Migrieren Sie von LDAP über die REST-API zu SAML

Veröffentlicht: 2024-03-27

Die sichere SSO-Authentifizierung (Single Sign-On) für das ExtraHop-System ist einfach zu konfigurieren. Wenn Sie Ihr ExtraHop-System jedoch für die Remote-Authentifizierung über LDAP, TACACS+ oder RADIUS konfiguriert haben, werden durch den Wechsel zu SAML alle vorhandenen Remote-Benutzer und ihre Anpassungen, wie gespeicherte Dashboards, Activity Maps, Berichte und Datensatzabfragen, dauerhaft gelöscht.

Das GitHub-Repository von ExtraHop bietet eine Reihe von Beispielskripten, die Ihnen zeigen, wie Sie Benutzeranpassungen über die REST-API sicher von Remote-Benutzern zu SAML migrieren können. Für jedes Skript müssen Sie die Skriptvariablen durch Informationen über Ihre Umgebung ersetzen.

Wichtig: Anpassungen müssen von der Appliance aus gespeichert werden, auf der sie von Remote-Benutzern erstellt wurden. Wenn ein Remote-Benutzer beispielsweise über ein wichtiges Dashboard auf einer ECA-VM und einen Sensor verfügt, müssen Sie diese Verfahren auf beiden Appliances für diesen Remote-Benutzer ausführen.

Wenn Sie eine schlüsselfertige Lösung für die Migration bevorzugen, wenden Sie sich an Ihren ExtraHop-Vertriebsmitarbeiter.

Überblick über das Verfahren

Die Migration zu einer neuen Fernauthentifizierungsmethode ist ein komplexer Prozess. Stellen Sie sicher, dass Sie alle Schritte verstanden haben, bevor Sie beginnen, und planen Sie ein Wartungsfenster ein, um Benutzer nicht zu stören.

Bevor Sie beginnen

1. Aktivieren Sie Ausnahmedateien auf Ihren Appliances. Wenn die Appliance während des Migrationsprozesses unerwartet stoppt oder neu gestartet wird, wird die Ausnahmedatei auf die Festplatte geschrieben. Die Ausnahmedatei kann dem ExtraHop-Support dabei helfen, das Problem zu diagnostizieren, das den Fehler verursacht hat.
2. Erstellen Sie ein Backup Ihrer Appliances. Zu den Sicherungsdateien gehören alle Benutzer, Anpassungen und gemeinsamen Einstellungen. Laden Sie die Sicherungsdatei herunter und speichern Sie sie auf einem lokalen Computer.

Da durch eine Änderung der Remoteauthentifizierungsmethode auf dem System effektiv alle Remotebenutzer gelöscht werden, müssen Sie SAML-Benutzer auf dem System erstellen, bevor Sie Remotebenutzer löschen. Sie können dann Anpassungen, die Remotebenutzern gehören, auf die SAML-Benutzer übertragen, wenn Sie die Remotebenutzer löschen.

Hier ist eine Erklärung der einzelnen Schritte:

1. Metadaten zum Teilen abrufen für Anpassungen, die von Remote-Benutzern erstellt wurden.
2. (Optional für Systeme mit einem konfigurierten Recordstore) Datensatzabfragen speichern von Remote-Benutzern für das Setup-Benutzerkonto erstellt.
3. Abrufen Remote-Benutzer und Benutzergruppen.
4. SAML konfigurieren auf dem System. (Alle Remotebenutzer und Benutzergruppen werden gelöscht.)
5. SAML-Benutzerkonten erstellen für jeden entfernten Benutzer, der gelöscht wurde. Nachdem das System für SAML konfiguriert wurde, können Sie ein Remote-Konto für Ihre Benutzer erstellen, bevor sie sich zum ersten Mal bei der Appliance anmelden.
6. Lokale Benutzergruppen neu erstellen die wurden gelöscht.

7. Löschen von Remotebenutzerkonten und Einstellungen für das Teilen von Benutzereinstellungen übertragen von den Remote-Benutzerkonten zu den neuen SAML-Benutzerkonten. Wenn sich Ihre SAML-Benutzer zum ersten Mal anmelden, sind ihre Anpassungen verfügbar.

Rufen Sie Freigabe-Metadaten für Anpassungen von Remotebenutzern ab

Das ExtraHop GitHub-Repository enthält ein Beispielskript, das eine Liste der Anpassungen von Remote-Benutzern und den zugehörigen Metadaten zum Teilen abruft und die Informationen in JSON-Dateien speichert. Führen Sie das Skript einmal für jede Art von Anpassung aus, nachdem Sie die Variablen durch Informationen aus Ihrer Umgebung ersetzt haben.

1. Gehe zum GitHub-Repository mit ExtraHop-Codebeispielen und laden Sie die `migrate_saml` Verzeichnis zu Ihrem lokalen Computer.
2. Legen Sie die folgenden Umgebungsvariablen fest:

   EXTRAHOP_HOST

   Die IP-Adresse oder der Hostname der Appliance.

   EXTRAHOP_API_KEY

   Der API-Schlüssel von der Appliance generiert.

   Mit dem folgenden Linux-Befehl wird beispielsweise der `EXTRAHOP_HOST` variabel zu `https://extrahop.example.com`:

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

3. Führen Sie die folgenden Schritte sowohl für Dashboards als auch für Aktivitätskarten aus.
   a) Öffnen Sie in einem Texteditor den `retrieve_sharing.py` Datei und konfigurieren Sie die folgenden Variablen, um den Anpassungstyp anzugeben. Um beispielsweise Dashboard-Metadaten abzurufen, geben Sie an `OBJECT_TYPE=dashboards` und `OBJECT_FILE=dashboards.json`

      OBJEKT_TYP

      Der Typ der abzurufenden Anpassungsmetadaten. Die folgenden Werte sind gültig:

      - `dashboards`
      - `activitymaps`

      AUSGABE_DATEI

      Der Name der JSON-Datei, in der Anpassungsmetadaten gespeichert werden sollen. Bewahren Sie diese Dateien auf Ihrem Computer auf, um sie später in der Migration in Skripts eingeben zu können.

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

   b) Führen Sie den folgenden Befehl aus:

      ```
      python3 retrieve_sharing.py
      ```

      Hinweis: Wenn das Skript eine Fehlermeldung zurückgibt, dass die SSL-Zertifikatsüberprüfung fehlgeschlagen ist, stellen Sie sicher, dass Ihrem Sensor oder Ihrer Konsole wurde ein vertrauenswürdiges Zertifikat hinzugefügt. Alternativ können Sie das hinzufügen `verify=False` Option zur Umgehung der Zertifikatsüberprüfung. Diese Methode ist jedoch nicht sicher und wird nicht empfohlen. Der folgende Code sendet eine HTTP GET-Anfrage ohne Zertifikatsüberprüfung:

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

Datensatzabfragen speichern

In den folgenden Schritten erfahren Sie, wie Sie von einem Remote-Benutzer gespeicherte Datensatzabfragen beibehalten können.

Da alle Systembenutzer auf gespeicherte Abfragen zugreifen können, können Sie alle gespeicherten Abfragen in ein Paket exportieren und sie dann nach der Migration zu SAML hochladen. Importierte Datensatzabfragen werden dem Benutzer zugewiesen, der das Paket hochlädt. (Wenn Sie beispielsweise Abfragen aus einem Paket importieren, während Sie als Setup-Benutzer angemeldet sind, wird in allen Abfragen das Setup als Eigentümer der Abfrage aufgeführt.) Nach der Migration können Remote-Benutzer die gespeicherten Datensatzabfragen anzeigen und eine Kopie für sich selbst speichern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>` mit dem `setup` Benutzerkonto.
2. Klicken Sie auf das Symbol Systemeinstellungen und wählen Sie dann **Bündel**.
3. Wählen Sie auf der Seite Bundles **Neu**.
4. Geben Sie einen Namen ein, um das Paket zu identifizieren.
5. Klicken Sie auf den Pfeil neben Abfragen in der Tabelle Inhalt und aktivieren Sie die Kontrollkästchen neben den gespeicherten Abfragen, die Sie exportieren möchten.
6. klicken **OK**. Das Paket wird in der Tabelle auf der Bundles-Seite angezeigt.
7. Wählen Sie das Paket aus und klicken Sie **Herunterladen**. Die Abfragen werden in einer JSON-Datei gespeichert.

Nächste Schritte
Nach der Migration lade das Paket hoch um die gespeicherten Datensatzabfragen wiederherzustellen.

Entfernte Benutzer abrufen

Das ExtraHop GitHub-Repository enthält ein Beispielskript, das eine Liste von Remote-Benutzern und ihren zugehörigen Metadaten abruft und die Informationen dann in einer JSON-Datei mit dem Namen speichert `user_map.json`.

In der `migrate_saml` Verzeichnis heruntergeladen von GitHub-Repository mit ExtraHop-Codebeispielen, führen Sie den folgenden Befehl aus:

```
python3 retrieve_remote_users.py
```

Wichtig: Wenn eine Appliance doppelte LDAP-Benutzerkontonamen enthält, schlägt das Skript fehl und listet die doppelten Namen in der Ausgabe auf. Bei LDAP-Benutzerkontonamen wird zwischen Groß- und Kleinschreibung unterschieden, bei SAML-Benutzerkontonamen jedoch nicht. Sie müssen doppelte LDAP-Benutzerkontonamen umbenennen, bevor Sie sie migrieren. Zum Beispiel, wenn Sie LDAP-Benutzernamen haben `user_1` und `User_1`, Sie müssen eines dieser Konten umbenennen, bevor Sie zu SAML migrieren.

Lokale Benutzergruppen abrufen

Das ExtraHop GitHub-Repository enthält ein Beispielskript, das eine Liste lokaler Benutzergruppen und Mitglieder abruft und die Informationen dann in einer JSON-Datei mit dem Namen speichert `user_groups.json`.

In der `migrate_saml` Verzeichnis heruntergeladen von GitHub-Repository mit ExtraHop-Codebeispielen, führen Sie den folgenden Befehl aus:

```
python3 retrieve_local_user_groups.py
```

SAML auf dem ExtraHop-System konfigurieren

Abhängig von Ihrer Umgebung SAML konfigurieren. Anleitungen sind für beide verfügbar Okta und Google. Nachdem Sie SAML auf Ihrem ExtraHop-System konfiguriert haben, können Sie Konten für Ihre Remote-Benutzer erstellen und deren Anpassungen übertragen, bevor sie sich zum ersten Mal anmelden.

SAML-Benutzerkonten erstellen

Das ExtraHop GitHub-Repository enthält ein Beispielskript, das SAML-Benutzerkonten für jedes gelöschte Remote-Benutzerkonto auf einer Appliance erstellt.

Hinweis: Überprüfen Sie das erforderliche Format für Benutzernamen, die in das Feld Anmelde-ID eingegeben werden, mit dem Administrator Ihres Identity Providers. Wenn die Benutzernamen nicht übereinstimmen, wird der Remote-Benutzer nicht dem auf der Appliance erstellten Benutzer zugeordnet.

Hinweis: Das Skript generiert SAML-Benutzernamen über den `generateName()` Methode. Standardmäßig erstellt das Skript neue Benutzernamen durch Anhängen `@example.com` bis zum Ende des Remote-Benutzernamens. Sie müssen die Methode zur Generierung von Benutzernamen gemäß Ihrem SAML-Benutzerkonten-Namensstandard konfigurieren. Erkundigen Sie sich beim Administrator Ihres Identity Providers, wie Benutzernamen formatiert werden.

Sie können auch SAML-Benutzernamen in einer CSV-Datei angeben. Um das Skript so zu konfigurieren, dass es Benutzernamen aus einer CSV-Datei abruft, setzen Sie `READ_CSV_FILE` Variable im Skript für `True`. Die CSV-Datei muss die folgenden Anforderungen erfüllen:

- Die CSV-Datei darf keine Kopfzeile enthalten.
- Jede Zeile der CSV-Datei muss die folgenden zwei Spalten in der angegebenen Reihenfolge enthalten:

ExtraHop-Benutzername	SAML-Benutzername

- Die CSV-Datei muss benannt werden `remote_to_saml.csv` und befinden sich im selben Verzeichnis wie das Python-Skript. Die `migrate_saml` Verzeichnis enthält eine CSV-Beispieldatei mit dem Namen `remote_to_saml.csv`.

In der `migrate_saml` Verzeichnis heruntergeladen von GitHub-Repository mit ExtraHop-Codebeispielen, führen Sie den folgenden Befehl aus:

```
python3 create_saml_accounts.py
```

Lokale Benutzergruppen neu erstellen

Das ExtraHop GitHub-Repository enthält ein Beispielskript, das die Mitgliedschaft von SAML-Benutzern in lokalen Benutzergruppen wiederherstellt.

In der `migrate_saml` Verzeichnis heruntergeladen von GitHub-Repository mit ExtraHop-Codebeispielen, führen Sie den folgenden Befehl aus:

```
python3 create_local_user_groups.py
```

Löschen von Remotebenutzerkonten

Das ExtraHop GitHub-Repository enthält ein Beispielskript, das Remote-Benutzerkonten löscht und die Anpassungen, die diesen Benutzerkonten gehören, auf SAML-Benutzerkonten überträgt.

In der `migrate_saml` Verzeichnis heruntergeladen von GitHub-Repository mit ExtraHop-Codebeispielen, führen Sie den folgenden Befehl aus:

```
python3 delete_remote_users.py
```

Einstellungen für die gemeinsame Nutzung von Anpassungen auf SAML-Benutzerkonten übertragen

Das ExtraHop GitHub-Repository enthält ein Beispielskript, das Einstellungen für die gemeinsame Nutzung von Anpassungen von gelöschten Remote-Benutzerkonten auf SAML-Benutzerkonten überträgt. Führen Sie das Skript einmal für jede Art von Anpassung aus, nachdem Sie die Variablen durch Informationen aus Ihrer Umgebung ersetzt haben. Wenn Sie beispielsweise gemeinsame Einstellungen für Dashboards und Activity Maps beibehalten möchten, führen Sie das Skript einmal mit den Anpassungsvariablen für Dashboards und einmal mit den Anpassungsvariablen für Activity Maps aus.

In der `migrate_saml` Verzeichnis heruntergeladen von GitHub-Repository mit ExtraHop-Codebeispielen, führen Sie die folgenden Schritte für Dashboards, Aktivitätskarten und Berichte aus.

a) Öffnen Sie in einem Texteditor `transfer_sharing.py` Datei und konfigurieren Sie die folgenden Variablen, um den Anpassungstyp anzugeben. Um beispielsweise Dashboard-Metadaten abzurufen, geben Sie an `OBJECT_TYPE=dashboards` und `OBJECT_FILE=dashboards.json`

OBJEKTTYP

Die Art der zu übertragenden Anpassung. Die folgenden Werte sind gültig:

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

OBJEKTDATEI

Der Name der JSON-Datei, die den Metadaten zur Anpassung. Diese Dateien müssen sich im selben Verzeichnis wie das Python-Skript befinden, zusammen mit dem `user_map.json` Datei, die enthält die Liste der Remote-Benutzer und der `user_groups.json` Datei, die enthält die Liste der Benutzergruppen. Die folgenden Werte sind gültig:

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

b) Führen Sie den folgenden Befehl aus:

```
python3 transfer_sharing.py
```