Mettre à jour les localités du réseau

Publié: 2024-02-16

Vous pouvez ajouter plusieurs blocs CIDR et adresses IP à une seule localité du réseau, et vous pouvez configurer un nom pour cette localité. Le dépôt GitHub d'ExtraHop contient des scripts Python qui vous aident à consolider et à renommer automatiquement les localités.

Note: Si vous avez créé des localisations réseau dans un microprogramme antérieur à la version 9.0, dans lesquelles vous ne pouviez spécifier qu'un seul bloc CIDR ou adresse IP pour une localité du réseau, vous souhaiterez peut-être consolider et renommer les localisations réseau afin de faciliter la recherche et le filtrage par localité.

Le `retrieve_network_localities.py` Le script récupère toutes les informations de localisation du réseau à partir d'une sonde ou d'une console spécifiée et enregistre les informations dans un fichier CSV. Vous pouvez modifier le fichier CSV pour spécifiez les localités que vous souhaitez consolider et spécifier de nouveaux noms pour les localités existantes. Le `create_network_localities.py` Le script lit ensuite le fichier CSV mis à jour pour remplacer les localités existantes sur une sonde ou une console spécifiée.

Avertissement: Le `create_network_localities.py` Le script supprime toutes les localisations du réseau sur la sonde ou la console cible avant de créer les nouvelles entrées spécifiées dans le fichier CSV.

Consolidation des localités du réseau

Dans le fichier CSV, vous pouvez spécifier les localités que vous souhaitez consolider en attribuant la même description à plusieurs localités. Lorsque le `create_network_localities.py` Un script consolide les localités, il attribue le nom de la première localité du groupe à la nouvelle localité. Supposons, par exemple, que le fichier CSV contienne les entrées suivantes :

réseaux	externe	description	nom
192,168.1.2	Faux	groupe1	[auto] : Interne - 192.168.1.2
192.168.1.1	Faux	groupe1	[auto] : Interne - 192.168.1.1

Exécution du `create_network_localities.py` le script crée la localité réseau suivante sur la sonde ou la console cible :

réseaux	externe	description	nom
192.168.1.2 et 192.168.1.1	Faux	groupe1	[auto] : Interne - 192.168.1.2

Pour consolider les localités du réseau avec la même description dans le fichier CSV que celle décrite dans cette rubrique, vous devez spécifier le `--group description` option lorsque vous exécutez le `create_network_localities.py` script.

Modification du nom des localités du réseau

Dans le fichier CSV, vous pouvez définir des noms descriptifs pour les localités. Le système ExtraHop génère automatiquement des noms pour les localités du réseau s'ils ne sont pas spécifiés par un utilisateur.

Note: Si vous exécutez le `retrieve_network_localities.py` script sur une sonde ou une console exécutant la version 8.9 ou antérieure du microprogramme, le script génère automatiquement des noms pour chaque localité et les ajoute au fichier CSV. Vous pouvez modifier ces noms pour qu'ils soient plus descriptifs en modifiant les noms dans le fichier CSV avant d'exécuter `create_network_localities.py` script.

Le script et le système ExtraHop génèrent des noms selon le format suivant :

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

Dans le texte ci-dessus, l'EXTERNALITÉ est remplacée par « Externe » ou « Interne », et le RÉSEAU est remplacé par l'adresse IP ou le bloc CIDR du réseau. Par exemple, le nom suivant est attribué à une localité réseau pour le bloc CIDR 192.168.1.0/24 :

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

Récupérez et exécutez les scripts Python

Note: Le `create_network_localities.py` Le script supprime toutes les localisations réseau de la sonde ou de la console cible avant de créer les nouvelles entrées spécifiées dans le fichier CSV.

1. Accédez au Exemples de code ExtraHop GitHub référentiel et téléchargez le contenu du `update_network_localities` répertoire sur votre machine locale.
2. Exécutez le `retrieve_network_localities.py` script.
   - Pour les capteurs et les machines virtuelles ECA, exécutez la commande suivante :

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

     Remplacez les variables suivantes de la commande par des informations provenant de votre système ExtraHop :

     • **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console.

     • **CLÉ_API:** La clé API.
   - Pour Reveal (x) 360, exécutez la commande suivante :

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

     Remplacez les variables suivantes de la commande par des informations provenant de votre système ExtraHop :

     • **HÔTE:** Le nom d'hôte de l'API Reveal (x) 360. Ce nom d'hôte est affiché sur la page d'accès à l'API Reveal (x) 360 sous API Endpoint. Le nom d'hôte n'inclut pas le /oauth2/token.

     • **IDENTIFIANT:** L'ID des informations d'identification de l'API REST Reveal (x) 360.

     • **SECRET:** Le secret des informations d'identification de l'API REST Reveal (x) 360.

   Le script enregistre les informations de localisation du réseau dans `localities.csv` fichier dans le répertoire en cours. Une fois le fichier enregistré, une sortie similaire au texte suivant s' affiche :

   ```
   Successfully downloaded network localities.
   ```
3. Mettez à jour le fichier CSV pour spécifier les modifications à apporter aux localités du réseau.

   Pour plus d'informations, voir Consolidation des localités du réseau et Modification du nom des localités du réseau.
4. Exécutez le `create_network_localities.py` script.

- Pour les capteurs et les machines virtuelles ECA, exécutez la commande suivante :

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

  Remplacez les variables suivantes de la commande par des informations provenant de votre système ExtraHop :

  • **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console.

  • **CLÉ_API:** La clé API.
- Pour Reveal (x) 360, exécutez la commande suivante :

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

  Remplacez les variables suivantes de la commande par des informations provenant de votre système ExtraHop :

  • **HÔTE:** Le nom d'hôte de l'API Reveal (x) 360. Ce nom d'hôte est affiché sur la page d'accès à l'API Reveal (x) 360 sous API Endpoint. Le nom d'hôte n'inclut pas le /oauth2/token.

  • **IDENTIFIANT:** L'ID des informations d'identification de l'API REST Reveal (x) 360.

  • **SECRET:** Le secret des informations d'identification de l'API REST Reveal (x) 360.

Le script ajoute chaque entrée à la sonde ou à la console. Après l' ajout de chaque entrée, une sortie similaire au texte suivant s' affiche :

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