Konfigurieren Sie die Remote-Authentifizierung über LDAP

Veröffentlicht: 2024-04-10

Das ExtraHop-System unterstützt das Lightweight Directory Access Protocol (LDAP) für 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 nicht nach anderen Entitäten ab, die sich möglicherweise im LDAP-Verzeichnis befinden.

Bevor Sie beginnen

- Dieses Verfahren erfordert Vertrautheit mit der Konfiguration von LDAP.
- 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 um 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 beim 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 Remoteauthentifizierungsmethode ändern, werden die Benutzer, Benutzergruppen und zugehörigen Anpassungen, die durch die Remoteauthentifizierung erstellt wurden, entfernt. Lokale Benutzer sind davon nicht betroffen.

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 **Fernauthentifizierung**.
3. Aus dem Methode zur Fernauthentifizierung Drop-down-Liste, wählen **LDAP** und dann klicken **Weiter**.
4. Auf dem LDAP-Einstellungen Seite, füllen Sie die folgenden Felder mit Serverinformationen 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 Feld, geben Sie die Portnummer ein, auf der der LDAP-Server lauscht.
   c) Aus dem Typ des Servers Drop-down-Liste, wählen **Posix** oder **Active Directory**.
   d) Optional: In der DN binden Feld, geben Sie den Bind-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 für die LDAP-Authentifizierung erforderlichen Organisationseinheiten, Gruppen oder Benutzerkonto haben. 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 Bind-Passwort ein. Das Bind-Passwort ist das Passwort, das für die Authentifizierung mit dem LDAP-Server als dem 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. Erkundigen Sie sich bei Ihrem 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.
- **LAPPEN:** Diese Option spezifiziert LDAP, das in SSL eingeschlossen ist.
- **Starten Sie TLS:** Diese Option spezifiziert TLS LDAP. (SSL 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 vom Trusted Certificates Manager angegebenen Stammzertifikate validiert. Sie müssen auf der Seite Vertrauenswürdige Zertifikate konfigurieren, welchen Zertifikaten Sie vertrauen möchten. Weitere Informationen finden Sie unter Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu.

h) Geben Sie einen Zeitwert in das Aktualisierungsintervall Feld oder belassen Sie die Standardeinstellung von 1 Stunde. Das Aktualisierungsintervall stellt sicher, dass alle Änderungen, die am Benutzer- oder Gruppenzugriff auf dem LDAP-Server vorgenommen werden, auf dem ExtraHop-System aktualisiert werden.

5. Konfigurieren Sie die folgenden Benutzereinstellungen:

a) Geben Sie den Basis-DN in das Basis-DN Feld. 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. Die Benutzer können direkte Mitglieder des Basis-DN sein oder innerhalb einer OU innerhalb des Basis-DN verschachtelt sein, wenn **Ganzer Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

b) Geben Sie einen Suchfilter in das Suchfilter Feld. 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 einzuschließen, und analysiert diesen Parameter nicht korrekt, wenn Sie Klammern manuell hinzufügen. Fügen Sie Ihre Suchfilter in diesem Schritt und in Schritt 5b hinzu, ähnlich dem folgenden Beispiel:

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

Wenn Ihre Gruppennamen das Sternchen (*) enthalten, muss das Sternchen außerdem maskiert werden als `\2a`. Zum Beispiel, wenn Ihre Gruppe eine CN namens 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 Teilbaum:** 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: Benutzergruppen importieren. Wählen Sie den **Benutzergruppen vom LDAP-Server importieren** kreuzen Sie das Kästchen an 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) Geben Sie den Basis-DN in das Basis-DN Feld. 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. Die Benutzergruppen können direkte Mitglieder des Basis-DN sein oder innerhalb einer OU innerhalb des Basis-DN verschachtelt sein, wenn **Ganzer Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

b) Geben Sie einen Suchfilter in das Suchfilter Feld. Mit 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 Teilbaum:** 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 Fehlerliste zu sehen. Sie müssen alle Fehler beheben, bevor Sie fortfahren können.
8. klicken **Speichern und fortfahren**.

Nächste Schritte
Benutzerrechte für die Remote-Authentifizierung konfigurieren

Benutzerrechte für die Remote-Authentifizierung konfigurieren

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

Wenn Sie Benutzerrechte 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 vorhanden sind, werden auf dem 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 der Optionen für die Zuweisung von Rechten Drop-down-Liste:

   • **Berechtigungsstufe vom Remoteserver abrufen**

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

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

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

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

• **Persönlicher Schreib-DN:** Erstellen Sie persönliche Dashboards und ändern Sie Dashboards, die für den angemeldeten Benutzer freigegeben wurden.

• **Vollständiger, nur lesbarer DN:** Objekte im ExtraHop-System anzeigen.

• **Eingeschränkter Nur-Lese-DN:** Zeigen Sie Dashboards an, die mit dem angemeldeten Benutzer geteilt wurden.

• **Packet Slices-Zugriffs-DN:** Sehen Sie sich die ersten 64 Byte der Pakete an, die über die ExtraHop Trace-Appliance erfasst wurden, und laden Sie sie herunter.

• **Paketzugriffs-DN:** Mit der ExtraHop Trace-Appliance erfasste Pakete anzeigen und herunterladen.

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

• **NDR-Modulzugriffs-DN:** Sicherheitserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und verbergen.

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

- **Remote-Benutzer haben vollen Schreibzugriff**

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

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

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