

Erstellen Sie eine Gerätegruppe basierend auf der Erkennungszeit

Veröffentlicht: 2024-04-10

Das ExtraHop-System erkennt automatisch Geräte, die Datenverkehr über das Kabel senden und empfangen. Zusätzlich zu den integrierten Gruppen, die Geräte erkennen, die in den letzten 24 Stunden und den letzten 7 Tagen hinzugefügt wurden, können Sie eine benutzerdefinierte dynamische Gerätegruppe erstellen, die automatisch Geräte hinzufügt, die in einem bestimmten Zeitintervall erkannt wurden.

Weitere Informationen zu den verschiedenen Zeitformaten finden Sie unter [Discovery-Zeitformate](#).

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 Sie in der oberen rechten Ecke auf **Gerätegruppe erstellen**.
4. In der **Name der Gruppe**Feld, geben Sie einen Namen für die Gerätegruppe ein.
5. In der **Beschreibung der Gruppe**Feld, geben Sie alle Informationen ein, die als Referenz für den von Ihnen angegebenen Ermittlungszeitraum dienen können.
6. In der Art der Gruppe Abschnitt, klicken Sie **Dynamisch**. Der Abschnitt Filterkriterien wird angezeigt.

7. Wählen Sie einen Vergleichsoperator aus der Dropdownliste aus:

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

8. Klicken Sie in der Dropdownliste mit den Kategorien auf **Entdeckungszeit**.

9. Wählen Sie einen Suchoperator aus der Dropdownliste aus:

Option	Description
=	Filtert Geräte, die exakt dem Erkennungszeitintervall entsprechen.
≈	Filtert Geräte, die nicht genau dem Erkennungszeitintervall entsprechen.

10. In der **Von (In Unix-Zeit)** Feld, führen Sie einen der folgenden Schritte aus:

- Lassen Sie dieses Feld leer, um anzugeben, wann Ihr System zum ersten Mal Traffic empfangen hat.
- Geben Sie ein festes Datum in das [Unix-Epoch-Zeitformat](#) oder geben Sie einen Wert in das [relatives Zeitformat](#).

11. In der **Bis (In Unix-Zeit)** Feld, schließen Sie die folgenden Schritte ab:

- Lassen Sie dieses Feld leer, um das Geschenk anzugeben.
-  **Wichtig:** Wenn das Feld Von leer ist, können Sie das Feld Bis nicht leer lassen und müssen ein festes oder relatives Zeitformat eingeben.
- Geben Sie ein festes Datum in das [Unix-Epoch-Zeitformat](#) oder geben Sie einen Wert in das [relatives Zeitformat](#).

 **Wichtig:** Das Format des Feld Bis muss dem Format des Feld Von entsprechen.

12. Klicken Sie **Speichern**.

Nächste Schritte

- [Erstellen Sie ein Diagramm in Ihrem Dashboard](#) und wähle deine neue Gerätegruppe als Quelle
- [Aktivitätenkarten-Verbindungen nach Gruppe filtern](#)

Discovery-Zeitformate

Wenn Sie eine benutzerdefinierte Gerätegruppe für Geräte erstellen, die während eines bestimmten Zeitintervalls erkannt wurden, müssen die Kriterien für die Erkennungszeit entweder in der Unix-Epochenzeit oder in einem relativen Zeitraum angegeben werden.

Zeit der Unix-Epoche

Bestimmte Daten müssen in die Unix-Epochenzeit konvertiert werden. Diese Konvertierung trägt dazu bei, Diskrepanzen zwischen Zeitzonen und unterschiedlichen Serverzeiten zu verringern.

Sie können Ihr Datum mit einem Online-Tool in einen Zeitstempel umwandeln, wie <https://www.epochconverter.com/>. Nachdem Sie den Unix-Epoch-Zeitstempel erstellt haben, kopieren Sie den Zeitstempel und fügen Sie ihn in die Felder FROM und UNTIL für Ihre Gerätegruppenkriterien ein. Der Zeitstempel muss Millisekunden enthalten. Um beispielsweise den 16. August 2018, 18:16:51 Uhr anzugeben, geben Sie 1534443411000, wie in der folgenden Abbildung dargestellt.

Mon	Day	Yr	Hr	Min	Sec		
8	16	2018	18	16	51	GMT	Human date to Timestamp

Epoch timestamp: 1534443411

Timestamp in milliseconds: 1534443411000

Human time (GMT): Thursday, August 16, 2018 6:16:51 PM

Human time (your time zone): Thursday, August 16, 2018 11:16:51 AM GMT-07:00

Beispiel für einen gültigen Zeiteintrag für die Unix-Epoche

1534238700000

Beispiel für einen ungültigen Zeiteintrag für die Unix-Epoche

1534238700ms

Relativer Zeitbereich

Um einen Zeitpunkt relativ zu einem anderen Zeitpunkt anzugeben, z. B. vor einer Woche, müssen Sie einem Wert ein Minuszeichen voranstellen und dann eine der folgenden Zeiteinheiten anhängen: y, M, w, d, h, m, ms. Geben Sie beispielsweise `-1 w` vor einer Woche zu spezifizieren. Sie können keinen zukünftigen Zeitraum angeben. Relative Zeitbereiche müssen mit einem negativen Wert beginnen.

Die folgende Tabelle zeigt die unterstützten Zeiteinheiten.

Zeiteinheit	Einheitensuffix
Jahr	y
Monat	M
Woche	w

Zeiteinheit	Einheitensuffix
Tag	d
Stunde	h
Minute	m
Zweiter	s
Millisekunde	Frau

Beispiel für einen gültigen relativen Zeiteintrag

-12 h

Beispiele für ungültige relative Zeiteinträge

12 h

-12 H

Beispiele für Kriterien zur Erkennungszeit

Hier finden Sie Beispiele für Kriterien für verschiedene Entdeckungszeiträume.

Von 1. Jan 2018 12:23:23:00 UTC bis jetzt

GROUP TYPE

- Static (add devices manually)
 Dynamic (specify filter criteria)

FILTER CRITERIA

Match All ▾

Discovery Time ▾ = ▾ 1514838203000 Until (In Unix time)...

January 1st 2018, 20:23:23.000 UTC

Von vor einem Monat bis vor einer Minute

GROUP TYPE

- Static (add devices manually)
 Dynamic (specify filter criteria)

FILTER CRITERIA

Match All ▾

Discovery Time ▾ = ▾ -1M -1m

a month ago

a minute ago