Benutzer und Benutzergruppen

Veröffentlicht: 2024-02-12

Benutzer können auf drei Arten auf das ExtraHop-System zugreifen: über eine Reihe vorkonfigurierter Benutzerkonten, über lokale Benutzerkonten, die auf der Appliance konfiguriert sind, oder über Remote-Benutzerkonten, die auf vorhandenen Authentifizierungsservern wie LDAP, SAML, Radius und TACACS+ konfiguriert sind.

Lokale Benutzer

In diesem Thema geht es um Standard- und lokale Konten. siehe Fernauthentifizierung um zu lernen, wie man Remote-Konten konfiguriert.

Die folgenden Konten sind standardmäßig auf ExtraHop-Systemen konfiguriert, erscheinen jedoch nicht in der Namensliste auf der Benutzerseite. Diese Konten können nicht gelöscht werden und Sie müssen das Standardkennwort bei der ersten Anmeldung ändern.

Einrichten

Dieses Konto bietet volle System-Lese- und Schreibrechte für die browserbasierte Benutzeroberfläche und die ExtraHop-Befehlszeilenschnittstelle (CLI). Auf physischem Sensoren, das Standardkennwort für dieses Konto ist die Service-Tag-Nummer auf der Vorderseite der Appliance. Auf virtuellem Sensoren, das Standardpasswort ist `default`.

Schale

Die `shell` Das Konto hat standardmäßig Zugriff auf nicht administrative Shell-Befehle in der ExtraHop-CLI. Bei physischen Sensoren ist das Standardkennwort für dieses Konto die Service-Tag-Nummer auf der Vorderseite der Appliance. Bei virtuellen Sensoren lautet das Standardkennwort `default`.

Hinweis: Das standardmäßige ExtraHop-Passwort für eines der Konten, wenn es in Amazon Web Services (AWS) und Google Cloud Platform (GCP) bereitgestellt wird, ist die Instanz-ID der virtuellen Maschine.

Nächste Schritte

- Fügen Sie ein lokales Benutzerkonto hinzu

Fernauthentifizierung

Das ExtraHop-System unterstützt die Fernauthentifizierung für den Benutzerzugriff. Mithilfe der Remoteauthentifizierung können Unternehmen, die über Authentifizierungssysteme wie LDAP (z. B. OpenLDAP oder Active Directory) verfügen, allen oder einem Teil ihrer Benutzer die Möglichkeit geben, sich mit ihren vorhandenen Anmeldedaten am System anzumelden.

Die zentralisierte Authentifizierung bietet die folgenden Vorteile:

- Synchronisation von Benutzerkennwörtern.
- Automatische Erstellung von ExtraHop-Konten für Benutzer ohne Administratoreingriff.
- Verwaltung von ExtraHop-Privilegien auf der Grundlage von Benutzergruppen.
- Administratoren können allen bekannten Benutzern Zugriff gewähren oder den Zugriff einschränken, indem sie LDAP-Filter anwenden.

Nächste Schritte

- Konfigurieren Sie die Remote-Authentifizierung über LDAP
- Konfigurieren Sie die Remote-Authentifizierung über SAML
- Konfiguration der Fernauthentifizierung über TACACS+

- Konfigurieren Sie die Remoteauthentifizierung über RADIUS

Entfernte Benutzer

Wenn Ihr ExtraHop-System für die SAML- oder LDAP-Fernauthentifizierung konfiguriert ist, können Sie ein Konto für diese Remote-Benutzer erstellen. Durch die Vorkonfiguration von Konten auf dem ExtraHop-System für Remote-Benutzer können Sie Systemanpassungen mit diesen Benutzern teilen, bevor sie sich anmelden.

Wenn Sie sich bei der Konfiguration der SAML-Authentifizierung für die automatische Bereitstellung von Benutzern entscheiden, wird der Benutzer bei der ersten Anmeldung automatisch zur Liste der lokalen Benutzer hinzugefügt. Sie können jedoch ein SAML-Remotebenutzerkonto auf dem ExtraHop-System erstellen, wenn Sie einen Remote-Benutzer bereitstellen möchten, bevor sich dieser Benutzer am System angemeldet hat. Rechte werden dem Benutzer vom Anbieter zugewiesen. Nachdem der Benutzer erstellt wurde, können Sie ihn zu lokalen Benutzergruppen hinzufügen.

Nächste Schritte

- Konto für einen Remote-Benutzer hinzufügen

Benutzergruppen

Benutzergruppen ermöglichen es Ihnen, den Zugriff auf gemeinsam genutzte Inhalte nach Gruppen statt nach einzelnen Benutzern zu verwalten. Benutzerdefinierte Objekte wie Activity Maps können mit einer Benutzergruppe geteilt werden, und jeder Benutzer, der der Gruppe hinzugefügt wird, hat automatisch Zugriff. Sie können eine lokale Benutzergruppe erstellen, die Remote- und lokale Benutzer umfassen kann. Wenn Ihr ExtraHop-System für die Fernauthentifizierung über LDAP konfiguriert ist, können Sie alternativ Einstellungen für den Import Ihrer LDAP-Benutzergruppen konfigurieren.

- klicken **Benutzergruppe erstellen** um eine lokale Gruppe zu erstellen. Die Benutzergruppe wird in der Liste angezeigt. Aktivieren Sie dann das Kontrollkästchen neben dem Namen der Benutzergruppe und wählen Sie Benutzer aus der **Benutzer filtern...** Drop-down-Liste. klicken **Benutzer zur Gruppe hinzufügen**.
- (nur LDAP) Klicken Sie **Alle Benutzergruppen aktualisieren** oder wählen Sie mehrere LDAP-Benutzergruppen aus und klicken Sie auf **Benutzer in Gruppen aktualisieren**.
- klicken **Benutzergruppe zurücksetzen** um alle geteilten Inhalte aus einer ausgewählten Benutzergruppe zu entfernen. Wenn die Gruppe auf dem Remote-LDAP-Server nicht mehr existiert, wird die Gruppe aus der Benutzergruppenliste entfernt.
- klicken **Benutzergruppe aktivieren** oder **Benutzergruppe deaktivieren** um zu kontrollieren, ob ein Gruppenmitglied auf geteilte Inhalte für die ausgewählte Benutzergruppe zugreifen kann.
- klicken **Benutzergruppe löschen** um die ausgewählte Benutzergruppe aus dem System zu entfernen.
- Sehen Sie sich die folgenden Eigenschaften für aufgelistete Benutzergruppen an:

  Name der Gruppe

  Zeigt den Namen der Gruppe an. Um die Mitglieder der Gruppe anzuzeigen, klicken Sie auf den Gruppennamen.

  Typ

  Zeigt Lokal oder Remote als Art der Benutzergruppe an.

  Mitglieder

  Zeigt die Anzahl der Benutzer in der Gruppe an.

  Geteilter Inhalt

  Zeigt die Anzahl der vom Benutzer erstellten Objekte an, die mit der Gruppe gemeinsam genutzt werden.

Status

Zeigt an, ob die Gruppe auf dem System aktiviert oder deaktiviert ist. Wenn der Status ist `Disabled`, wird die Benutzergruppe bei der Durchführung von Mitgliedschaftsprüfungen als leer betrachtet. Die Benutzergruppe kann jedoch weiterhin angegeben werden, wenn Inhalte geteilt werden.

Mitglieder aktualisiert (nur LDAP)

Zeigt die Zeit an, die seit der Aktualisierung der Gruppenmitgliedschaft vergangen ist. Benutzergruppen werden unter den folgenden Bedingungen aktualisiert:

- Standardmäßig einmal pro Stunde. Die Einstellung für das Aktualisierungsintervall kann auf der **Fernauthentifizierung** > **LDAP-Einstellungen** Seite.
- Ein Administrator aktualisiert eine Gruppe, indem er auf **Alle Benutzergruppen aktualisieren** oder **Benutzer in der Gruppe aktualisieren**, oder programmgesteuert über die REST-API. Sie können eine Gruppe aktualisieren über Benutzergruppe Seite oder aus dem Liste der Mitglieder Seite.
- Ein Remote-Benutzer meldet sich zum ersten Mal beim ExtraHop-System an.
- Ein Benutzer versucht, ein geteiltes Dashboard zu laden, auf das er keinen Zugriff hat.

Benutzerrechte

Administratoren bestimmen die Modulzugriffsebene für Benutzer im ExtraHop-System.

Informationen zu Benutzerberechtigungen für die REST-API finden Sie in der REST-API-Leitfaden.

Informationen zu Remote-Benutzerrechten finden Sie in den Konfigurationsanleitungen für LDAP, RADIUS, SAML, und TACACS+.

Privilegienstufen

Legen Sie die Berechtigungsstufe für Ihren Benutzer fest, um zu bestimmen, auf welche Bereiche des ExtraHop-Systems er zugreifen kann.

Zugriffsrechte für Module

Diese Rechte bestimmen die Funktionen, auf die Benutzer im ExtraHop-System zugreifen können. Administratoren können Benutzern rollenbasierten Zugriff auf eines oder alle Module NDR, NPM und Packet Forensics gewähren. Für den Zugriff auf die Modulfunktionen ist eine Modullizenz erforderlich.

Netzwerkerkennung und Reaktion (NDR)

Ermöglicht dem Benutzer den Zugriff auf Sicherheitsfunktionen wie die Erkennung von Angriffen, Untersuchungen und Bedrohungsinformationen.

Netzwerkleistung und Überwachung (NPM)

Ermöglicht dem Benutzer den Zugriff auf Leistungsfunktionen wie Betriebserkennungen und die Möglichkeit, benutzerdefinierte Dashboards zu erstellen.

Paketforensik

Ermöglicht dem Benutzer das Anzeigen und Herunterladen von Paketen und Sitzungsschlüsseln, nur Pakete oder nur Paketsegmente.

Systemzugriffsrechte

Diese Rechte bestimmen den Funktionsumfang, über den Benutzer in den Modulen verfügen, auf die ihnen Zugriff gewährt wurde.

Für Reveal (x) Enterprise können Benutzer mit Systemzugriffs- und Administratorrechten auf alle Funktionen, Pakete und Sitzungsschlüssel für ihre lizenzierten Module zugreifen.

Für Reveal (x) 360 müssen Systemzugriffs- und Administratorrechte, der Zugriff auf lizenzierte Module, Pakete und Sitzungsschlüssel separat zugewiesen werden. Reveal (x) 360 bietet auch ein zusätzliches Systemadministrationskonto, das alle Systemberechtigungen gewährt, mit Ausnahme der Möglichkeit, Benutzer und API-Zugriff zu verwalten.

Die folgende Tabelle enthält ExtraHop-Funktionen und die erforderlichen Rechte. Wenn keine Modulanforderung angegeben ist, ist die Funktion sowohl im NDR- als auch im NDM-Modul verfügbar.

	System- und Zugriffsadmi	**Systemadmi (nur Reveal (x) 360)**	**Vollständige Schreibvorga**	**Eingeschränk Schreiben**	**Persönliches Schreiben**	**Vollständig schreibgesch**	**Eingeschränkt schreibgeschützt**
Karten mit Aktivitäten							
Karten mit geteilten Aktivitäten erstellen, anzeigen und laden	Y	Y	Y	Y	Y	Y	N
Aktivitätskarten speichern	Y	Y	Y	Y	Y	N	N
Aktivitätskarten teilen	Y	Y	Y	Y	N	N	N
Warnmeldungen	NDM-Modullizenz und Zugriff erforderlich.						
Benachrichtigungen anzeigen	Y	Y	Y	Y	Y	Y	Y
Benachrichtigungen erstellen und ändern	Y	Y	Y	N	N	N	N
Prioritäten der Analyse							
Seite „Analyseprioritäten anzeigen“	Y	Y	Y	Y	Y	Y	N
Analyseebenen für Gruppen hinzufügen und ändern	Y	Y	Y	N	N	N	N
Geräte zu einer Beobachtungsliste hinzufügen	Y	Y	Y	N	N	N	N
Verwaltung von Transferprioritäten	Y	Y	Y	N	N	N	N
Bündel							

	System- und Zugriffsadmi	Systemadmi (nur Reveal (x) 360)	Vollständige Schreibvorga	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkt schreibgeschützt
Ein Paket erstellen	Y	Y	Y	N	N	N	N
Paket hochladen und anwenden	Y	Y	Y	N	N	N	N
Liste der Bundles anzeigen	Y	Y	Y	Y	Y	Y	N
Armaturenbretter	NPM-Modullizenz und Zugriff erforderlich, um Dashboards zu erstellen und zu ändern.						
Dashboards anzeigen und organisieren	Y	Y	Y	Y	Y	Y	Y
Dashboards erstellen und ändern	Y	Y	Y	Y	Y	N	N
Dashboards teilen	Y	Y	Y	Y	N	N	N
Erkennungen	Lizenz und Zugriff auf das NDR-Modul sind erforderlich, um Sicherheitserkennungen anzuzeigen und zu optimieren und Ermittlungen einzuleiten. NPM-Modullizenz und Zugriff erforderlich, um Leistungserkennungen anzuzeigen und zu optimieren.						
Erkennungen anzeigen	Y	Y	Y	Y	Y	Y	Y
Erkennungen bestätigen	Y	Y	Y	Y	Y	N	N
Erkennungsstatus und Hinweise ändern	Y	Y	Y	Y	N	N	N
Untersuchungen erstellen und ändern	Y	Y	Y	Y	N	N	N
Optimierungsregeln erstellen und ändern	Y	Y	Y	N	N	N	N
Gerätegruppen	Administratoren können das konfigurieren Globale Richtlinie „Gerätegruppe bearbeiten“ und „Steuerung“ um festzulegen , ob Benutzer mit eingeschränkten Schreibrechten Gerätegruppen erstellen und bearbeiten können.						
Gerätegruppen erstellen und ändern	Y	Y	Y	Y (Wenn die globale	N	N	N

	System- und Zugriffsadmi	Systemadmi (nur Reveal (x) 360)	Vollständige Schreibvorga	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkt schreibgeschützt
				Rechterichtlinie aktiviert ist)			
Metriken							
Metriken anzeigen	Y	Y	Y	Y	Y	Y	N
Regeln für Benachrichtigungen	NDR-Modullizenz und Zugriff erforderlich, um Benachrichtigungen für Sicherheitserkennungen und Bedrohungsinformationen zu erstellen und zu ändern. NPM-Modullizenz und Zugriff erforderlich, um Benachrichtigungen für Leistungserkennungen zu erstellen und zu ändern.						
Regeln für Erkennungsbenachrichtigungen erstellen und ändern	Y	Y	Y	N	N	N	N
Benachrichtigungsregeln Bedrohungsübersicht erstellen und ändern	Y	Y	Y	N	N	N	N
Regeln für Systembenachrichtigungen erstellen und ändern (nur Reveal (x))	Y	Y	N	N	N	N	N
Rekorde	Recordstore erforderlich.						
Datensatzabfragen anzeigen	Y	Y	Y	Y	Y	Y	N
Datensatzformate anzeigen	Y	Y	Y	Y	Y	Y	N
Datensatzabfragen erstellen, ändern und speichern	Y	Y	Y	N	N	N	N
Datensatzformate erstellen, ändern und speichern	Y	Y	Y	N	N	N	N
Dashboard-Berichte	Konsole erforderlich.						
Geplante Berichte erstellen, anzeigen und verwalten	Y	Y	Y	Y	N	N	N

	System- und Zugriffsadmi	Systemadmi (nur Reveal (x) 360)	Vollständige Schreibvorga	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkt schreibgeschützt
Bedrohungsinformationen	NDR-Modullizenz und Zugriff erforderlich.						
Bedrohungssammlungen verwalten	Y	Y	N	N	N	N	N
Informationen zu Bedrohungsinformationen anzeigen	Y	Y	Y	Y	Y	Y	N
Auslöser							
Trigger erstellen und ändern	Y	Y	Y	N	N	N	N
Administratorrechte							
Greifen Sie auf die ExtraHop-Administrationseinstellungen zu	Y	Y	N	N	N	N	N
Stellen Sie eine Verbindung zu anderen Geräten her	Y	Y	N	N	N	N	N
Andere Appliances verwalten (Konsole)	Y	Y	N	N	N	N	N
Benutzer und API-Zugriff verwalten	Y	N	N	N	N	N	N