

Konfiguration der Fernauthentifizierung über TACACS+

Veröffentlicht: 2024-04-10

Das ExtraHop-System unterstützt Terminal Access Controller Access-Control System Plus (TACACS+) für die Fernauthentifizierung und Autorisierung.

Stellen Sie sicher, dass jeder Benutzer, der per Fernzugriff autorisiert werden soll, über die **Auf dem TACACS+-Server konfigurierter ExtraHop-Dienst** bevor Sie mit diesem Verfahren beginnen.

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 **TACACS+**, und klicken Sie dann **Weiter**.
4. Auf dem TACACS+ Server hinzufügen Seite, geben Sie die folgenden Informationen ein:
 - **Gastgeber** : Der Hostname oder die IP-Adresse des TACACS+-Servers. Stellen Sie sicher, dass der DNS des ExtraHop-Systems richtig konfiguriert ist, wenn Sie einen Hostnamen eingeben.
 - **Geheim** : Das gemeinsame Geheimnis zwischen dem ExtraHop-System und dem TACACS+-Server . Wenden Sie sich an Ihren TACACS+-Administrator, um den gemeinsamen geheimen Schlüssel zu erhalten.



Hinweis Das Geheimnis darf das Nummernzeichen (#) nicht enthalten.

- **Auszeit** : Die Zeit in Sekunden, die das ExtraHop-System auf eine Antwort vom TACACS+-Server wartet, bevor es erneut versucht, eine Verbindung herzustellen.
5. klicken **Server hinzufügen**.
 6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
 7. klicken **Speichern und beenden**.
 8. Aus dem Optionen für die Zuweisung von Berechtigungen Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:
 - **Berechtigungsstufe vom Remoteserver abrufen**
Diese Option ermöglicht es entfernten Benutzern, Rechtstufen vom Remoteserver zu erhalten. Sie müssen auch Berechtigungen auf dem TACACS+-Server konfigurieren.
 - **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.
 9. 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**

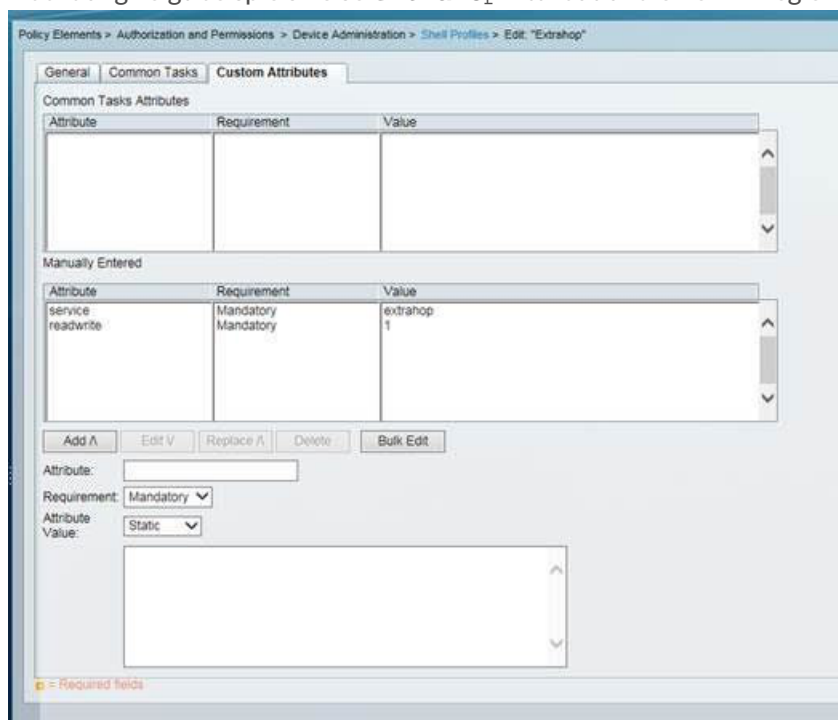
10. Optional: Konfigurieren Sie den Zugriff auf NDR- und NPM-Module.
 - **Kein Zugriff**
 - **Voller Zugriff**
11. klicken **Speichern und beenden**.
12. klicken **Erledigt**.

Den TACACS+-Server konfigurieren

Zusätzlich zur Konfiguration der Remote-Authentifizierung auf Ihrem ExtraHop-System müssen Sie Ihren TACACS+-Server mit zwei Attributen konfigurieren, einem für den ExtraHop-Dienst und einem für die Berechtigungsstufe. Wenn Sie einen ExtraHop-Packetstore haben, können Sie optional ein drittes Attribut für die PCAP und Sitzungsschlüsselprotokollierung hinzufügen.

1. Melden Sie sich bei Ihrem TACACS+-Server an und navigieren Sie zum Shell-Profil für Ihre ExtraHop-Konfiguration.
2. Fügen Sie für das erste Attribut hinzu `Bedienung`.
3. Fügen Sie für den ersten Wert hinzu `zusätzlicher Hop`.
4. Fügen Sie für das zweite Attribut die Berechtigungsstufe hinzu, z. B. `lesen/schreiben`.
5. Für den zweiten Wert addieren Sie `1`.

Die folgende Abbildung zeigt beispielsweise `extrahop` Attribut und eine Privilegienstufe von



`readwrite`.

Hier ist eine Tabelle mit verfügbaren Berechtigungsattributen, Werten und Beschreibungen:

Attribut	Wert	Beschreibung
setup	1	Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System und verwalten Sie den Benutzerzugriff
readwrite	1	Alle Objekte und Einstellungen auf dem ExtraHop-System

Attribut	Wert	Beschreibung
		erstellen und ändern, ohne Administrationseinstellungen
limited	1	Dashboards erstellen, ändern und teilen
readonly	1	Objekte im ExtraHop-System anzeigen
personal	1	Erstellen Sie persönliche Dashboards für sich selbst und ändern Sie alle Dashboards, die mit ihnen geteilt wurden
limited_metrics	1	Geteilte Dashboards anzeigen
ndrfull	1	Sicherheitserkennungen anzeigen, bestätigen und verbergen
npmfull	1	Leistungserkennungen anzeigen, bestätigen und verbergen
packetsfull	1	Pakete anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind.
packetslicesonly	1	Paketsegmente in einem verbundenen Packetstore anzeigen und herunterladen.
packetsfullwithkeys	1	Pakete und zugehörige Sitzungsschlüssel, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen.

6. Optional: Fügen Sie das folgende Attribut hinzu, damit Benutzer Sicherheitserkennungen anzeigen, bestätigen und verbergen können

Attribut	Wert
ndr voll	1

7. Optional: Fügen Sie das folgende Attribut hinzu, damit Benutzer Leistungserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und verbergen können.

Attribut	Wert
npm voll	1

8. Optional: Wenn Sie einen ExtraHop-Packetstore haben, fügen Sie ein Attribut hinzu, das es Benutzern ermöglicht, Paketerfassungen oder Paketerfassungen mit zugehörigen Sitzungsschlüsseln herunterzuladen.

Attribut	Wert	Beschreibung
nur Scheiben verpacken	1	Benutzer mit jeder Berechtigungsstufe können die ersten 64 Byte von Paketen anzeigen und herunterladen.
volle Pakete	1	Benutzer mit jeder Berechtigungsstufe können Pakete, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen.
packetslicesonly	1	Paketsegmente in einem verbundenen Packetstore anzeigen und herunterladen.
Pakete voll mit Schlüsseln	1	Benutzer mit jeder Berechtigungsstufe können Pakete und zugehörige Sitzungsschlüssel, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen.