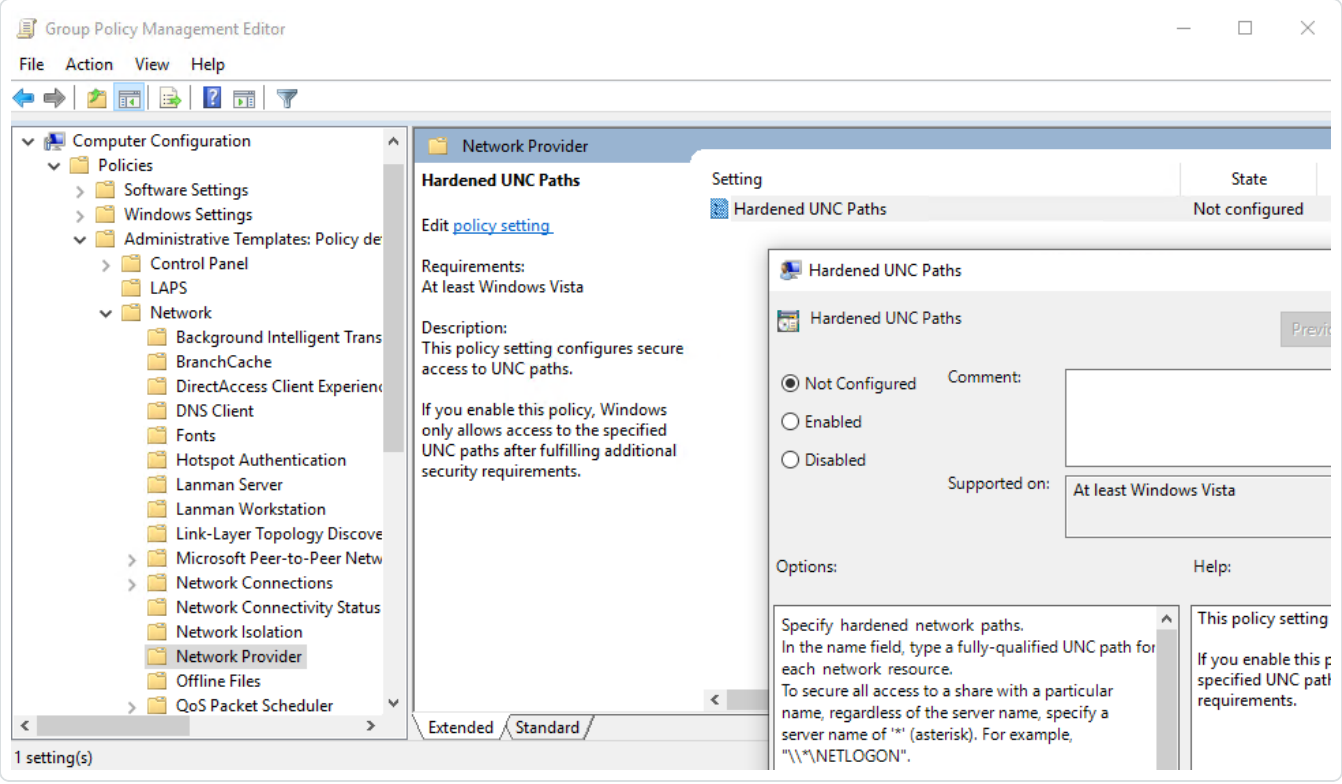
Windows active ce paramètre par défaut et il peut interférer avec Tenable Identity Exposure.

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` » :



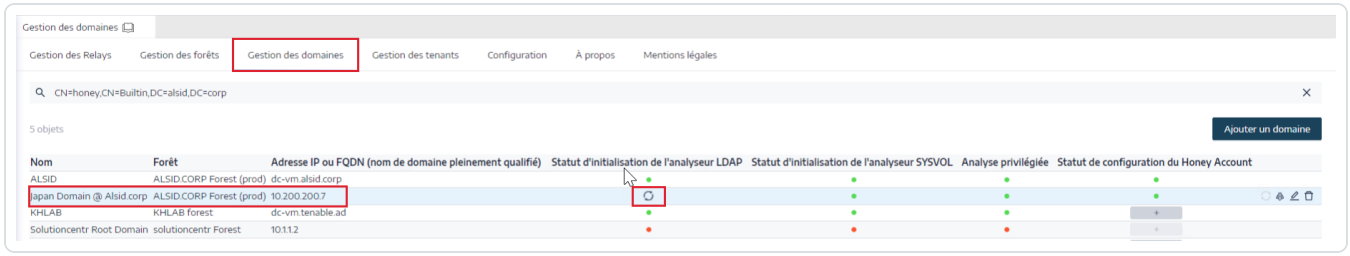
L'application du durcissement SYSVOL se produit lorsque les paramètres « `RequireMutualAuthentication` » et « `RequireIntegrity` » d'un chemin UNC faisant référence à SYSVOL, par exemple « `\\*\SYSVOL` », ont la valeur « `1` ».

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.

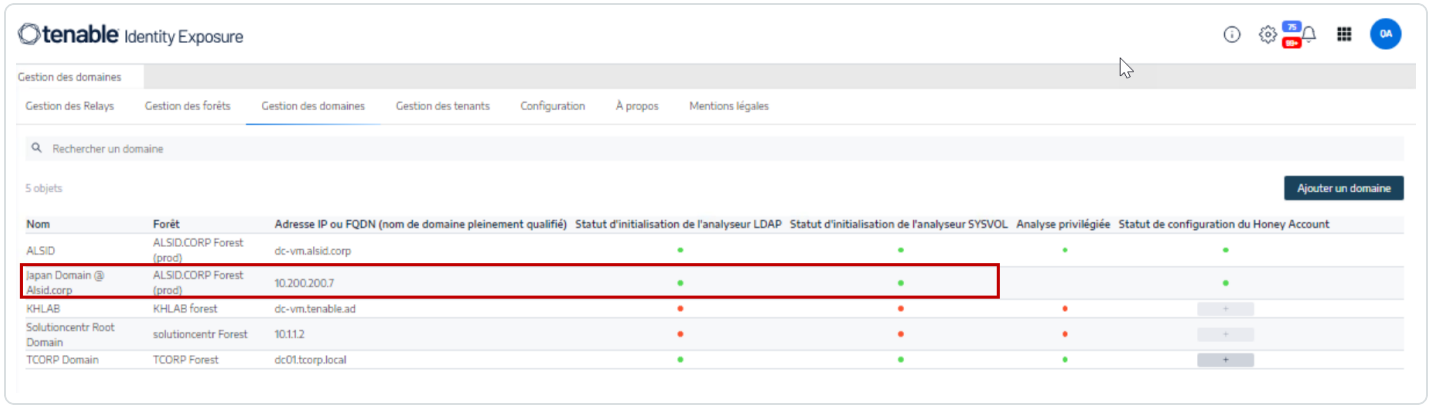
Les programmes d'installation Tenable Identity Exposure utilisés sur la machine qui héberge le Directory Listener (sur site) ou le Relay (SaaS avec Secure Relay) désactivent déjà le durcissement SYSVOL localement. Cependant, une GPO ou un script de votre environnement peut supprimer ou remplacer la clé 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.

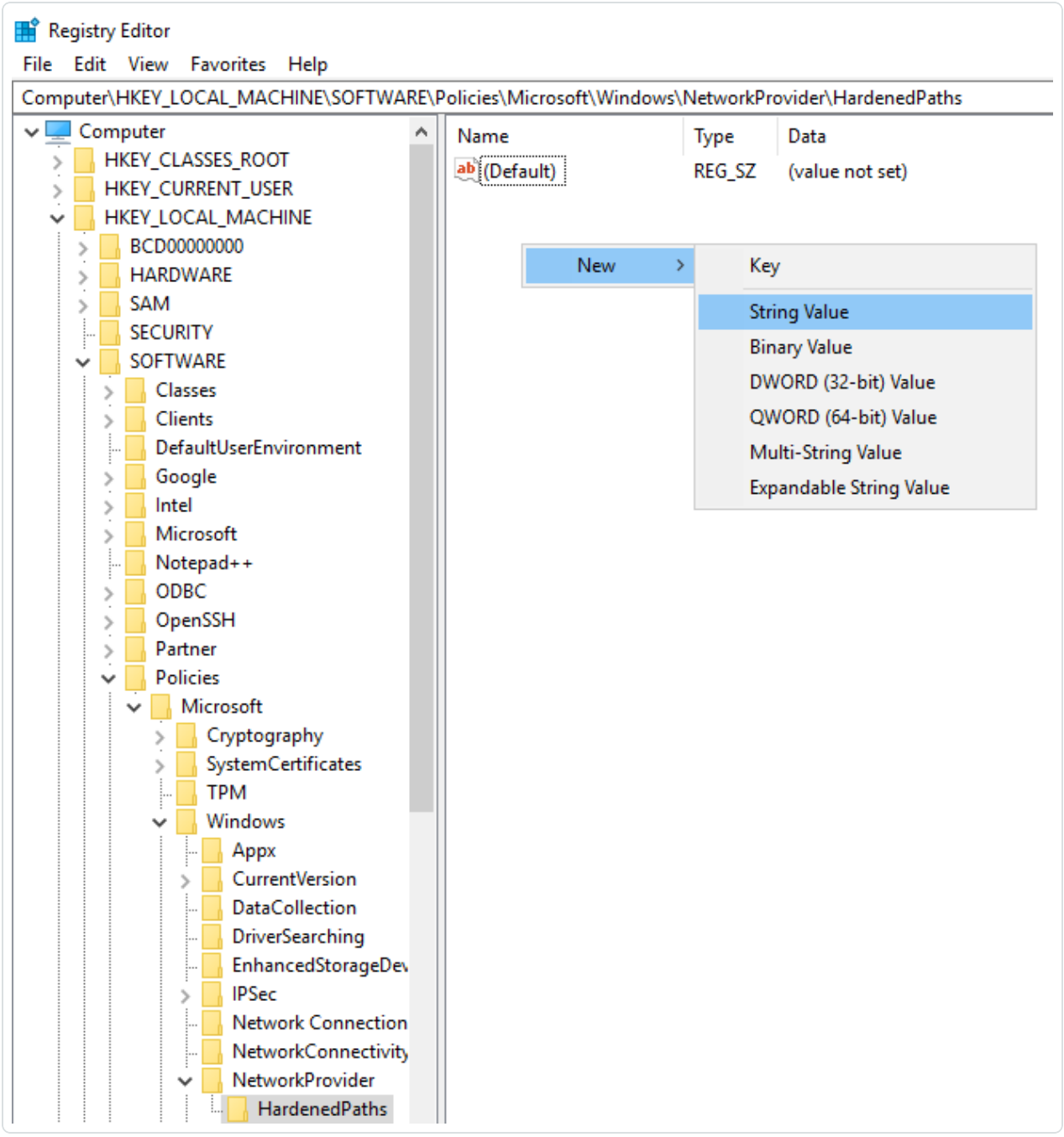
Après avoir redémarré le Directory Listener ou la machine Relay, l'indicateur d'exploration du domaine modifié doit devenir vert :



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**.



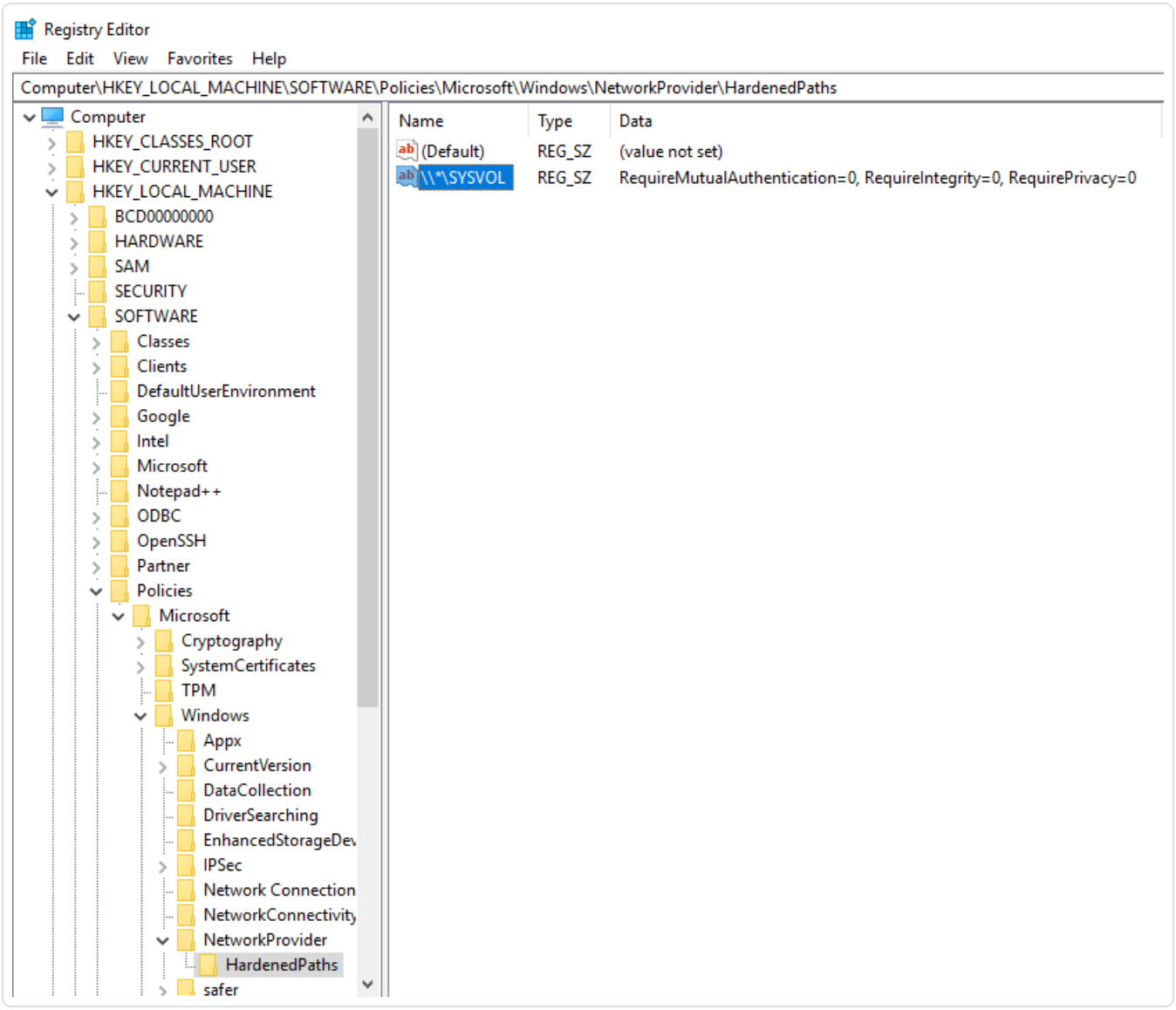
b. Dans le champ Nom, saisissez `\\*\SYSVOL`.

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.

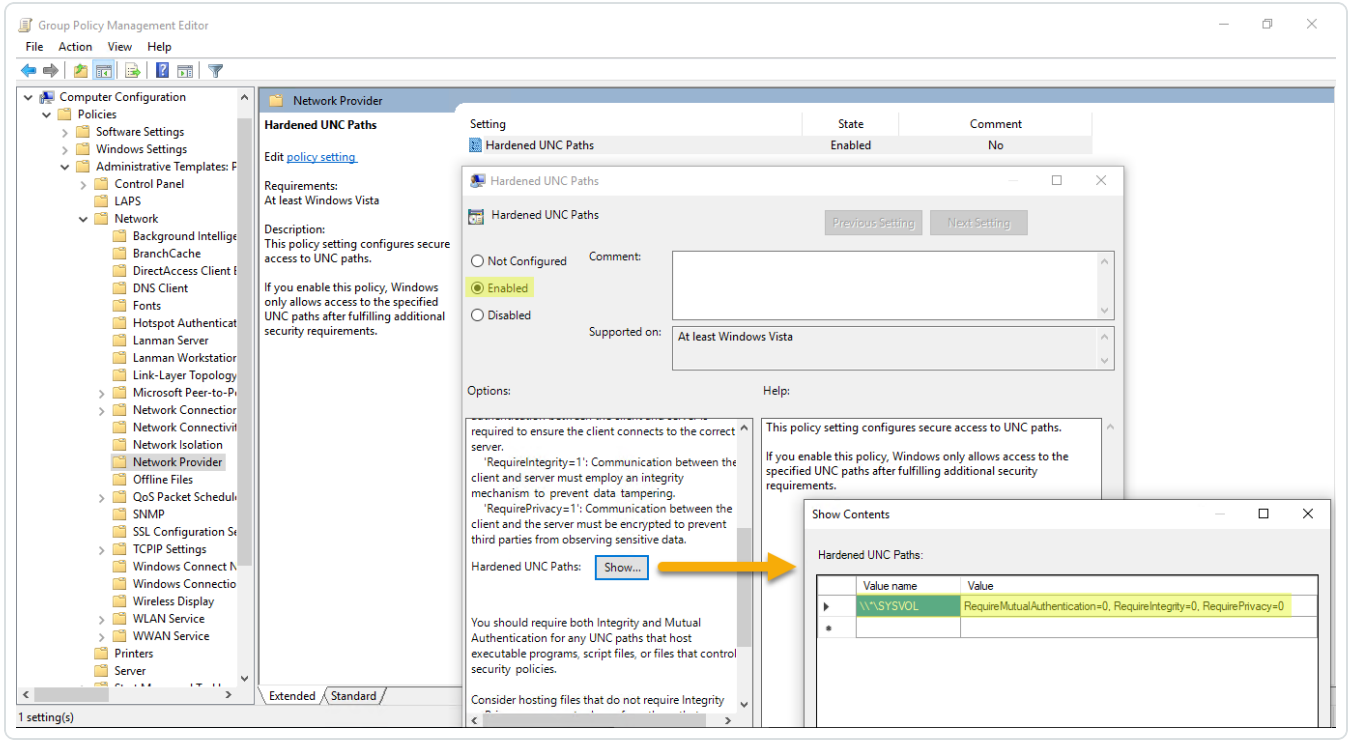
GPO

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 :

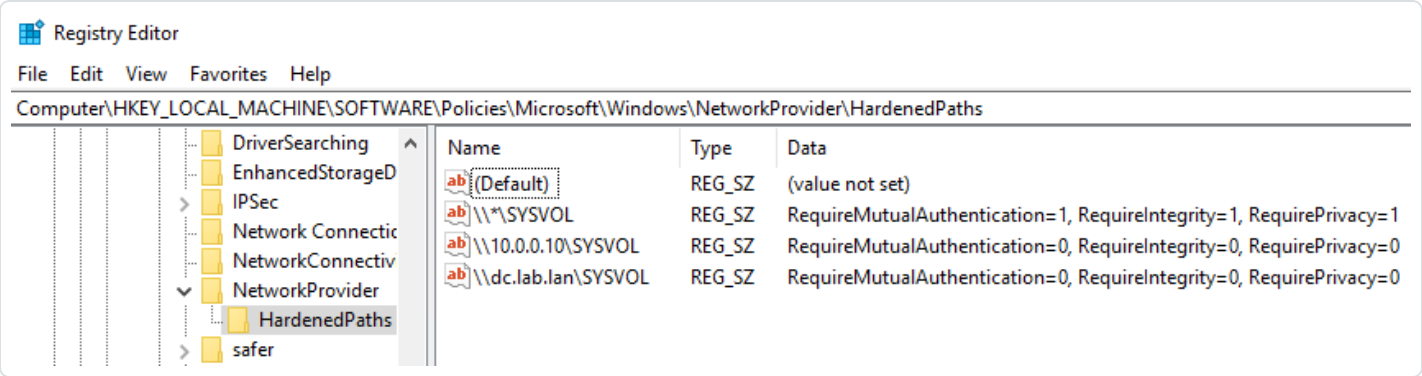


5. Cliquez sur **OK** pour confirmer.
6. Liez cette GPO à l'unité d'organisation qui contient le Tenable Identity Exposure Directory Listener ou la machine Relay. Vous pouvez également utiliser la fonction de filtrage de groupe de sécurité pour vérifier que cette GPO s'applique uniquement à cette machine.

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.