Netzwerk aktualisieren

Veröffentlicht: 2024-02-16

Sie können einer einzelnen Netzwerklokalität mehrere CIDR-Blöcke und IP-Adressen hinzufügen und einen Namen für die Lokalität konfigurieren. Das ExtraHop GitHub-Repository enthält Python-Skripte, mit denen Sie Lokalitäten automatisch konsolidieren und umbenennen können.

Hinweis: Wenn Sie in Firmware vor Version 9.0 Netzwerklokalitäten erstellt haben, in denen Sie nur einen einzigen CIDR-Block oder eine IP-Adresse für eine Netzwerklokalität angeben konnten, möchten Sie möglicherweise Netzwerklokalitäten konsolidieren und umbenennen, um die Suche und Filterung nach Lokalität zu vereinfachen.

Die `retrieve_network_localities.py` Das Skript ruft alle Informationen zur Netzwerklokalität von einem bestimmten Sensor oder einer bestimmten Konsole ab und speichert die Informationen in einer CSV-Datei. Sie können die CSV-Datei ändern in geben Sie an, welche Orte Sie konsolidieren möchten und neue Namen für bestehende Orte angeben. Die `create_network_localities.py` Das Skript liest dann die aktualisierte CSV-Datei, um die vorhandenen Lokalitäten auf einem bestimmten Sensor oder einer Konsole zu ersetzen.

Warnung: Die `create_network_localities.py` Das Skript löscht alle Netzwerkstandorte auf dem Zielsensor oder der Zielkonsole, bevor die in der CSV-Datei angegebenen neuen Einträge erstellt werden.

Konsolidierung von Netzwerkstandorten

In der CSV-Datei können Sie angeben, welche Orte Sie konsolidieren möchten, indem Sie mehreren Orten dieselbe Beschreibung zuweisen. Wenn der `create_network_localities.py` Das Skript konsolidiert die Lokalitäten und weist der neuen Lokalität den Namen der ersten Lokalität in der Gruppe zu. Nehmen wir zum Beispiel an , dass die CSV-Datei die folgenden Einträge enthält:

Netzwerke	extern	Beschreibung	Name
192.168.1.2	Falsch	gruppe1	[auto]: Intern - 192.168.1.2
192.168.1.1	Falsch	gruppe1	[auto]: Intern - 192.168.1.1

Ausführen des `create_network_localities.py` Das Skript erstellt die folgende Netzwerklokalität auf dem Zielsensor oder der Zielkonsole:

Netzwerke	extern	Beschreibung	Name
192.168.1.2 und 192.168.1.1	Falsch	gruppe1	[auto]: Intern - 192.168.1.2

Um Netzwerklokalitäten mit derselben Beschreibung in der CSV-Datei wie in diesem Thema beschrieben zu konsolidieren, müssen Sie Folgendes angeben: `--group description` Option, wenn Sie das ausführen `create_network_localities.py` skript.

Umbenennen von Netzwerkorten

In der CSV-Datei können Sie beschreibende Namen für Orte angeben. Das ExtraHop-System generiert automatisch Namen für Netzwerkstandorte, wenn sie nicht von einem Benutzer angegeben wurden.

Hinweis: Wenn du das ausführst `retrieve_network_localities.py` Skript auf einem Sensor oder einer Konsole, auf der Firmware-Version 8.9 oder früher ausgeführt wird. Das Skript generiert automatisch Namen für jede Lokalität und fügt sie der CSV-Datei hinzu. Sie können diese Namen so ändern, dass sie aussagekräftiger sind, indem Sie die Namen in der CSV-Datei ändern, bevor Sie den `create_network_localities.py` skript.

Sowohl das Skript als auch das ExtraHop-System generieren Namen im folgenden Format:

```
[auto]: EXTERNALITY - NETWORK
```

Im obigen Text wird EXTERNALITY entweder durch „Extern“ oder „Intern“ und Netzwerk durch die IP-Adresse oder den CIDR-Block des Netzwerks ersetzt. Beispielsweise wird einer Netzwerklokalität für den CIDR-Block 192.168.1.0/24 der folgende Name zugewiesen:

```
[auto]: Internal - 192.168.1.0/24
```

Python-Skripte abrufen und ausführen

Hinweis: Das `create_network_localities.py` Das Skript löscht alle Netzwerklokalisationen auf dem Zielsensor oder der Zielkonsole, bevor die in der CSV-Datei angegebenen neuen Einträge erstellt werden.

1. Gehe zum ExtraHop Code-Beispiele GitHub Repository und laden Sie den Inhalt des `update_network_localities` Verzeichnis auf Ihrem lokalen Computer.
2. Starte den `retrieve_network_localities.py` Drehbuch.
   - Führen Sie für Sensoren und ECA-VMs den folgenden Befehl aus:

     ```
     python3 retrieve_network_localities.py HOST --apikey API_KEY
     ```

     Ersetzen Sie die folgenden Variablen im Befehl durch Informationen aus Ihrem ExtraHop-System:

     • **GASTGEBER:** Die IP-Adresse oder der Hostname des Sensor oder der Konsole.

     • **API-SCHLÜSSEL:** Der API-Schlüssel.
   - Führen Sie für Reveal (x) 360 den folgenden Befehl aus:

     ```
     python3 retrieve_network_localities.py HOST --id ID --secret SECRET
     ```

     Ersetzen Sie die folgenden Variablen im Befehl durch Informationen aus Ihrem ExtraHop-System:

     • **GASTGEBER:** Der Hostname der Reveal (x) 360-API. Dieser Hostname wird auf der Reveal (x) 360 API Access-Seite unter API-Endpunkt angezeigt. Der Hostname enthält das /oauth2/token nicht.

     • **ID:** Die ID der Reveal (x) 360-REST-API-Anmeldeinformationen.

     • **GEHEIM:** Das Geheimnis der Reveal (x) 360 REST-API-Anmeldeinformationen.

   Das Skript speichert Informationen zur Netzwerklokalität im `localities.csv` Datei im aktuellen Verzeichnis. Nach dem Speichern der Datei wird eine Ausgabe ähnlich dem folgenden Text angezeigt:

   ```
   Successfully downloaded network localities.
   ```
3. Aktualisieren Sie die CSV-Datei, um Änderungen an den Netzwerk anzugeben.

   Weitere Informationen finden Sie unter Konsolidierung von Netzwerkstandorten und Umbenennen von Netzwerkorten.
4. Starte den `create_network_localities.py` Drehbuch.

- Führen Sie für Sensoren und ECA-VMs den folgenden Befehl aus:

  ```
  python3 create_network_localities.py HOST --apikey API_KEY --group
   description
  ```

  Ersetzen Sie die folgenden Variablen im Befehl durch Informationen aus Ihrem ExtraHop-System:

  • **GASTGEBER:** Die IP-Adresse oder der Hostname des Sensor oder der Konsole.

  • **API-SCHLÜSSEL:** Der API-Schlüssel.
- Führen Sie für Reveal (x) 360 den folgenden Befehl aus:

  ```
  python3 retrieve_network_localities.py HOST --id ID --secret SECRET --
  group description
  ```

  Ersetzen Sie die folgenden Variablen im Befehl durch Informationen aus Ihrem ExtraHop-System:

  • **GASTGEBER:** Der Hostname der Reveal (x) 360-API. Dieser Hostname wird auf der Reveal (x) 360 API Access-Seite unter API-Endpunkt angezeigt. Der Hostname enthält das /oauth2/token nicht.

  • **ID:** Die ID der Reveal (x) 360-REST-API-Anmeldeinformationen.

  • **GEHEIM:** Das Geheimnis der Reveal (x) 360 REST-API-Anmeldeinformationen.

Das Skript fügt jeden Eintrag zum Sensor oder zur Konsole hinzu. Nach dem Hinzufügen jedes Eintrags wird eine Ausgabe angezeigt, die dem folgenden Text ähnelt:

```
Successfully uploaded entry [auto]: Internal - 192.168.1.0/24
```