Modul-Migration

Veröffentlicht: 2024-07-02

Das ExtraHop-System bietet jetzt separate Module mit segmentierten und optimierten Funktionen für Sicherheits- und Performance-Anwendungsfälle.

Das Network Detection and Response (NDR) -Modul bietet Sicherheits- und Ermittlungsworkflows, und das Network Performance Management (NPM) -Modul bietet Betriebs- und Leistungsworkflows. Zusätzliche Module sind für Paketforensik und Intrusion Detection Systems erhältlich. Erfahre mehr über Module.

Dieses Handbuch enthält Informationen über globale Systemveränderungen und administrative Aufgaben. Erfahre mehr darüber, welche Eigenschaften sind für jedes Modul verfügbar.

Globale Systemänderungen

Das ExtraHop-System aktualisiert im Rahmen der Modulmigration automatisch bestimmte Funktionen.

Standard-Anmeldeseite

Für Benutzer mit NPM-Zugriff kann die Standard-Dashboard-Seite, die nach der Anmeldung angezeigt wird, von einem Administrator angegeben werden.

Für NPM-Benutzer die Standardeinstellung Dashboard Die Seite , die nach der Anmeldung angezeigt wird, kann angegeben werden weltweit von einem Administrator oder von einem Benutzer persönlich festgelegt werden. Wenn kein Dashboard angegeben ist, Active Directory Directory-Dashboard erscheint.

Benutzer können zu ihrem bevorzugten Standard-Dashboard navigieren, auf das Befehlsmenü in der oberen rechten Ecke der Seite klicken und Als Standard-Dashboard festlegen auswählen.

Tuning-Regeln

Das System entfernt die Option Alle Erkennungstypen aus den Erkennungstyp-Kriterien für Optimierungsregeln.

Tuning-Regeln werden basierend auf den Modulzugriffsoptionen angezeigt, die von angegeben sind Benutzerrechte.

Bestehende Optimierungsregeln, die die Kriterien „Alle Erkennungstypen“ enthalten, werden automatisch in zwei Regeln aufgeteilt, die entweder für Sicherheits- oder Leistungskategorien spezifisch sind. Die bestehende Regel wird geändert, um Alle Sicherheitserkennungstypen anzugeben, und eine neue Regel wird für Alle Leistungserkennungstypen erstellt. Während der Migration können versteckte Erkennungen mit einer neuen Optimierungsregel verknüpft werden, die den Erkennungskriterien entspricht.

Wenn Sie eine Optimierungsregel erstellen oder bearbeiten, können Sie abhängig von Ihren Modulzugriffsberechtigungen Kriterien für den Erkennungstyp angeben. Die Dropdownliste Erkennungstyp kann Optionen für Alle Sicherheitserkennungstypen oder Alle Leistungserkennungstypen enthalten.

Regeln für Benachrichtigungen

Regeln für Erkennungsbenachrichtigungen unterstützen keine Kriterien mehr, die sowohl für Sicherheits - als auch für Leistungserkennungen gelten. Benachrichtigungsregeln werden auf der Grundlage Ihrer Modulzugriffsrechte angezeigt.

Regeln für Erkennungsbenachrichtigungen die den Ereignistyp Erkennung angeben, werden automatisch in zwei Regeln aufgeteilt, die entweder für Sicherheits- oder Leistungskategorien spezifisch sind. Die bestehende Regel wird geändert, um den neuen Ereignistyp Sicherheitserkennung anzugeben, und enthält nur die Sicherheitskriterien der ursprünglichen Regel. Für den neuen Ereignistyp Leistungserkennung wird eine neue Regel erstellt, die nur die Leistungskriterien der ursprünglichen Regel enthält.

Wenn eine Benachrichtigungsregel während der Migration aufgeteilt wird, sind Erkennungstypen, die sowohl mit Sicherheit als auch mit Leistung verknüpft sind, nur in der Sicherheitsversion der Regel enthalten, um doppelte Benachrichtigungen zu vermeiden.

Deaktivierte Benachrichtigungsregeln, die sowohl Sicherheits- als auch Leistungskriterien enthalten, werden nicht aufgeteilt. Die Regel wird in eine reine Sicherheitsregel umgewandelt und bleibt deaktiviert.

Aktionen, die durch Benachrichtigungsregeln spezifiziert werden, wie E-Mail-Verteilerlisten und Webhooks, sind in der geänderten NDR-Regel und der neuen NPM-Regel enthalten. Überprüfen Sie diese Aktionen, um sicherzustellen, dass Sicherheits- und Leistungsbenachrichtigungen an die richtige Zielgruppe gesendet werden.

Wenn Sie eine Benachrichtigungsregel erstellen, können Sie entweder die Ereignistypen Sicherheitserkennung oder Leistungserkennung angeben, abhängig von den in Ihrem Benutzerrechte. Nachdem Sie einen Ereignistyp ausgewählt haben, können Sie nur Erkennungstyp und Kategoriekriterien hinzufügen, die dem ausgewählten Ereignistyp zugeordnet sind.

Administrative Aufgaben

Migrierte Systeme gewähren allen Benutzern Zugriff auf die Module Network Performance Monitoring (NPM) und Network Detection and Response (NDR).

Administratoren müssen allen Benutzern, die sich anmelden, rollenbasierten Zugriff gewähren Fernauthentifizierung (LDAP, RADIUS, SAML und TACACS+) sowie lokale Benutzer.

Es gibt zwei Sätze von Benutzerrechte das muss gewährt werden:

Zugriff auf das Modul

Diese Benutzerrechte bestimmen, auf welche Funktionen ein Benutzer zugreifen kann. Beispielsweise muss einem Benutzer Vollzugriff auf das NDR-Modul gewährt werden, um Angriffserkennungen sehen zu können. siehe spezifische Funktionen für jedes Modul.

Zugriff auf das System

Diese Benutzerberechtigungsstufen bestimmen den Funktionsumfang, den Benutzer mit Modulfunktionen haben. Beispielsweise können Benutzer mit vollem Schreibzugriff alle Systemobjekte erstellen und bearbeiten.

Die folgenden Abschnitte enthalten Anweisungen zum Aktualisieren von Benutzerrechten.

Aktualisierung der Einstellungen für die Fernauthentifizierung

Administratoren müssen die Remote-Authentifizierungseinstellungen für die NDR- und NPM-Module überprüfen und bei Bedarf aktualisieren.

Zugriff auf das Network Detection and Response (NDR) -Modul

Die Einstellungen für die Fernauthentifizierung für den NDR-Modulzugriff müssen konfiguriert werden unter RevealX Enterprise Systeme, auf denen die jetzt veraltete globale Zugriffsberechtigungsrichtlinie für Erkennungen zuvor nicht aktiviert war.

Der Benutzerzugriff auf das NDR-Modul wird direkt von der globalen Rechterichtlinieneinstellung Erkennungszugriff übernommen. Wenn beispielsweise vor der Migration nur bestimmten Benutzern Erkennungszugriff mit vollem Schreibsystemzugriff gewährt wurde, haben dieselben Benutzer jetzt nach der Migration Zugriff auf das NDR-Modul mit vollen Schreibsystemberechtigungen.

Zugriff auf das Modul Network Performance and Monitoring (NPM)

Die Einstellungen für die Fernauthentifizierung für den NPM-Modulzugriff müssen auf beiden konfiguriert werden Reveal X 360 und RevealX Enterprise systeme.

Aktualisieren Sie die benutzerdefinierte IdP-Konfiguration in RevealX 360

Aktualisieren Sie Ihre benutzerdefinierte Identity Provider-Konfiguration (IdP) in RevealX 360, um Benutzerberechtigungen für den Zugriff auf NDR- und NPM-Module zu gewähren.

Fernauthentifizierung für den Zugriff auf das NDR-Modul
Der Zugriff auf das NDR-Modul wird automatisch mit den vorherigen Einstellungen für Detections Access Control konfiguriert.

Fernauthentifizierung für den NPM-Modulzugriff
Sie müssen Ihre benutzerdefinierte Identity Provider-Konfiguration (IdP) aktualisieren, um Benutzern Zugriff auf das NPM-Modul in RevealX 360 zu gewähren.

Fügen Sie der ExtraHop-Anwendung in Ihrem Identitätsanbieter NPM-Rechte hinzu
Wenn Ihr IdP kein Gruppenattribut für die ExtraHop-Anwendung enthält, müssen Sie ein Benutzerattribut und einen Namen hinzufügen, die mit der Konfiguration in RevealX 360 übereinstimmen.

1. Loggen Sie sich bei Ihrem Identitätsanbieter ein.
2. Fügen Sie einen Attributnamen und einen Wert hinzu.
3. Speichern Sie die Konfiguration.

Nächste Schritte
Erfahren Sie mehr über die Konfiguration Okta, Google, Microsoft Entra ID oder Sprungwolke.
Fügen Sie NPM-Rechte zu Ihren Identitätsanbieter-Einstellungen in RevealX 360 hinzu

1. Melden Sie sich mit einem Konto, das über System- und Zugriffsadministrationsrechte verfügt, beim RevealX 360-System an.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **Benutzerzugriff**.
   Ein Fenster „Aktion erforderlich“ führt Sie durch die verbleibenden Konfigurationsschritte. Wenn das Fenster Aktion erforderlich nicht angezeigt wird, müssen Sie Ihre IdP-Einstellungen nicht aktualisieren.
3. Geben Sie einen Namen in das Feld Attributname ein.
4. Geben Sie einen Namen in das Feld Attributwert ein.

   Hinweis: Der Name und der Wert des Attributs müssen mit den auf Ihrem IdP konfigurierten Einstellungen übereinstimmen.
5. Markieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie bereit sind, mit dem Update zu beginnen.

   Wichtig: Alle Benutzer werden vom System abgemeldet, nachdem Sie geklickt haben **Jetzt aktualisieren** im nächsten Schritt.
6. Klicken Sie **Jetzt aktualisieren**.

Aktualisieren Sie die benutzerdefinierte IdP-Konfiguration in RevealX Enterprise

Aktualisieren Sie Ihre benutzerdefinierte Identity Provider (IdP) -Konfiguration in RevealX Enterprise, um Benutzerberechtigungen für den Zugriff auf NDR- und NPM-Module zu gewähren.

Fernauthentifizierung für den NPM-Modulzugriff
Sie müssen Ihre benutzerdefinierte Identity Provider-Konfiguration (IdP) aktualisieren, um Benutzern Zugriff auf das NPM-Modul in RevealX Enterprise zu gewähren.

1. Melden Sie sich bei der RevealX Enterprise-Konsole mit einem Konto an, das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **Die gesamte Verwaltung**.
3. Klicken Sie im Abschnitt Zugriffseinstellungen auf **Globale Richtlinien**.
   In einem Bereich „Aktion erforderlich“ wird ein Link angezeigt, über den Sie Ihre Einstellungen für die Fernauthentifizierung einsehen können. Wenn das Fenster Aktion erforderlich nicht angezeigt wird, müssen Sie Ihre IdP-Einstellungen nicht aktualisieren.
4. klicken **Fernauthentifizierung anzeigen**.
5. Wählen Sie Ihre Authentifizierungsmethode aus dem **Methode der Fernauthentifizierung** Dropdown.

6. Führen Sie die folgenden Schritte für die von Ihnen gewählte Fernauthentifizierungsmethode aus:

Option	Description

LDAP	Konfigurieren Sie den NPM-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Berechtigungsstufe vom Remoteserver abrufen:
	    1. Geben Sie einen eindeutigen Namen in das NPM-Modulzugriffs-DN Feld.
	2. Remote-Benutzer haben vollen Schreibzugriff
	    a. Wählen **Voller Zugriff**.
	3. Remote-Benutzer haben vollen Lesezugriff
	    a. Wählen **Voller Zugriff**.

RADIUS	Konfigurieren Sie den NPM-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Remote-Benutzer haben vollen Schreibzugriff
	    a. Wählen **Voller Zugriff**.
	2. Remote-Benutzer haben vollen Lesezugriff
	    a. Wählen **Voller Zugriff**.

SAML	Bearbeiten Sie die Einstellungen des Identitätsanbieters, um einen Attributnamen und einen Attributwert für den NPM-Modulzugriff hinzuzufügen. Der Name und die Werte des Attributs müssen mit den in Ihrem Identitätsanbieter konfigurierten Werten übereinstimmen.

TACACS+	Konfigurieren Sie den NPM-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Berechtigungsstufe vom Remoteserver abrufen:
	    1. Fügen Sie auf Ihrem TACACS+-Server das folgende benutzerdefinierte Attribut hinzu:
	    Attribut: `npm voll`
	    Wert: 1
	2. Remote-Benutzer haben vollen Schreibzugriff
	    a. Wählen **Voller Zugriff**.
	3. Remote-Benutzer haben vollen Lesezugriff
	    a. Wählen **Voller Zugriff**.

7. Kehren Sie zurück zum Globale Richtlinien Seite.
8. Markieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie bereit sind, das Update zu starten.

   Wichtig: Alle Benutzer mit Ausnahme des eingerichteten Benutzerkonto werden vom System abgemeldet.
9. klicken **Jetzt aktualisieren**.

Fernauthentifizierung für den NDR-Modulzugriff
Wenn auf Ihrem RevealX Enterprise-System vor der Migration Detection Access Control als globale Richtlinie aktiviert war, wird der NDR-Modulzugriff automatisch mit den vorherigen Einstellungen für Erkennungszugriffskontrolle konfiguriert.

Wenn Detection Access Control nicht aktiviert war, müssen Sie Ihre benutzerdefinierte Identity Provider-Konfiguration (IdP) aktualisieren, um Benutzern Zugriff auf das NDR-Modul in RevealX Enterprise zu gewähren.

1. Melden Sie sich bei der RevealX Enterprise-Konsole mit einem Konto an, das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Die gesamte Verwaltung**.
3. Klicken Sie im Abschnitt Zugriffseinstellungen auf **Globale Richtlinien**.

   In einem Bereich „Aktion erforderlich“ wird ein Link angezeigt, über den Sie Ihre Einstellungen für die Fernauthentifizierung einsehen können. Wenn das Fenster Aktion erforderlich nicht angezeigt wird, müssen Sie Ihre IdP-Einstellungen nicht aktualisieren.
4. klicken **Fernauthentifizierung anzeigen**.
5. Wählen Sie Ihre Authentifizierungsmethode aus dem **Methode der Fernauthentifizierung** Dropdown.
6. Führen Sie die folgenden Schritte für die von Ihnen gewählte Fernauthentifizierungsmethode aus:

Option	Description

LDAP	Konfigurieren Sie den NDR-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Berechtigungsstufe vom Remoteserver abrufen:
	  1. Geben Sie einen eindeutigen Namen in das NDR-Modulzugriff DN Feld.
	2. Remote-Benutzer haben vollen Schreibzugriff
	  a. Wählen **Voller Zugriff**.
	3. Remote-Benutzer haben vollen Lesezugriff
	  a. Wählen **Voller Zugriff**.

RADIUS	Konfigurieren Sie den NDR-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Remote-Benutzer haben vollen Schreibzugriff
	  a. Wählen **Voller Zugriff**.
	2. Remote-Benutzer haben vollen Lesezugriff
	  a. Wählen **Voller Zugriff**.

SAML	Bearbeiten Sie die Einstellungen des Identitätsanbieters, um einen Attributnamen und einen Attributwert für den NDR-Modulzugriff hinzuzufügen. Der Name und die Werte des Attributs müssen mit den in Ihrem Identitätsanbieter konfigurierten Werten übereinstimmen.
TACACS+	Konfigurieren Sie den NDR-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung. 1. Berechtigungsstufe vom Remoteserver abrufen:

Option	Description
	1. Fügen Sie auf Ihrem TACACS+-Server das folgende benutzerdefinierte Attribut hinzu: Attribut: `ndrvoll` Wert: 1 2. Remote-Benutzer haben vollen Schreibzugriff a. Wählen **Voller Zugriff**. 3. Remote-Benutzer haben vollen Lesezugriff a. Wählen **Voller Zugriff**.

7. Kehren Sie zurück zum Globale Richtlinien Seite.
8. Markieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie bereit sind, das Update zu starten.

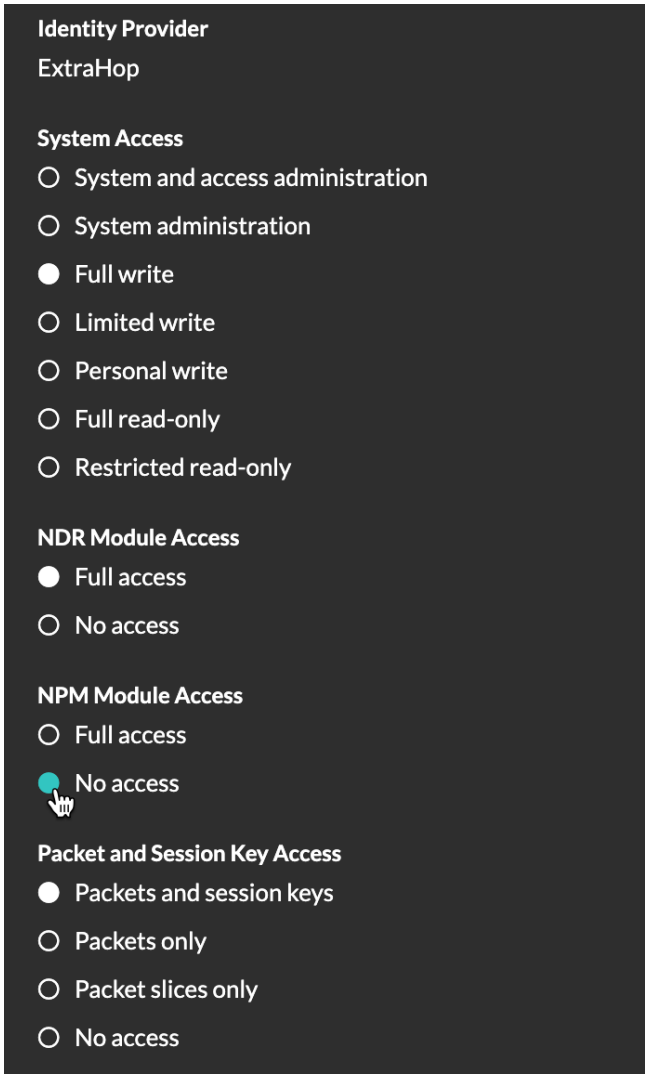
   Wichtig: Alle Benutzer mit Ausnahme des eingerichteten Benutzerkonto werden vom System abgemeldet.
9. klicken **Jetzt aktualisieren**.

Lokale Benutzereinstellungen aktualisieren

Administratoren müssen die lokalen Benutzerzugriffsrechte für die NDR- und NPM-Module überprüfen und gegebenenfalls aktualisieren.

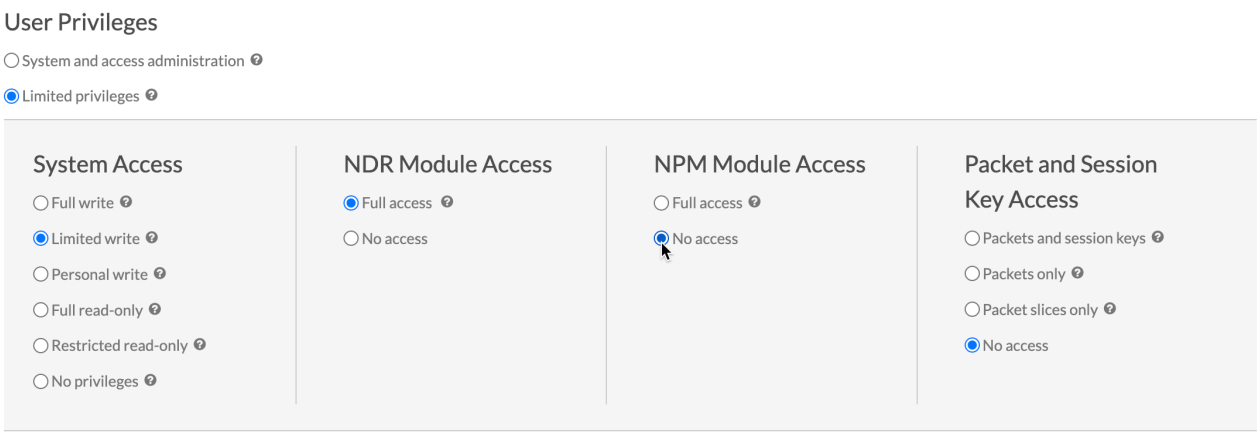
Aktualisieren Sie lokale Benutzer in RevealX 360

1. Melden Sie sich bei RevealX 360 an und klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Die gesamte Verwaltung**.
2. Klicken Sie **Benutzerzugriff**.
3. In der Nutzer Abschnitt, klicken **Benutzer anzeigen**.
4. Klicken Sie auf einen Benutzer, um die Zugriffsrechte anzuzeigen und zu ändern.



Aktualisieren Sie lokale Benutzer in RevealX Enterprise

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 Sie **Nutzer**.
3. Klicken Sie auf einen Benutzer, um die Zugriffsrechte anzuzeigen und zu ändern.


User Privileges
System and access administration
Limited privileges
System Access
Full write
Limited write
Personal write
Full read-only
Restricted read-only
No privileges
NDR Module Access
Full access
No access
NPM Module Access
Full access
No access
Packet and Session Key Access
Packets and session keys
Packets only
Packet slices only
No access