Konfigurieren Sie die Fernauthentifizierung über TACACS+

Veröffentlicht: 2025-03-28

Das ExtraHop-System unterstützt das 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 ExtraHop-Dienst, der auf dem TACACS+-Server konfiguriert ist bevor Sie mit diesem Verfahren beginnen.

Wichtig: Bei Recordstores und Packetstores gewährt die Aktivierung des Fernzugriffs allen Benutzern im TACACS+-Authentifizierungssystem Administratorrechte, unabhängig von den Rechten, die das Authentifizierungssystem für jeden Benutzer festlegt.

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 Drop-down-Menü, wählen **TACACS+**, und klicken Sie dann auf **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 das 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 das gemeinsame Geheimnis 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 Sie **Server hinzufügen**.
6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
7. Klicken Sie **Speichern und fertig**.
8. Für Recordstores und Packetstores klicken Sie auf **Erledigt** und dann springe zu Konfiguration des TACACS+-Servers . Führen Sie für Sensoren und Konsolen die verbleibenden Schritte unten aus.
9. Aus dem Optionen für die Zuweisung von Berechtigungen Wählen Sie im Drop-down-Menü eine der folgenden Optionen aus:

   - **Berechtigungsstufe vom Remoteserver abrufen**

     Diese Option ermöglicht es Remotebenutzern, Berechtigungsstufen vom Remoteserver zu erhalten. Sie müssen auch Berechtigungen auf dem TACACS+-Server konfigurieren.

   - **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.
10. 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 Paket-Header**
- **Nur Pakete**
- **Pakete und Sitzungsschlüssel**

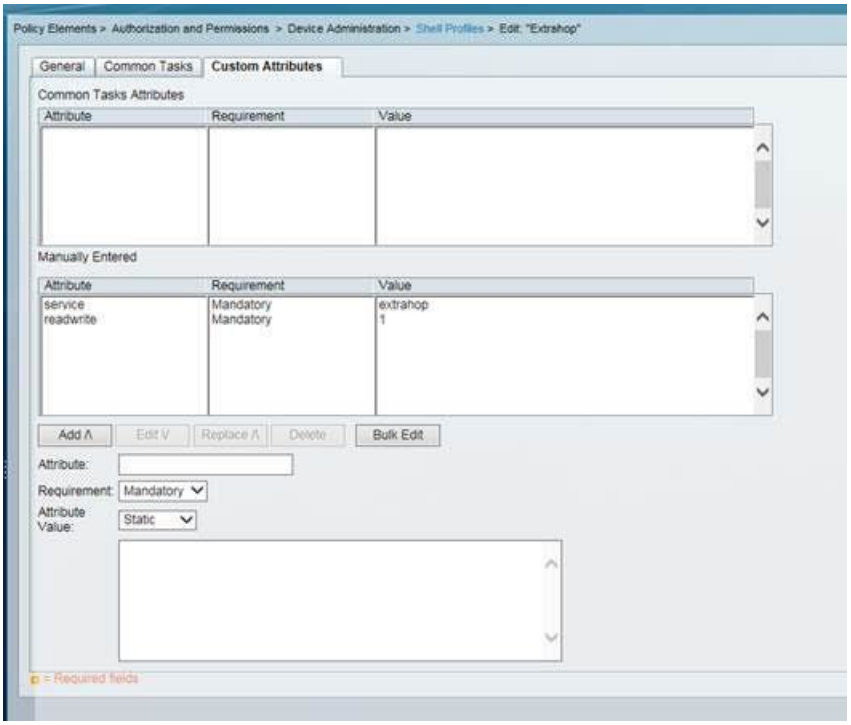
11. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff (nur auf Sensoren und Konsolen).
    - **Kein Zugriff**
    - **Voller Zugriff**
12. Klicken Sie **Speichern und fertig**.
13. Klicken Sie **Erledigt**.

Konfigurieren Sie den TACACS+-Server

Zusätzlich zur Konfiguration der Fernauthentifizierung auf Ihrem ExtraHop-System müssen Sie Ihren TACACS+-Server mit zwei Attributen konfigurieren, eines für den ExtraHop-Dienst und eines für die Berechtigungsstufe. Wenn Sie einen ExtraHop-Paketstore 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. Für den ersten Wert addieren `zusätzlicher Hopfen`.
4. Fügen Sie für das zweite Attribut die Berechtigungsstufe hinzu, z. B. `lesen/schreiben`.
5. Für den zweiten Wert addieren `1`.

   Die folgende Abbildung zeigt zum Beispiel `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`	Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System, ohne die 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 ausblenden
`npmfull`	`1`	Leistungserkennungen anzeigen, bestätigen und ausblenden
`packetsfull`	`1`	Pakete anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind.
`packetslicesonly`	`1`	Paketsegmente in einem verbundenen Packetstore anzeigen und herunterladen.
`packetheadersonly`	`1`	Sucht und lädt nur Paket-Header in einem verbundenen Packetstore herunter.
`packetsfullwithkeys`	`1`	Pakete und zugehörige Sitzungsschlüssel anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind.

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

Attribut	Wert
`ndrvoll`	`1`

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

Attribut	Wert
`npm voll`	`1`

8. Optional: Wenn Sie einen ExtraHop-Paketstore haben, fügen Sie ein Attribut hinzu, damit Benutzer Paketerfassungen oder Paketerfassungen mit zugehörigen Sitzungsschlüsseln herunterladen können.

Attribut	Wert	Beschreibung
`Pakete nur Scheiben`	`1`	Benutzer mit jeder Berechtigungsstufe können die ersten 64 Byte an Paketen anzeigen und herunterladen.
`Nur Paketheader`	`1`	Benutzer mit jeder Berechtigungsstufe können Paket-Header in einem verbundenen Packetstore suchen und herunterladen.
`Pakete voll`	`1`	Benutzer mit jeder Berechtigungsstufe können Pakete, die in einem verbundenen Packetstore gespeichert sind, 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.