Konfigurieren Sie die Fernauthentifizierung über LDAP

Veröffentlicht: 2024-11-03

Das ExtraHop-System unterstützt das Lightweight Directory Access Protocol (LDAP) zur Authentifizierung und Autorisierung. Anstatt Benutzeranmeldedaten lokal zu speichern, können Sie Ihr ExtraHop-System so konfigurieren, dass Benutzer remote mit einem vorhandenen LDAP-Server authentifiziert werden. Beachten Sie, dass die ExtraHop-LDAP-Authentifizierung nur Benutzerkonten abfragt; sie fragt keine anderen Entitäten ab, die sich möglicherweise im LDAP-Verzeichnis befinden.

Bevor Sie beginnen

- Für dieses Verfahren müssen Sie mit der Konfiguration von LDAP vertraut sein.
- Stellen Sie sicher, dass sich jeder Benutzer in einer berechtigungsspezifischen Gruppe auf dem LDAP-Server befindet, bevor Sie mit diesem Verfahren beginnen.
- Wenn Sie verschachtelte LDAP-Gruppen konfigurieren möchten, müssen Sie die Datei Running Configuration ändern. Kontakt ExtraHop-Unterstützung für Hilfe.

Wenn ein Benutzer versucht, sich bei einem ExtraHop-System anzumelden, versucht das ExtraHop-System, den Benutzer auf folgende Weise zu authentifizieren:

- Versucht, den Benutzer lokal zu authentifizieren.
- Versucht, den Benutzer über den LDAP-Server zu authentifizieren, wenn der Benutzer nicht lokal existiert und wenn das ExtraHop-System für die Fernauthentifizierung mit LDAP konfiguriert ist.
- Meldet den Benutzer im ExtraHop-System an, wenn der Benutzer existiert und das Passwort entweder lokal oder über LDAP validiert wurde. Das LDAP-Passwort wird nicht lokal auf dem ExtraHop-System gespeichert. Beachten Sie, dass Sie den Benutzernamen und das Passwort in dem Format eingeben müssen, für das Ihr LDAP-Server konfiguriert ist. Das ExtraHop-System leitet die Informationen nur an den LDAP-Server weiter.
- Wenn der Benutzer nicht existiert oder ein falsches Passwort eingegeben wurde, erscheint eine Fehlermeldung auf der Anmeldeseite.

> **Wichtig:** Wenn Sie die LDAP-Authentifizierung zu einem späteren Zeitpunkt auf eine andere Methode der Fernauthentifizierung umstellen, werden die Benutzer, Benutzergruppen und zugehörigen Anpassungen, die über die Remote-Authentifizierung erstellt wurden, entfernt. Lokale Benutzer sind nicht betroffen.

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 **Fernauthentifizierung**.
3. Aus dem Methode der Fernauthentifizierung Dropdownliste, wählen **LDAP** und klicken Sie dann **Weiter**.
4. Auf dem LDAP-Einstellungen Seite, füllen Sie die folgenden Serverinformationsfelder aus:
   a) In der Hostname Feld, geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers ein. Wenn Sie einen Hostnamen konfigurieren, stellen Sie sicher, dass der DNS-Eintrag des ExtraHop-Systems richtig konfiguriert ist.
   b) In der Hafen In diesem Feld geben Sie die Portnummer ein, auf der der LDAP-Server lauscht.
   c) Aus dem **Servertyp** Dropdownliste, wählen **Posix** oder **Aktives Verzeichnis**.
   d) Optional: In der Binden Sie DN Feld, geben Sie den Bindungs-DN ein. Der Bind-DN sind die Benutzeranmeldedaten, mit denen Sie sich beim LDAP-Server authentifizieren können, um die Benutzersuche durchzuführen. Der Bind-DN muss Listenzugriff auf den Basis-DN und alle Organisationseinheiten, Gruppen oder Benutzerkonto haben, die für die LDAP-Authentifizierung erforderlich sind. Wenn dieser Wert nicht gesetzt ist, wird eine anonyme Bindung durchgeführt. Beachten Sie, dass anonyme Bindungen nicht auf allen LDAP-Servern aktiviert sind.

e) Optional: In der Passwort binden Feld, geben Sie das Bindungskennwort ein. Das Bind-Passwort ist das Passwort, das für die Authentifizierung beim LDAP-Server als den oben angegebenen Bind-DN erforderlich ist. Wenn Sie eine anonyme Bindung konfigurieren, lassen Sie dieses Feld leer. In einigen Fällen ist eine nicht authentifizierte Bindung möglich, bei der Sie einen Bind-DN-Wert, aber kein Bind-Passwort angeben. Fragen Sie Ihren LDAP-Administrator nach den richtigen Einstellungen.

f) Aus dem **Verschlüsselung** Wählen Sie in der Dropdownliste eine der folgenden Verschlüsselungsoptionen aus.

- **Keine:** Diese Option spezifiziert Klartext-TCP-Sockets. In diesem Modus werden alle Passwörter im Klartext über das Netzwerk gesendet.
- **SPRÜNGE:** Diese Option gibt LDAP an, das in TLS eingeschlossen ist.
- **TLS starten:** Diese Option spezifiziert TLS LDAP. (TLS wird ausgehandelt, bevor Passwörter gesendet werden.)

g) Wählen **SSL-Zertifikate validieren** um die Zertifikatsvalidierung zu aktivieren. Wenn Sie diese Option auswählen, wird das Zertifikat auf dem Remote-Endpunkt anhand der Stammzertifikate überprüft, die vom Trusted Certificates Manager angegeben wurden. Auf der Seite Vertrauenswürdige Zertifikate müssen Sie konfigurieren, welchen Zertifikaten Sie vertrauen möchten. Weitere Informationen finden Sie unter Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu.

h) In der Aktualisierungsintervall Feld, geben Sie einen Zeitwert ein oder belassen Sie die Standardeinstellung von 1 Stunde.

Das Aktualisierungsintervall stellt sicher, dass alle Änderungen am Benutzer- oder Gruppenzugriff auf dem LDAP-Server auf dem ExtraHop-System aktualisiert werden.

5. Konfigurieren Sie die folgenden Benutzereinstellungen:

a) In der Basis DN Feld, geben Sie den eindeutigen Basisnamen (DN) ein.

Der Basis-DN ist der Punkt, von dem aus ein Server nach Benutzern sucht. Der Basis-DN muss alle Benutzerkonten enthalten, die Zugriff auf das ExtraHop-System haben werden. Die Benutzer können direkte Mitglieder des Basis-DN sein oder innerhalb einer Organisationseinheit innerhalb des Basis-DN verschachtelt sein, wenn **Gesamter Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

b) In der Suchfilter Feld, geben Sie einen Suchfilter ein.

Mithilfe von Suchfiltern können Sie Suchkriterien definieren, wenn Sie das LDAP-Verzeichnis nach Benutzerkonten durchsuchen.

Wichtig: Das ExtraHop-System fügt automatisch Klammern hinzu, um den Filter zu umschließen, und analysiert diesen Parameter nicht korrekt, wenn Sie Klammern manuell hinzufügen. Fügen Sie in diesem Schritt und in Schritt 5b Ihre Suchfilter hinzu, ähnlich dem folgenden Beispiel:

```
cn=atlas*
|(cn=EH-*)(cn=IT-*)
```

Wenn Ihre Gruppennamen außerdem das Sternchen (*) enthalten, muss das Sternchen als maskiert werden `\2a`. Zum Beispiel, wenn Ihre Gruppe eine CN mit dem Namen hat `test*group`, typ `cn=test\2agroup` im Feld Suchfilter.

c) Aus dem **Umfang der Suche** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus.

Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzerentitäten an.

- **Ganzer Unterbaum:** Diese Option sucht rekursiv unter dem Gruppen-DN nach passenden Benutzern.
- **Einstufig:** Diese Option sucht nur nach Benutzern, die im Basis-DN existieren, nicht nach Unterbäumen.

6. Optional: Um Benutzergruppen zu importieren, wählen Sie das **Benutzergruppen vom LDAP-Server importieren** setzen Sie ein Häkchen und konfigurieren Sie die folgenden Einstellungen.

   Hinweis: Durch den Import von LDAP-Benutzergruppen können Sie Dashboards mit diesen Gruppen teilen. Die importierten Gruppen werden auf der Seite Benutzergruppe in den Administrationseinstellungen angezeigt.

   a) In der Basis DN Feld, geben Sie den Basis-DN ein.

   Der Basis-DN ist der Punkt, von dem aus ein Server nach Benutzergruppen sucht. Der Basis-DN muss alle Benutzergruppen enthalten, die Zugriff auf das ExtraHop-System haben werden. Die Benutzergruppen können direkte Mitglieder des Basis-DN sein oder innerhalb einer Organisationseinheit innerhalb des Basis-DN verschachtelt sein, wenn **Gesamter Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

   b) In der Suchfilter Feldtyp einen Suchfilter.

   Mithilfe von Suchfiltern können Sie Suchkriterien definieren, wenn Sie das LDAP-Verzeichnis nach Benutzergruppen durchsuchen.

   Wichtig: Bei Gruppensuchfiltern filtert das ExtraHop-System implizit nach objectclass=group, weshalb objectclass=group diesem Filter nicht hinzugefügt werden sollte.

   c) Aus dem **Umfang der Suche** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus.

   Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzergruppenentitäten an.

   • **Ganzer Unterbaum:** Diese Option sucht rekursiv unter dem Basis-DN nach passenden Benutzergruppen.

   • **Einstufig:** Diese Option sucht nach Benutzergruppen, die im Basis-DN existieren, nicht nach Unterbäumen.

7. klicken **Einstellungen testen**.

   Wenn der Test erfolgreich ist, wird unten auf der Seite eine Statusmeldung angezeigt. Wenn der Test fehlschlägt, klicken Sie auf **Zeige Details** um eine Liste der Fehler zu sehen. Sie müssen alle Fehler beheben, bevor Sie fortfahren.

8. Klicken Sie **Speichern und fortfahren**.

Nächste Schritte
Benutzerrechte für die Fernauthentifizierung konfigurieren

Benutzerrechte für die Fernauthentifizierung konfigurieren

Sie können einzelnen Benutzern in Ihrem ExtraHop-System Benutzerrechte zuweisen oder Rechte über Ihren LDAP-Server konfigurieren und verwalten.

Wenn Sie Benutzerberechtigungen über LDAP zuweisen, müssen Sie mindestens eines der verfügbaren Benutzerberechtigungsfelder ausfüllen. Für diese Felder sind Gruppen (keine Organisationseinheiten) erforderlich , die auf Ihrem LDAP-Server vordefiniert sind. Ein Benutzerkonto mit Zugriff muss ein direktes Mitglied einer bestimmten Gruppe sein. Benutzerkonten, die nicht Mitglied einer oben angegebenen Gruppe sind, haben keinen Zugriff. Gruppen, die nicht anwesend sind, werden im ExtraHop-System nicht authentifiziert.

Das ExtraHop-System unterstützt sowohl Active Directory- als auch POSIX-Gruppenmitgliedschaften. Für Active Directory `memberOf` wird unterstützt. Für POSIX `memberuid`, `posixGroups`, `groupofNames`, und `groupofuniqueNames` werden unterstützt.

1. Wählen Sie eine der folgenden Optionen aus dem Optionen für die Zuweisung von Rechten Dropdownliste:

   - **Berechtigungsstufe vom Remoteserver abrufen**

Diese Option weist Rechte über Ihren Remote-Authentifizierungsserver zu. Sie müssen mindestens eines der folgenden Distinguished Name (DN) -Felder ausfüllen.

• **System- und Zugriffsverwaltung DN:** Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System, einschließlich der Administrationseinstellungen.

• **Vollständiger Schreib-DN:** Erstellen und ändern Sie Objekte auf dem ExtraHop-System, ohne die Administrationseinstellungen.

• **Eingeschränkte Schreib-DN:** Erstellen, ändern und teilen Sie Dashboards.

• **Persönliches Schreiben DN:** Erstellen Sie persönliche Dashboards und ändern Sie Dashboards, die mit dem angemeldeten Benutzer geteilt werden.

• **Vollständiger schreibgeschützter DN:** Objekte im ExtraHop-System anzeigen.

• **Eingeschränkter schreibgeschützter DN:** Sehen Sie sich Dashboards an, die mit dem angemeldeten Benutzer geteilt wurden.

• **Packet Slices Access DN:** Zeigen Sie die ersten 64 Byte an Paketen an, die über die ExtraHop Trace-Appliance erfasst wurden, und laden Sie sie herunter.

• **Paketzugriffs-DN:** Über die ExtraHop Trace-Appliance erfasste Pakete anzeigen und herunterladen.

• **Paket- und Sitzungsschlüssel Access DN:** Pakete und alle zugehörigen TLS-Sitzungsschlüssel, die über die ExtraHop Trace-Appliance erfasst wurden, anzeigen und herunterladen.

• **NDR-Modulzugriff DN:** Sicherheitserkennungen, die im ExtraHop-System erscheinen, anzeigen, bestätigen und ausblenden.

• **NPM-Modulzugriffs-DN:** Leistungserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und ausblenden.

- **Remote-Benutzer haben vollen Schreibzugriff**

  Diese Option gewährt Remote-Benutzern vollen Schreibzugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
- **Remote-Benutzer haben vollen Lesezugriff**

  Diese Option gewährt Remote-Benutzern schreibgeschützten Zugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.

2. Optional: Konfigurieren Sie den Zugriff auf Paket und Sitzungsschlüssel. Wählen Sie eine der folgenden Optionen, um Remote-Benutzern das Herunterladen von Paketerfassungen und TLS-Sitzungsschlüsseln zu ermöglichen.
   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
3. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff.
   - **Kein Zugriff**
   - **Voller Zugriff**
4. Klicken Sie **Speichern und fertig**.
5. Klicken Sie **Erledigt**.