Erstellen Sie eine Gerätegruppe basierend auf der Erkennungszeit

Veröffentlicht: 2023-09-13

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.

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 oben auf der Seite auf **Vermögenswerte**, und klicken Sie dann **Gerätegruppen** im linken Bereich.
3. Klicken Sie in der oberen rechten Ecke **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 Entdeckungszeitraum dienen können.
6. In der Art der Gruppe Abschnitt, klicken **Dynamisch**.
   Der Abschnitt Filterkriterien wird angezeigt.
7. Wählen Sie einen Match-Operator aus der Drop-down-Liste aus:

Option	Description
Alle abgleichen	Filtert nur Geräte, die allen angegebenen Filterkriterien entsprechen.
Beliebiges abgleichen	Filtert Geräte, die einem der angegebenen Filterkriterien entsprechen.
Kein Spiel	Filtert Geräte, die keinem der angegebenen Filterkriterien entsprechen.

8. Klicken Sie in der Dropdownliste mit den Kategorien auf **Entdeckungszeit**.
9. Wählen Sie einen Suchoperator aus der Drop-down-Liste 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 Verkehr empfangen hat.
    - Geben Sie ein festes Datum in das Zeitformat der Unix-Epoche oder geben Sie einen Wert in das relatives Zeitformat.
11. In der **Bis (In Unix-Zeit)** Feld, indem Sie die folgenden Schritte ausführen:
    - 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 Zeitformat der Unix-Epoche oder geben Sie einen Wert in das relatives Zeitformat.

Wichtig: Das Format des Feld Bis muss mit dem Format des Feld Von übereinstimmen.

12. klicken **Speichern**.

Nächste Schritte

- Erstellen Sie ein Diagramm in Ihrem Dashboard und wähle deine neue Gerätegruppe als Quelle
- Verbindungen auf der Aktivitätsdiagramm nach Gruppen filtern

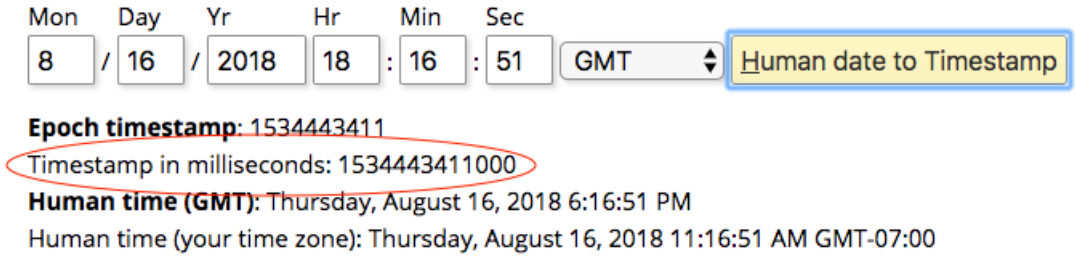
Discovery-Zeitformate

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.



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

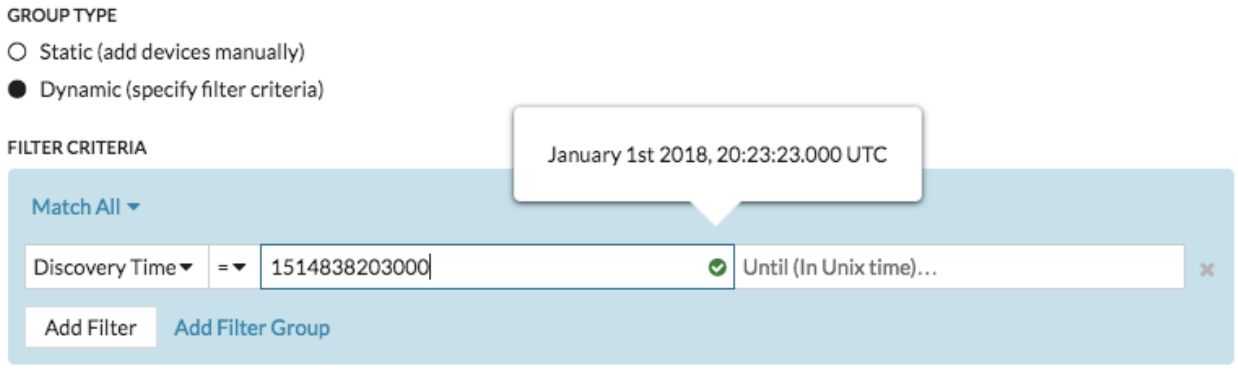
12 h

-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



Von vor einem Monat bis vor einer Minute