Migrer vers SAML depuis LDAP via l'API REST

Publié: 2024-07-03

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 et les requêtes d'enregistrement.

Le référentiel GitHub d'ExtraHop fournit une série d'exemples de scripts qui vous montrent comment migrer en toute sécurité les personnalisations utilisateur d'utilisateurs distants vers SAML via l'API REST. Pour chaque script, vous devez remplacer les variables de script par des informations relatives à votre environnement.

Important: Les personnalisations doivent être enregistrées depuis l'appliance où les utilisateurs distants les ont créées. Par exemple, si un utilisateur distant possède un tableau de bord critique sur une machine virtuelle ECA et une sonde, vous devez effectuer ces procédures sur les deux appareils pour cet utilisateur distant.

Si vous préférez opter pour une solution clé en main pour la migration, contactez votre représentant commercial ExtraHop.

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 appareils. Si l'appliance 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 appareils. Les fichiers de sauvegarde incluent tous les utilisateurs, les personnalisations et les paramètres partagés. Téléchargez et stockez le fichier de sauvegarde sur un ordinateur local.

Étant donné que la modification de la méthode d'authentification à distance sur le système supprime effectivement tous les utilisateurs distants, vous devez créer des utilisateurs SAML sur le système avant de supprimer des utilisateurs distants. Vous pouvez ensuite transférer les personnalisations détenues par les utilisateurs distants aux utilisateurs SAML lorsque vous supprimez les utilisateurs distants.

Voici une explication de chaque étape :

1. Récupérez les métadonnées de partage pour les personnalisations créées par des utilisateurs distants.
2. (Facultatif pour les systèmes dotés d'un espace de stockage des enregistrements configuré) Enregistrer les requêtes d'enregistrement créé par des utilisateurs distants sur le compte utilisateur de configuration.
3. Récupérez utilisateurs distants et groupes d'utilisateurs.
4. Configuration de SAML sur le système. (Tous les utilisateurs distants et les groupes d'utilisateurs sont supprimés.)
5. Création de comptes utilisateur SAML pour chaque utilisateur distant qui a été supprimé. Une fois le système configuré pour SAML, vous pouvez créer un compte distant pour vos utilisateurs avant qu'ils ne se connectent à l'appliance pour la première fois.
6. Recréez des groupes d'utilisateurs locaux qui ont été supprimés.

7. Supprimer des comptes d'utilisateurs distants et transférer, personnaliser, partager les paramètres depuis les comptes d'utilisateurs distants vers les nouveaux comptes d'utilisateurs SAML. Lorsque vos utilisateurs SAML se connectent pour la première fois, leurs personnalisations seront disponibles.

Récupérez les métadonnées de partage pour les personnalisations des utilisateurs distants

Le référentiel GitHub d'ExtraHop contient un exemple de script qui récupère une liste des personnalisations des utilisateurs distants et des métadonnées de partage associées et enregistre les informations dans des fichiers JSON. Exécutez le script une fois pour chaque type de personnalisation après avoir remplacé les variables par des informations provenant de votre environnement.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `migrate_saml` répertoire vers votre machine locale.
2. Définissez les variables d'environnement suivantes :

   EXTRAHOP_HOST

   L'adresse IP ou le nom d'hôte de l'appliance.

   EXTRAHOP_API_KEY

   La clé API généré à partir de l'appliance.

   Par exemple, la commande Linux suivante définit le `EXTRAHOP_HOST` variable à `https://extrahop.example.com`:

   ```
   export EXTRAHOP_HOST=https://extrahop.example.com
   ```

3. Procédez comme suit pour les tableaux de bord et les cartes d'activité.
   a) Dans un éditeur de texte, ouvrez `retrieve_sharing.py` fichier et configurez les variables suivantes pour spécifier le type de personnalisation. Par exemple, pour récupérer les métadonnées d'un tableau de bord, spécifiez `OBJECT_TYPE=dashboards` et `OBJECT_FILE=dashboards.json`

      TYPE_OBJET

      Type de métadonnées de personnalisation à récupérer. Les valeurs suivantes sont valides :

      - `dashboards`
      - `activitymaps`

      FICHIER_SORTIE

      Nom du fichier JSON dans lequel enregistrer les métadonnées de personnalisation. Conservez ces fichiers sur votre ordinateur pour les saisir dans des scripts ultérieurement au cours de la migration.

      - `dashboards.json`
      - `activity_maps.json`

   b) Exécutez la commande suivante :

      ```
      python3 retrieve_sharing.py
      ```

      Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat SSL a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

      ```
      requests.get(url, headers=headers, verify=False)
      ```

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.

Récupérez des utilisateurs distants

Le référentiel GitHub d'ExtraHop contient un exemple de script qui récupère une liste d'utilisateurs distants et leurs métadonnées associées, puis enregistre les informations dans un fichier JSON nommé `user_map.json`.

Dans le `migrate_saml` répertoire téléchargé depuis le Référentiel GitHub d'exemples de code ExtraHop, exécutez la commande suivante :

```
python3 retrieve_remote_users.py
```

Important: Si une appliance contient des noms de compte utilisateur LDAP dupliqués, le script échouera et listera les noms dupliqués dans la sortie. Les noms de compte utilisateur LDAP distinguent les majuscules des minuscules, mais pas les noms de compte utilisateur SAML. Vous devez renommer les noms de compte utilisateur LDAP dupliqués avant de les migrer. Par exemple, si vous avez des noms d'utilisateur LDAP `user_1` et `User_1`, vous devez renommer l'un de ces comptes avant de migrer vers SAML.

Récupérez les groupes d'utilisateurs locaux

Le référentiel GitHub d'ExtraHop contient un exemple de script qui récupère une liste de groupes d'utilisateurs et de membres locaux, puis enregistre les informations dans un fichier JSON nommé `user_groups.json`.

Dans le `migrate_saml` répertoire téléchargé depuis le Référentiel GitHub d'exemples de code ExtraHop, exécutez la commande suivante :

```
python3 retrieve_local_user_groups.py
```

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.

Création de comptes utilisateur SAML

Le référentiel GitHub ExtraHop contient un exemple de script qui crée des comptes utilisateur SAML pour chaque compte utilisateur distant supprimé sur une appliance.

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 mis en correspondance avec l'utilisateur créé sur l'appliance.

Note: Le script génère des noms d'utilisateur SAML via `generateName()` méthode. Par défaut, le script crée de nouveaux noms d'utilisateur en ajoutant `@example.com` à la fin du nom d'utilisateur distant. Vous devez configurer la méthode pour générer des noms d'utilisateur conformément à la norme de dénomination de votre compte utilisateur SAML. Vérifiez comment formater les noms d'utilisateur auprès de l'administrateur de votre fournisseur d'identité.

Vous pouvez également spécifier des noms d'utilisateur SAML dans un fichier CSV. Pour configurer le script afin de récupérer les noms d'utilisateur d'un fichier CSV, définissez `READ_CSV_FILE` variable dans le script pour `True`. Le fichier CSV doit répondre aux exigences suivantes :

- Le fichier CSV ne doit pas contenir de ligne d'en-tête.
- Chaque ligne du fichier CSV doit contenir les deux colonnes suivantes dans l'ordre indiqué :

Nom d'utilisateur ExtraHop	Nom d'utilisateur SAML

- Le fichier CSV doit être nommé `remote_to_saml.csv` et se situer dans le même répertoire que le script Python. Le `migrate_saml` le répertoire contient un exemple de fichier CSV nommé `remote_to_saml.csv`.

Dans le `migrate_saml` répertoire téléchargé depuis le Référentiel GitHub d'exemples de code ExtraHop, exécutez la commande suivante :

```
python3 create_saml_accounts.py
```

Recréez des groupes d'utilisateurs locaux

Le référentiel GitHub ExtraHop contient un exemple de script qui rétablit l'adhésion des utilisateurs SAML à des groupes d'utilisateurs locaux.

Dans le `migrate_saml` répertoire téléchargé depuis le Référentiel GitHub d'exemples de code ExtraHop, exécutez la commande suivante :

```
python3 create_local_user_groups.py
```

Supprimer des comptes d'utilisateurs distants

Le référentiel GitHub d'ExtraHop contient un exemple de script qui supprime les comptes d'utilisateurs distants et transfère les personnalisations détenues par ces comptes d'utilisateurs vers des comptes utilisateur SAML.

Dans le `migrate_saml` répertoire téléchargé depuis le Référentiel GitHub d'exemples de code ExtraHop, exécutez la commande suivante :

```
python3 delete_remote_users.py
```

Transférer les paramètres de partage de personnalisation vers les comptes utilisateur SAML

Le référentiel GitHub d'ExtraHop contient un exemple de script qui transfère les paramètres de partage de personnalisation des comptes d'utilisateurs distants supprimés vers des comptes d'utilisateurs SAML. Exécutez le script une fois pour chaque type de personnalisation après avoir remplacé les variables par des informations provenant de votre environnement. Par exemple, si vous souhaitez conserver les paramètres partagés pour les tableaux de bord et les cartes d'activité, vous exécuterez le script une fois avec les variables de personnalisation pour les tableaux de bord et une fois avec les variables de personnalisation pour les cartes d'activité.

Dans le `migrate_saml` répertoire téléchargé depuis le Référentiel GitHub d'exemples de code ExtraHop, procédez comme suit pour les tableaux de bord, les cartes d'activité et les rapports.

a) Dans un éditeur de texte, ouvrez `transfer_sharing.py` fichier et configurez les variables suivantes pour spécifier le type de personnalisation. Par exemple, pour récupérer les métadonnées d'un tableau de bord, spécifiez `OBJECT_TYPE=dashboards` et `OBJECT_FILE=dashboards.json`

TYPE_OBJET

Type de personnalisation à transférer. Les valeurs suivantes sont valides :

- `dashboards`
- `activitymaps`
- `reports`

FICHIER_OBJET

Le nom du fichier JSON qui inclut métadonnées de personnalisation. Ces fichiers doivent se trouver dans le même répertoire que le script Python avec le `user_map.json` fichier contenant la liste des utilisateurs distants et le `user_groups.json` fichier contenant la liste des groupes d'utilisateurs. Les valeurs suivantes sont valides :

- `dashboards.json`
- `activity_maps.json`
- `reports.json`

b) Exécutez la commande suivante :

```
python3 transfer_sharing.py
```