Von LDAP zu SAML migrieren

Veröffentlicht: 2023-09-30

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 dauerhaft gelöscht, z. B. gespeicherte Dashboards, Aktivitätskarten, Berichte (nur auf Konsolen verfügbar) und Datensatzabfragen (Recordstore ist erforderlich).

Die Migration ist ein mehrstufiger Prozess. In jedem Abschnitt finden Sie die Schritte zur sicheren Migration eines einzelnen Benutzers und seiner Anpassungen über die Administrationseinstellungen von LDAP zu SAML. Wenn Sie eine große Anzahl von Remote-Benutzern mit Anpassungen migrieren müssen, empfehlen wir dringend, zu SAML zu migrieren. über die REST-API. Wenn Sie eine schlüsselfertige Lösung für die Migration bevorzugen, wenden Sie sich an Ihren ExtraHop-Vertriebsmitarbeiter.

Wichtig: Anpassungen müssen dort gespeichert werden, wo Remotebenutzer sie erstellt haben. Wenn ein Remote-Benutzer beispielsweise ein wichtiges Dashboard auf einer Konsole und einen Sensor hat, müssen Sie diese Verfahren sowohl auf der Konsole als auch auf dem Sensor für diesen Remote-Benutzer ausführen.

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 Sensoren und Ihrer Konsole. Wenn das ExtraHop-System während des Migrationsprozesses unerwartet stoppt oder neu startet, 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 Sensoren und Konsole. Zu den Sicherungsdateien gehören alle Benutzer, Anpassungen und gemeinsamen Einstellungen. Laden Sie die Sicherungsdatei herunter und speichern Sie sie außerhalb des Systems auf einem lokalen Computer.

Weil das Ändern der Fernauthentifizierungsmethode auf einem Sensor oder Konsole löscht effektiv alle Remote-Benutzer. Sie müssen zunächst für jeden Remote-Benutzer einen (gespiegelten) lokalen Benutzer erstellen, auf den Sie Anpassungen und Freigabeeinstellungen vorübergehend übertragen können. Nachdem Sie diese Einstellungen einmal übertragen haben, müssen Sie SAML konfigurieren für Sensor oder Konsole, und übertragen Sie dann die Einstellungen ein zweites Mal von den lokalen Benutzern auf die SAML-Benutzer. Schließlich können Sie die temporären lokalen Benutzer aus dem löschen Sensor oder Konsole.

Hier ist eine Erklärung der einzelnen Schritte:

1. Wenn Sie planen, nur einige ausgewählte Konten über die Administrationseinstellungen zu migrieren, überprüfen Sie die vorhandenen Remotebenutzerkonten unter Benutzer mit Anpassungen identifizieren die Sie beibehalten möchten, und identifizieren Sie die Benutzergruppen, denen gemeinsame Berechtigungen für Anpassungen erteilt wurden.
2. Erstellen Sie ein temporäres lokales Benutzerkonto für jeden Remote-Benutzer die du bewahren willst.
3. (Optional für Recordstore-Benutzer) Speichern Sie Datensatzabfragen, die von Remote-Benutzern erstellt wurden, im Setup-Benutzerkonto.
4. Löschen Sie Remote-Benutzer und übertragen Sie ihre Anpassungen auf das lokale Konto.
5. SAML konfigurieren. (Alle verbleibenden Remotebenutzer und Benutzergruppen werden zusammen mit ihren Anpassungen gelöscht.)

6. Erstellen Sie ein Konto für den SAML-Benutzer auf der Appliance. Nachdem der Sensor oder die Konsole für SAML konfiguriert wurde, können Sie ein Remote-Konto für Ihre Benutzer erstellen, bevor sie sich zum ersten Mal beim ExtraHop-System anmelden.
7. Löschen Sie das lokale Benutzerkonto und übertragen Sie die Anpassungen wieder, diesmal vom temporären lokalen Konto zum SAML-Benutzerkonto. Wenn sich Ihre SAML-Benutzer zum ersten Mal anmelden, sind ihre Anpassungen verfügbar.

Identifizieren Sie kritische Remote-Benutzer und Benutzergruppen

Da die Migration über die Administrationseinstellungen ein zeitaufwändiger Prozess ist, empfehlen wir, die Anzahl der Benutzerkonten, die Sie behalten, auf solche mit komplexen oder geschäftskritischen Anpassungen zu beschränken. Wenn Sie LDAP-Benutzergruppen importiert haben, werden außerdem alle Dashboards oder Aktivitätskarten, die mit diesen Gruppen geteilt wurden, nach der Konfiguration von SAML nicht mehr geteilt. Benutzergruppen können zwar nicht aus SAML importiert werden, Sie können jedoch Anpassungen konfigurieren und mit einer lokalen Benutzergruppe auf dem ExtraHop-System teilen.

- Erstellen Sie eine Liste von Remote-Benutzern mit wichtigen Dashboards, Aktivitätskarten, gespeicherten Datensatzabfragen (nur Datensatzspeicher) und Dashboard-Berichten (nur Konsolen)
- LDAP-Benutzergruppen anzeigen und ihre gemeinsamen Einstellungen, eine lokale Benutzergruppe erstellen, und dann manuell Dashboards teilen und Aktivitätskarten mit der lokalen Benutzergruppe nach der Migration zu SAML.

Dashboard-Verknüpfungen

Sie müssen Informationen über den Besitz und die gemeinsame Nutzung von Dashboard abrufen, bevor Sie SAML auf Ihrem ExtraHop-System konfigurieren.

Da Dashboards nur für die Benutzer sichtbar sind, die sie erstellt haben, oder für Benutzer, die über geteilte Berechtigungen verfügen, empfehlen wir Ihnen, diesen Schritt über die REST-API.

Wenn Sie diesen Schritt über die Administrationseinstellungen ausführen müssen, muss jeder Remote-Benutzer manuell ihr Dashboard teilen mit einem lokalen Benutzer.

Assoziationen auf der Aktivitätskarte

Sie können Informationen über den Besitz und die gemeinsame Nutzung von Aktivitätsdiagramm abrufen, bevor Sie SAML auf Ihrer Appliance konfigurieren.

Alle Aktivitätskarten sind für Benutzer sichtbar mit System- und Zugriffsadministrationsrechte.

1. <extrahop-hostname-or-IP-address>Melden Sie sich über https://beim ExtraHop-System an.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. klicken **Aktivität** im linken Bereich und klicken Sie dann auf die Gruppe von Clients, Servern oder Geräten für das gewünschte Protokoll.
4. klicken **Karte der Aktivitäten**, befindet sich in der Nähe der oberen rechten Ecke der Seite.
5. Klicken Sie auf **Laden** Symbol 🗁 in der oberen rechten Ecke.
6. Notieren Sie sich jeden Besitzer der Aktivitätsdiagramm.
7. Identifizieren Sie die Eigenschaften der Aktivitätsdiagramm und die Freigabeoptionen für jede Aktivitätskarte.
   a) Klicken Sie auf den Namen der Aktivitätsdiagramm.
   b) Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke und wählen Sie dann **Teilen**.
   c) Notieren Sie sich alle Benutzer oder Gruppen, mit denen die Aktivitätsdiagramm geteilt wird.

(Nur Konsolen) Verknüpfungen von Dashboard-Berichten

Sie müssen Informationen über den Besitz von geplanten Dashboard-Berichten abrufen, bevor Sie SAML auf Ihrem ExtraHop-System konfigurieren.

Alle Berichte sind sichtbar für Benutzer mit System- und Zugriffsadministrationsrechte.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>` mit einem Benutzerkonto mit unbegrenzten Rechten.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Dashboard-Berichte**.
3. Identifizieren Sie alle Dashboard-Berichte, die Sie beibehalten möchten, und notieren Sie sich den Benutzer , der in der Besitzer Spalte.

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.

Erstellen Sie ein temporäres lokales Konto

In den folgenden Schritten erfahren Sie, wie Sie ein lokales Benutzerkonto als Spiegelbild eines Remote-Benutzerkontos erstellen.

Wir empfehlen Ihnen, einen lokalen Benutzernamen zu erstellen, der _local an den vorhandenen Remote-Benutzernamen anhängt. Zum Beispiel für LDAP-Benutzer `john_smith`, erstellen Sie einen lokalen Benutzer mit dem Namen `john_smith_local`.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Zugriffs-Einstellungen Abschnitt, klicken **Nutzer**.
3. klicken **Nutzer hinzufügen**.
4. In der Personenbezogene Daten Abschnitt, geben Sie die folgenden Informationen ein:
   a) Login-ID: Der temporäre Benutzername für den Benutzer, der keine Leerzeichen enthalten darf.
   b) Vollständiger Name: Ein Anzeigename für den Benutzer, der Leerzeichen enthalten kann.
   c) Passwort: Das Passwort für dieses Konto.
   d) Passwort bestätigen: Geben Sie das Passwort erneut aus dem Feld Passwort ein.
5. In der Art der Authentifizierung Abschnitt, wählen **Lokal**.
6. In der Benutzertyp Abschnitt, wählen Sie den Typ von Privilegien für den Benutzer.
7. klicken **Speichern**.

Entfernte Benutzer löschen und Anpassungen übertragen

In den Administrationseinstellungen erfordert dieser Schritt ein bestimmtes Verfahren zum Löschen eines Benutzers, das die Option beinhaltet, den Besitz für ein einzelnes Benutzerkonto zu übertragen. Diese Option ist am besten geeignet, wenn Sie nur wenige Benutzeranpassungen haben, die beibehalten werden müssen. Beachten Sie, dass Sie in der REST-API zuerst jede Anpassung übertragen und dann den Benutzer separat löschen müssen. Wenn Sie alle Benutzer löschen, indem Sie die Remoteauthentifizierungsmethode auf SAML umstellen, kann der Besitz nicht übertragen werden.)

In den folgenden Schritten erfahren Sie, wie Sie Anpassungen auf das temporäre lokale Konto übertragen, das Sie beim Löschen des zugehörigen Remote-Benutzers erstellt haben.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Nutzer**.
3. Scrollen Sie zu dem Remote-Benutzer, den Sie löschen möchten, und klicken Sie auf **X** ganz rechts.
   a) Es wird eine Option zum Übertragen von Dashboards, Sammlungen und Aktivitätskarten angezeigt. (Auf einem Konsole, in diesem Schritt können Sie auch geplante Berichte übertragen.)
4. Wählen **Übertragen Sie Dashboards, Sammlungen, Aktivitätskarten und geplante Berichte, die einem gehören, an den folgenden Benutzer** *<remote user>* und wählen Sie dann das temporäre lokale Benutzerkonto aus, das Sie erstellt haben. Zum Beispiel beim Löschen eines Remote-Benutzers `john_smith` Sie können Anpassungen an lokale Benutzer übertragen `john_smith_local`.
5. Wiederholen Sie den Vorgang für jeden Benutzer, dessen Anpassungen Sie beibehalten möchten.

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.

Erstellen Sie SAML-Konten auf dem ExtraHop-System

In den folgenden Schritten erfahren Sie, wie Sie einen SAML-Benutzer auf Ihrem ExtraHop-System erstellen.

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

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen aufrufen Abschnitt, klicken **Nutzer**.
3. klicken **Nutzer hinzufügen**.
4. In der Anmelde-ID Feld, geben Sie den SAML-Benutzernamen ein. (Bei SAML-Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden.)
5. In der Vollständiger Name Feld, geben Sie den Vor- und Nachnamen des Benutzers ein.
6. In der Art der Authentifizierung Abschnitt, wählen **Fernsteuerung**.
7. klicken **Speichern**.
8. Wiederholen Sie den Vorgang für jeden Benutzer, dessen Anpassungen Sie beibehalten möchten.

Lokale Benutzer löschen und Anpassungen übertragen

In den folgenden Schritten erfahren Sie, wie Sie die temporären lokalen Benutzerkonten löschen, in denen Remotebenutzeranpassungen gespeichert sind, und wie Sie die Anpassungen auf die endgültigen SAML-Benutzerkonten übertragen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Zugriffs-Einstellungen Abschnitt, klicken **Nutzer**.
3. Scrollen Sie zu dem lokalen Benutzer, den Sie löschen möchten, und klicken Sie auf **X** ganz rechts.
   a) Es wird eine Option zum Übertragen von Dashboards, Sammlungen und Aktivitätskarten angezeigt. (Auf einem Konsole, in diesem Schritt können Sie auch geplante Berichte übertragen.)
4. Wählen **Übertragen Sie Dashboards, Sammlungen, Aktivitätskarten und Dashboard-Berichte, die einem gehören, an den folgenden Benutzer** *<local user>* und wählen Sie dann das von Ihnen erstellte SAML-Benutzerkonto aus. Zum Beispiel beim Löschen eines lokalen Benutzers `john_smith_local` Sie können Anpassungen an den SAML-Benutzer übertragen `johnsmith`.
5. Wiederholen Sie den Vorgang für jeden Benutzer, dessen Anpassungen Sie beibehalten möchten.