Migrer vers SAML depuis LDAP

Publié: 2024-07-02

L'authentification sécurisée par authentification unique (SSO) sur le système ExtraHop est facile à configurer. Toutefois, 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 (un espace de stockage des enregistrements est requis).

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

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

Aperçu 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 de planifier une période 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 façon inattendue pendant le processus de migration, le fichier d'exception est écrit sur le disque. Le fichier d'exception peut aider le support d'ExtraHop à diagnostiquer le problème à l'origine de l'échec.
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 un ordinateur local.

Parce que la modification de la méthode d'authentification à distance sur un sonde ou console supprime efficacement 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 fois, vous devez configurer SAML pour sonde ou console, puis transférez les paramètres une seconde fois des utilisateurs locaux aux utilisateurs SAML. Enfin, vous pouvez supprimer les utilisateurs locaux temporaires de sonde ou console.

Voici une explication de chaque étape :

1. Si vous prévoyez de ne migrer que quelques comptes via les paramètres d' administration, passez en revue les comptes d'utilisateurs distants existants sur identifier les utilisateurs grâce à des 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 utilisateur local temporaire pour chaque utilisateur distant que vous souhaitez préserver.
3. (Facultatif pour les utilisateurs de l'espace de stockage des enregistrements) Enregistrez les requêtes d'enregistrement créées par des utilisateurs distants dans le compte utilisateur de configuration.
4. Supprimer des utilisateurs distants et transférer leurs personnalisations sur le compte local.

5. Configuration de SAML. (Tous les utilisateurs distants et groupes d'utilisateurs restants sont supprimés avec leurs personnalisations.)
6. Créez un compte pour l'utilisateur SAML sur l'appliance. Une fois la sonde ou la console configurée pour SAML, vous pouvez créer un compte à distance pour vos utilisateurs avant qu'ils ne se connectent au système ExtraHop pour la première fois.
7. Supprimer le compte utilisateur local et transférer les personnalisations encore une fois, cette fois du compte local temporaire vers le compte utilisateur SAML. Lorsque vos utilisateurs SAML se connectent pour la première fois, leurs personnalisations seront disponibles.

Identifiez les utilisateurs distants et les groupes d'utilisateurs critiques

La migration étant un processus fastidieux via les paramètres d'administration, nous vous recommandons de limiter le nombre de comptes utilisateurs que vous conservez uniquement à ceux qui comportent des personnalisations complexes ou critiques pour l'entreprise. En outre, si vous avez importé des groupes d'utilisateurs LDAP, les tableaux de bord ou les cartes d'activité partagés avec ces groupes ne seront plus partagés une fois que vous aurez configuré SAML. Bien que les groupes d'utilisateurs ne puissent pas être importés depuis SAML, vous pouvez configurer et partager des personnalisations avec un groupe d'utilisateurs local sur le système ExtraHop.

- Dressez une liste des utilisateurs distants avec des tableaux de bord critiques, des cartes d'activité, des requêtes d'enregistrement enregistrées (magasins de disques uniquement) et des rapports planifiés (consoles uniquement)
- Afficher les groupes d'utilisateurs LDAP et leurs paramètres partagés, créer un groupe d'utilisateurs local, puis manuellement partager des tableaux de bord et cartes d'activités avec le groupe d'utilisateurs local après la migration vers SAML.

Associations de tableaux de

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

Dans la mesure où les tableaux de bord ne sont visibles que par les utilisateurs qui les ont créés ou par ceux qui ont des autorisations partagées, nous vous recommandons de suivre cette étape via le API REST.

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

Associations de cartes d'activités

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

Toutes les cartes d'activités sont visibles par les utilisateurs avec privilèges d'administration du système et des accès.

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

(Consoles uniquement) Associations de rapports planifiées

Vous devez récupérer les informations relatives à la propriété planifiée des rapports avant de configurer SAML sur votre système ExtraHop.

Tous les rapports sont visibles pour les utilisateurs avec 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 doté de privilèges illimités.
2. Cliquez sur l'icône Paramètres système, puis cliquez sur **Rapports planifiés**.
3. Identifiez tous les rapports que vous souhaitez conserver et notez l'utilisateur répertorié dans le Propriétaires colonne.

Enregistrer les requêtes d'enregistrement

Dans les étapes suivantes, vous allez apprendre à conserver les requêtes d'enregistrement enregistrées par un utilisateur distant.

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

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>` avec le `setup` compte utilisateur.
2. Cliquez sur l'icône Paramètres système, puis sélectionnez **Bundles**.
3. Sur la page Bundles, sélectionnez **Nouveau**.
4. Entrez un nom pour identifier le bundle.
5. Cliquez sur la flèche à côté de Requêtes dans le tableau des matières et cochez les cases à côté des requêtes enregistrées que vous souhaitez exporter.
6. Cliquez **OK.**. Le bundle apparaît dans le tableau de la page Bundles.
7. Sélectionnez le bundle et cliquez sur **Télécharger**. Les requêtes sont enregistrées dans un fichier JSON.

Prochaines étapes
Après la migration, télécharger le bundle pour restaurer les requêtes d'enregistrement enregistrées.

Créez un compte local temporaire

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

Nous vous recommandons de créer un nom d'utilisateur local qui ajoute _local au nom d'utilisateur distant existant. Par exemple, pour un 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 le Paramètres d'accès section, cliquez **Utilisateurs**.
3. Cliquez **Ajouter un utilisateur**.
4. Dans le Informations personnelles section, saisissez les informations suivantes :
   a) ID de connexion : nom d'utilisateur temporaire de l'utilisateur, qui ne peut contenir aucun espace.
   b) Nom complet : nom d'affichage de l'utilisateur, qui peut contenir des espaces.
   c) Mot de passe : 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 le Type d'authentification section, sélectionnez **Local**.
6. Dans le Type d'utilisateur section, sélectionnez le type de privilèges pour l'utilisateur.
7. Cliquez **Enregistrer**.

Supprimer des utilisateurs distants et transférer les personnalisations

Dans les paramètres d'administration, cette étape nécessite une procédure de suppression d'utilisateur spécifique, qui inclut la possibilité de transférer la propriété d'un seul compte utilisateur. Cette option est préférable si vous ne devez conserver que quelques personnalisations utilisateur. 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 passant de la méthode d'authentification à distance à SAML, la propriété ne peut pas être transférée.)

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez **Utilisateurs**.
3. Faites défiler la page jusqu'à l'utilisateur distant que vous souhaitez supprimer, puis cliquez sur **X** à l'extrême droite.
   a) Une option apparaît pour transférer les tableaux de bord, les collections et les cartes d'activité. (Sur un console, vous pouvez également transférer des rapports planifiés à cette étape.)
4. Sélectionnez **Transférez les tableaux de bord, les collections, les cartes d'activité et les rapports planifiés appartenant à un utilisateur à l'utilisateur suivant** *<remote user>* puis sélectionnez le compte utilisateur local temporaire que vous avez créé. Par exemple, lors de la suppression d'un 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, configurer SAML. Des guides sont disponibles pour les deux 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.

Créez des comptes SAML sur le système ExtraHop

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

Note: Vérifiez le format requis pour les noms d'utilisateur saisis dans ID de connexion champ avec l'administrateur de votre fournisseur d'identité. Si les noms d'utilisateur ne correspondent pas, l'utilisateur distant ne sera pas mis en correspondance avec 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 le Paramètres d'accès section, cliquez **Utilisateurs**.
3. Cliquez **Ajouter un utilisateur**.

4. Dans le ID de connexion dans ce champ, saisissez le nom d'utilisateur SAML. (Les noms d'utilisateur SAML distinguent les majuscules et minuscules.)
5. Dans le Nom complet dans ce champ, saisissez le prénom et le nom de famille de l'utilisateur.
6. Dans le Type d'authentification section, sélectionnez **télécommande**.
7. Cliquez **Enregistrer**.
8. Répétez l'opération pour chaque utilisateur dont vous souhaitez conserver les personnalisations.

Supprimer des utilisateurs locaux et transférer les personnalisations

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

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