Migrer vers SAML à partir de LDAP

Publié: 2023-09-19

L'authentification unique et sécurisée au système ExtraHop est facile à configurer. Cependant, si vous avez configuré votre système ExtraHop pour l'authentification à distance via LDAP, TACACS+ ou RADIUS, le passage à SAML supprime définitivement tous les utilisateurs distants existants et leurs personnalisations, telles que les tableaux de bord enregistrés, les cartes d'activité, les rapports (disponibles sur les consoles uniquement) et les requêtes d'enregistrement (recordstore requis).

La migration est un processus en plusieurs étapes ; dans chaque section, nous fournissons les étapes pour migrer en toute sécurité un seul utilisateur et ses personnalisations de LDAP à SAML par le biais des paramètres d'administration. Si vous devez migrer un grand nombre d'utilisateurs distants avec des personnalisations, nous vous recommandons vivement de migrer vers SAML via l'API REST. Si vous préférez faire appel à une solution clé en main pour la migration, contactez votre représentant commercial ExtraHop

Important: .Les personnalisations doivent être sauvegardées à l'endroit où les utilisateurs distants les ont créées. Par exemple, si un utilisateur distant dispose d'un tableau de bord critique sur une console et un capteur, vous devez effectuer ces procédures à la fois sur la console et sur le capteur pour cet utilisateur distant.

Présentation de la procédure

La migration vers une nouvelle méthode d'authentification à distance est un processus complexe. Assurez-vous de bien comprendre toutes les étapes avant de commencer et veillez à planifier une fenêtre de maintenance pour éviter de perturber les utilisateurs.

Avant de commencer

1. Activez les fichiers d'exception sur vos capteurs et votre console. Si le système ExtraHop s'arrête ou redémarre de manière inattendue pendant le processus de migration, le fichier d'exception est écrit sur le disque. Le fichier d'exception peut aider l'assistance ExtraHop à diagnostiquer le problème à l'origine de la panne.
2. Créez une sauvegarde de vos capteurs et de votre console. Les fichiers de sauvegarde incluent tous les utilisateurs, les personnalisations et les paramètres partagés. Téléchargez et stockez le fichier de sauvegarde hors système sur une machine locale.

Étant donné que la modification de la méthode d'authentification à distance sur un capteur ou une console supprime effectivement tous les utilisateurs distants, vous devez d'abord créer un utilisateur local (en miroir) pour chaque utilisateur distant, où vous pouvez transférer temporairement les personnalisations et les paramètres de partage. Après avoir transféré ces paramètres une première fois, vous devez configurer SAML pour le capteur ou la console, puis transférer une seconde fois les paramètres des utilisateurs locaux vers les utilisateurs SAML. Enfin, vous pouvez supprimer les utilisateurs locaux temporaires du capteur ou de la console.

Voici une explication de chaque étape :

1. Si vous prévoyez de ne migrer qu'un petit nombre de comptes via les paramètres d'administration, passez en revue les comptes d'utilisateurs distants existants afin d'identifier les utilisateurs disposant de personnalisations que vous souhaitez conserver, et identifiez les groupes d'utilisateurs auxquels des autorisations partagées ont été accordées pour les personnalisations.
2. Créez un compte d'utilisateur local temporaire pour chaque utilisateur distant que vous souhaitez conserver.
3. (Facultatif pour les utilisateurs de magasins d'enregistrements) Enregistrez les requêtes d'enregistrements créées par les utilisateurs distants dans le compte utilisateur de configuration.
4. Supprimer les utilisateurs distants et transférer leurs personnalisations sur le compte local.

5. Configurer SAML. (Tous les utilisateurs et groupes d'utilisateurs distants restants sont supprimés avec leurs personnalisations).
6. Créez un compte pour l'utilisateur SAML sur l'appliance. Une fois le capteur ou la console configuré pour SAML, vous pouvez créer un compte distant pour vos utilisateurs avant qu'ils ne se connectent au système ExtraHop pour la première fois.
7. Supprimez le compte utilisateur local et transférez à nouveau les personnalisations, cette fois du compte local temporaire vers le compte utilisateur SAML. Lorsque vos utilisateurs SAML se connecteront pour la première fois, leurs personnalisations seront disponibles.

Identifier les utilisateurs et les groupes d'utilisateurs distants critiques

Parce que la migration est un processus qui prend du temps dans les paramètres d'administration, nous vous recommandons de limiter le nombre de comptes d'utilisateurs que vous préservez à ceux qui ont des personnalisations complexes ou critiques pour l'entreprise. De plus, si vous avez importé des groupes d'utilisateurs LDAP, les tableaux de bord ou les cartes d'activité partagés avec ces groupes ne le seront plus après la configuration de SAML. Bien que les groupes d'utilisateurs ne puissent pas être importés à partir de SAML, vous pouvez configurer et partager des personnalisations avec un groupe d'utilisateurs local sur le système ExtraHop.

- Dresser une liste des utilisateurs distants avec des tableaux de bord critiques, des cartes d'activité, des requêtes d'enregistrement sauvegardées (magasins d'enregistrement uniquement) et des rapports planifiés (consoles uniquement).
- Visualiser les groupes d'utilisateurs LDAP et leurs paramètres partagés, créer un groupe d'utilisateurs local, puis partager manuellement les tableaux de bord et les cartes d'activité avec le groupe d'utilisateurs local après avoir migré vers SAML.

Associations de tableaux de bord

Vous devez récupérer des informations sur la propriété et le partage des tableaux de bord avant de configurer SAML sur votre système ExtraHop.

Les tableaux de bord n'étant visibles que par les utilisateurs qui les ont créés ou par ceux qui disposent d'autorisations partagées, nous vous recommandons d'effectuer cette étape par le biais de l'API REST.

Si vous devez effectuer cette étape via les paramètres d'administration, chaque utilisateur distant doit partager manuellement son tableau de bord avec un utilisateur local.

Associations de cartes d'activité

Vous pouvez récupérer des informations sur la propriété et le partage des cartes d'activité avant de configurer SAML sur votre appliance.

Toutes les cartes d'activité sont visibles par les utilisateurs disposant de privilèges d'administration du système et des accès.

1. Connectez-vous au système ExtraHop via https://<extrahop-hostname-or-IP-address>.
2. En haut de la page, cliquez sur **Assets**.
3. Cliquez sur **Activité** dans le volet de gauche, puis cliquez sur le groupe de clients, de serveurs ou de périphériques correspondant au protocole souhaité.
4. Cliquez sur **Activity Map**, situé dans le coin supérieur droit de la page.
5. Cliquez sur l'icône **Charger** dans le coin supérieur droit.
6. Notez le nom de chaque propriétaire de carte d'activité.
7. Identifiez les propriétés de la carte d'activité et les options de partage pour chaque carte d'activité.
   a) Cliquez sur le nom de la carte d'activité.
   b) Cliquez sur le menu de commande dans le coin supérieur droit, puis sélectionnez **Partager**.
   c) Notez les utilisateurs ou les groupes avec lesquels la carte d'activité est partagée.

(Consoles uniquement) Associations de rapports programmés

Vous devez récupérer des informations sur la propriété des rapports programmés avant de configurer SAML sur votre système ExtraHop.

Tous les rapports sont visibles par les utilisateurs disposant de privilèges d'administration du système et des accès.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>` avec un compte utilisateur disposant de privilèges illimités.
2. Cliquez sur l'icône Paramètres système, puis sur **Rapports programmés**.
3. Identifiez les rapports programmés que vous souhaitez conserver et notez l'utilisateur figurant dans la colonne Propriétaires.

Sauvegarder les requêtes d'enregistrement

Dans les étapes suivantes, vous apprendrez à conserver les requêtes d'enregistrement sauvegardées par un utilisateur distant.

Comme les requêtes enregistrées sont accessibles à tous les utilisateurs du système, vous pouvez exporter toutes les requêtes enregistrées dans un paquet, puis les télécharger après la migration vers SAML. Les requêtes d'enregistrement importées sont attribuées à l'utilisateur qui télécharge le paquet. (Par exemple, si vous importez des requêtes à partir d'une liasse alors que vous êtes connecté en tant qu'utilisateur de configuration, toutes les requêtes mentionnent la configuration en tant que propriétaire de la requête). Après la migration, les utilisateurs distants peuvent consulter les requêtes d'enregistrement sauvegardées et en enregistrer une copie pour eux-mêmes.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>` avec le compte utilisateur `setup`.
2. Cliquez sur l'icône System Settings (Paramètres système), puis sélectionnez **Bundles (Groupes)**.
3. Sur la page Bundles, sélectionnez **New (Nouveau)**.
4. Saisissez un nom pour identifier l'offre groupée.
5. Cliquez sur la flèche en regard de Requêtes dans le tableau Contenu et cochez les cases en regard des requêtes enregistrées que vous souhaitez exporter.
6. Cliquez sur **OK**. Le groupe apparaît dans le tableau de la page Groupes.
7. Sélectionnez l'ensemble et cliquez sur **Télécharger**. Les requêtes sont enregistrées dans un fichier JSON.

Prochaines étapes
Après la migration, téléchargez l'ensemble pour restaurer les requêtes d'enregistrement sauvegardées.

Créer un compte local temporaire

Dans les étapes suivantes, vous apprendrez à créer un compte d'utilisateur local en tant que miroir d'un compte d'utilisateur distant.

Nous vous recommandons de créer un nom d'utilisateur local qui ajoute _local au nom d'utilisateur distant existant. Par exemple, pour l'utilisateur LDAP `john_smith`, créez un utilisateur local nommé `john_smith_local`.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Utilisateurs**.
3. Cliquez sur **Ajouter un utilisateur**.
4. Dans la section Informations personnelles, saisissez les informations suivantes :
   a) Login ID : Le nom d'utilisateur temporaire de l'utilisateur, qui ne peut pas contenir d'espaces.
   b) Nom complet : Le nom d'affichage de l'utilisateur, qui peut contenir des espaces.

c) Mot de passe : Le mot de passe de ce compte.
d) Confirmer le mot de passe : Saisissez à nouveau le mot de passe dans le champ Mot de passe.

5. Dans la section Type d'authentification, sélectionnez **Local**.
6. Dans la section Type d'utilisateur, sélectionnez le type de privilèges pour l'utilisateur.
7. Cliquez sur **Enregistrer**.

Supprimer des utilisateurs distants et transférer des personnalisations

Dans les paramètres d'administration, cette étape fait appel à une procédure spécifique de suppression d'utilisateur, qui inclut l'option de transfert de propriété pour un seul compte d'utilisateur. Cette option est préférable si vous n'avez que quelques personnalisations d'utilisateurs qui doivent être conservées. Notez que dans l'API REST, vous devez d'abord transférer chaque personnalisation, puis supprimer l'utilisateur séparément. Si vous supprimez tous les utilisateurs en changeant la méthode d'authentification à distance en SAML, la propriété ne peut pas être transférée).

Dans les étapes suivantes, vous apprendrez à transférer les personnalisations vers le compte local temporaire que vous avez créé lors de la suppression de l'utilisateur distant concerné.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Utilisateurs**.
3. Faites défiler jusqu'à l'utilisateur distant que vous souhaitez supprimer et cliquez sur le **X** à l'extrême droite.
   a) Une option apparaît pour transférer les tableaux de bord, les collections et les cartes d'activité. (Sur une console, vous pouvez également transférer des rapports planifiés au cours de cette étape).
4. Sélectionnez **Transférer les tableaux de bord, les collections, les cartes d'activité et les rapports planifiés appartenant à a à l'utilisateur suivant** *<utilisateur distant>*, puis sélectionnez le compte d'utilisateur local temporaire que vous avez créé. Par exemple, lorsque vous supprimez l'utilisateur distant `john_smith`, vous pouvez transférer les personnalisations à l'utilisateur local `john_smith_local`.
5. Répétez l'opération pour chaque utilisateur dont vous souhaitez conserver les personnalisations.

Configurer SAML sur le système ExtraHop

En fonction de votre environnement, configurez SAML. Des guides sont disponibles pour Okta et Google. Après avoir configuré SAML sur votre système ExtraHop, vous pouvez créer des comptes pour vos utilisateurs distants et transférer leurs personnalisations avant qu'ils ne se connectent pour la première fois.

Créer des comptes SAML sur le système ExtraHop

Dans les étapes suivantes, vous apprendrez à créer un utilisateur SAML sur votre système ExtraHop.

Note: Vérifiez le format requis pour les noms d'utilisateur saisis dans le champ ID de connexion auprès de l'administrateur de votre fournisseur d'identité. Si les noms d'utilisateur ne correspondent pas, l'utilisateur distant ne sera pas associé à l'utilisateur créé sur le système.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Utilisateurs**.
3. Cliquez sur **Ajouter un utilisateur**.

4. Dans le champ ID de connexion, saisissez le nom d'utilisateur SAML. (Les noms d'utilisateur SAML sont sensibles à la casse).
5. Dans le champ Nom complet, saisissez le nom et le prénom de l'utilisateur.
6. Dans la section Authentication Type (Type d'authentification), sélectionnez **Remote (À distance**).
7. Cliquez sur **Enregistrer**.
8. Répétez l'opération pour chaque utilisateur dont vous souhaitez conserver les personnalisations.

Supprimer les utilisateurs locaux et transférer les personnalisations

Dans les étapes suivantes, vous apprendrez à supprimer les comptes d'utilisateurs locaux temporaires qui stockent les personnalisations des utilisateurs distants et à transférer les personnalisations vers les comptes d'utilisateurs SAML finaux.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Utilisateurs**.
3. Faites défiler jusqu'à l'utilisateur local que vous souhaitez supprimer et cliquez sur le **X** à l'extrême droite.
   a) Une option apparaît pour transférer les tableaux de bord, les collections et les cartes d'activité. (Sur une console, vous pouvez également transférer des rapports planifiés au cours de cette étape).
4. Sélectionnez **Transférer les tableaux de bord, les collections, les cartes d'activité et les rapports planifiés appartenant à a à l'utilisateur suivant** *<utilisateur local>*, puis sélectionnez le compte utilisateur SAML que vous avez créé. Par exemple, lorsque vous supprimez l'utilisateur local `john_smith_local`, vous pouvez transférer les personnalisations à l'utilisateur SAML `johnsmith`.
5. Répétez l'opération pour chaque utilisateur dont vous souhaitez conserver les personnalisations.