

Eine Gerätegruppe erstellen

Veröffentlicht: 2024-04-10


Sie können sowohl dynamische als auch statische Gerätegruppen erstellen. Dynamische Gruppen fügen der Gruppe automatisch alle Geräte hinzu, die bestimmten Kriterien entsprechen, während bei statischen Gruppen jedes Gerät manuell hinzugefügt werden muss.

Erstellen Sie eine dynamische Gerätegruppe

Sie können dynamische Gerätegruppen mit komplexen Filtern erstellen, mit denen Sie mehrere Kriterien angeben und verschachtelte Kriteriengruppen erstellen können.



Hinweis Auf der Seite Geräte können Sie schnell eine dynamische Gerätegruppe aus einer gefilterten Geräteliste erstellen. Klicken Sie auf **Dynamische Gruppe erstellen** aus der oberen rechten Ecke.

Sie können auch eine dynamische Gerätegruppe aus einer integrierten Gerätegruppe erstellen. Klicken Sie auf der Seite Geräte auf eine Rolle oder ein Protokoll, aktualisieren Sie die Filterkriterien und klicken Sie dann auf Speichern  Symbol in der oberen rechten Ecke.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Vermögenswerte** und klicken Sie dann auf **Gerätegruppen** Diagramm.
3. klicken **Gerätegruppe erstellen**.
4. In der **Name der Gruppe** Feld, geben Sie einen beschreibenden Namen ein, um die Gruppe zu identifizieren
5. Optional: Aus dem **Redakteure** Wählen Sie in der Dropdownliste Benutzer mit eingeschränkten Schreibrechten aus, die diese Gerätegruppe bearbeiten können. Dieses globale Privileg muss in den Administrationseinstellungen aktiviert werden.
 - In der Liste werden nur begrenzte Schreibbenutzer mit aktiven Konten angezeigt.
 - Nur ein Benutzer mit Bearbeitungsberechtigungen für eine Gerätegruppe kann weitere Benutzer mit eingeschränktem Schreibzugriff hinzufügen.
6. Optional: In der **Beschreibung** Feld, fügen Sie Informationen zu dieser Gerätegruppe hinzu.
7. In der Art der Gruppe Abschnitt, klicken Sie **Dynamisch**.
8. In der Filterkriterien Abschnitt, klicken Sie **Alles abgleichen** und wählen Sie dann einen der folgenden Vergleichsoperatoren aus der Dropdownliste aus:

FILTER CRITERIA

Option	Description
Alles abgleichen	Filtert nur Geräte, die alle angegebenen Kriterien erfüllen.
Ordne jedem zu	Filtert Geräte, die einem der angegebenen Kriterien entsprechen.
Keine Treffer	Filtert Geräte, die keines der angegebenen Kriterien erfüllen.

9. klicken **Name** und wählen Sie eine der folgenden Kategorien aus der Dropdownliste aus:

FILTER CRITERIA

Option	Description
Name	Filtert Geräte nach dem erkannten Gerätenamen. Ein ermittelter Gerätenamen kann beispielsweise die IP-Adresse oder den Hostnamen enthalten.
MAC-Adresse	Filtert Geräte nach der MAC-Adresse des Gerät.
IP Adresse	Filtert Geräte nach IP-Adresse in den Blockformaten IPv4, IPv6 oder CIDR.
Standort	Filtert Geräte, die einer verbundenen Standort zugeordnet sind. Nur für die Konsole.
Zeit für Entdeckungsreisen	Filtert Geräte, die vom ExtraHop-System innerhalb des angegebenen Zeitintervalls automatisch erkannt werden. Weitere Informationen finden Sie unter Erstellen Sie eine Gerätegruppe basierend auf der Erkennungszeit .
Analyseebene	Filtert Geräte nach Analyseebene, die bestimmt, welche Daten und Metriken für ein Gerät erfasst werden. Sie können keine dynamische Gerätegruppe für Geräte erstellen, die nach Analyseebene gefiltert sind.
Modell	Filtert Geräte nach Marke und Modellname. Die folgenden Tipps können Ihnen helfen, das gewünschte Gerätemodell zu finden: <ul style="list-style-type: none"> • Wählen Sie den Operator für exakte Übereinstimmung (=), um eine Dropdownliste der vorhandenen Modelle und Modellsätze anzuzeigen. • Wählen Sie den Exact-Match-Operator (=) und wählen Sie dann Maßgeschneiderte Modelle um alle Geräte zu filtern, die einem benutzerdefinierten Modellsatz zugewiesen sind.

Option	Description
Aktivität	<p>Filtert Geräte nach Protokollaktivität, die dem Gerät zugeordnet ist. Wenn Sie beispielsweise HTTP-Server auswählen, werden Geräte mit HTTP-Server-Metriken und jedes andere Gerät zurückgegeben, dessen Geräterolle auf HTTP-Server festgelegt ist.</p> <p>Filtert auch Geräte, die eine externe Verbindung akzeptiert oder initiiert haben, sodass Sie feststellen können, ob Geräte verdächtige Aktivitäten ausführen.</p>
Cloud-Konto	Filtert Geräte nach dem Cloud-Dienstkonto, das dem Gerät zugeordnet ist.
Cloud-Instanz-ID	Filtert Geräte nach der Cloud-Instanz-ID, die dem Gerät zugeordnet ist.
Cloud-Instanztyp	Filtert Geräte nach dem Cloud-Instanztyp, der dem Gerät zugeordnet ist.
Hoher Wert	Filtert Geräte, die als hoher Wert eingestuft werden, weil sie Authentifizierungsdienste bereitstellen, wichtige Dienste in Ihrem Netzwerk unterstützen oder die vom Benutzer als hochwertig eingestuft wurden.
Derzeit aktiv	Filtert Geräte nach Aktivitäten, die in den letzten 30 Minuten auf einem Gerät beobachtet wurden.
Netzwerk-Lokalitätstyp	Filtert Geräte nach allen internen oder externen Netzwerkstandorten.
Name der Netzwerklokalität	Filtert Geräte nach dem Namen der Netzwerklokalität.
Rolle	Filtert Geräte nach der zugewiesenen Geräterolle wie Gateway, Firewall, Load Balancer und DNS-Server.
Software	Filtert Geräte nach der auf dem Gerät erkannten Betriebssystemsoftware.
Subnetz	Filtert Geräte nach dem Subnetz, das dem Gerät zugeordnet ist.
Schlagwort	Filtert Geräte nach benutzerdefinierten Geräte-Tags.
Verkäufer	Filtert Geräte nach dem Namen des Geräteherstellers, der durch die OUI-Suche (Organizationally Unique Identifier) ermittelt wurde.
Virtuelle private Cloud	Filtert Geräte nach der VPC, die dem Gerät zugeordnet ist.
VLAN	Filtert Geräte nach dem Geräte-VLAN-Tag. VLAN-Informationen werden aus VLAN-Tags extrahiert, wenn der Datenverkehrsspiegelungsprozess sie auf dem Spiegelpoint beibehält.

Option	Description
	Nur verfügbar, wenn <code>devices_accross_vlans</code> Einstellung ist gesetzt auf <code>False</code> in der laufenden Konfigurationsdatei.
CDP-Name	Filtert Geräte nach dem CDP-Namen, der dem Gerät zugewiesen ist.
Name der Cloud-Instanz	Filtert Geräte nach dem Cloud-Instanznamen, der dem Gerät zugewiesen ist.
Benutzerdefinierter Name	Filtert Geräte nach dem benutzerdefinierten Namen, der dem Gerät zugewiesen wurde.
DHCP-Name	Filtert Geräte nach dem DHCP-Namen, der dem Gerät zugewiesen ist.
DNS-Name	Filtert Geräte nach einem beliebigen DNS-Namen, der dem Gerät zugewiesen ist.
NetBIOS-Name	Filtert Geräte nach dem NetBIOS-Namen, der dem Gerät zugewiesen ist.
Erkennungsaktivität	Filtert Geräte mit Erkennungsaktivität ↗ wo das Gerät ein Teilnehmer war. Aktiviert zusätzliche Kriterien wie Kategorie, Risikoscore und MITRE-Technik.



Hinweis Sie können keine Gerätegruppe erstellen, die diese Kriterienoption enthält.

10. Wählen Sie einen der folgenden Operatoren aus der Dropdownliste aus. Die verfügbaren Operatoren basieren auf der ausgewählten Kategorie:



Option	Description
=	Filtert Geräte, die exakt dem Suchfeld für die ausgewählte Kategorie entsprechen.
≠	Filtert Geräte, die nicht genau dem Suchfeld entsprechen.
≈	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
≈/	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie ausschließen.
beginnt mit	Filtert Geräte, die mit dem Wert des Suchfeldes für die ausgewählte Kategorie beginnen.

Option	Description
existiert	Filtert Geräte, die einen Wert für die ausgewählte Kategorie haben.
existiert nicht	Filtert Geräte, die keinen Wert für die ausgewählte Kategorie haben.
Spiel	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
und	Filtert Geräte, die den in zwei oder mehr Suchfeldern angegebenen Bedingungen entsprechen.
oder	Filtert Geräte, die mindestens eine in zwei oder mehr Suchfeldern angegebene Bedingung erfüllen.
nicht	Filtert Geräte, die die in einem Suchfeld angegebenen Bedingungen nicht erfüllen.

11. Geben Sie im Suchfeld die Zeichenfolge ein, die abgeglichen werden soll, oder wählen Sie einen Wert aus der Dropdownliste aus. Der Eingabetyp wird durch die gewählte Kategorie bestimmt.

Wenn Sie beispielsweise Geräte anhand des Namens suchen möchten, geben Sie die Zeichenfolge, die abgeglichen werden soll, in das Suchfeld Feld. Wenn Sie Geräte anhand der Rolle suchen möchten, wählen Sie diese aus der Dropdownliste der Rollen aus.

FILTER CRITERIA

Match All ▾

Name ▾ ≈ ▾ accounting- .* ×

Add Filter Add Filter Group

FILTER CRITERIA

Match All ▾

Role ▾ = ▾ Select an item... ▾ ×

Add Filter Filter...

- Database
- DHCP Server
- DNS Server



Hinweis Abhängig von der ausgewählten Kategorie können Sie im Textfeld auf das Regex-Symbol klicken, um den Abgleich per regulärem Ausdruck zu aktivieren.

FILTER CRITERIA

The screenshot shows the 'FILTER CRITERIA' section. At the top, there is a dropdown menu currently set to 'Match All'. Below this is a search bar with 'Name' selected in a dropdown, followed by an equals sign operator. To the right of the search bar are icons for adding a filter and a close button. Below the search bar are two buttons: 'Add Filter' and 'Add Filter Group'. A tooltip with the text 'Type regular expression' is pointing to the search field.

12. Optional: klicken **Filter hinzufügen** um weitere Filterkriterien hinzuzufügen.
13. Optional: klicken **Filtergruppe hinzufügen** um Filterkriterien zu den Ergebnissen des ursprünglichen Filters hinzuzufügen.

Wenn Sie beispielsweise nach Gerätenamen filtern, die mit „Konto“ beginnen, können Sie eine neue Gruppe von Kriterien hinzufügen, die nach einer bestimmten Rolle oder einem bestimmten Tag innerhalb der Gruppe von Geräten filtern, die mit „Konto“ beginnen.

14. klicken **Speichern**.

Sie können die Kriterien ändern, indem Sie auf der Seite Gerätegruppen auf die Gruppe klicken, die Sie ändern möchten, und dann auf **Eigenschaften**.

Erstellen Sie eine statische Gerätegruppe

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Vermögenswerte** und klicken Sie dann auf **Gerätegruppen** Diagramm.
3. klicken **Gerätegruppe erstellen**.
4. In der **Name der Gruppe** Feld, geben Sie einen Namen für die neue Gruppe ein.
5. Optional: Aus dem **Redakteure** Wählen Sie in der Dropdownliste Benutzer mit eingeschränkten Schreibrechten aus, die diese Gerätegruppe bearbeiten können. Dieses globale Privileg muss in den Administrationseinstellungen aktiviert werden.
 - In der Liste werden nur begrenzte Schreibbenutzer mit aktiven Konten angezeigt.
 - Nur ein Benutzer mit Bearbeitungsberechtigungen für eine Gerätegruppe kann weitere Benutzer mit eingeschränktem Schreibzugriff hinzufügen.
6. Optional: In der **Beschreibung** Feld, fügen Sie Informationen zu dieser Gerätegruppe hinzu.
7. In der Art der Gruppe Abschnitt, auswählen **Statisch**.
8. klicken **Speichern**.
Ihre Gerätegruppe ist jetzt erstellt.
9. Füge deiner Gruppe ein bestimmtes Gerät hinzu.
 - a) Klicken Sie auf die gewünschte statische Gerätegruppe und klicken Sie auf **Geräte** aus dem linken Bereich.
 - b) Klicken Sie oben in der Gerätetabelle auf das Feld Gerät suchen..., geben Sie den Namen des gewünschten Gerät ein, und wählen Sie dann das Gerät aus der Liste aus.
 - c) klicken **Zur Gruppe hinzufügen**.
10. Fügen Sie Geräte mit bestimmten Kriterien zu Ihrer Gruppe hinzu.
 - a) klicken **Geräte** im linken Bereich.
 - b) **Finde ein Gerät** [🔍](#) und aktivieren Sie dann das Kontrollkästchen neben den Geräten, die Sie zu Ihrer Gruppe hinzufügen möchten.
 - c) Klicken Sie oben in der Gerätetabelle auf **Zur Gruppe zuweisen**.
 - d) Wählen Sie eine Gerätegruppe aus dem Gruppe Dropdownliste.

- e) klicken **Zur Gruppe hinzufügen**.

Nächste Schritte

Geräte aus einer Gruppe entfernen, indem Sie das Kontrollkästchen neben dem Gerätenamen markieren und auf **Aus Gruppe entfernen** in der oberen rechten Ecke.