Configuration de la détection des périphériques

Publié: 2023-09-19

Le système ExtraHop peut découvrir et suivre les périphériques par leur adresse MAC (découverte L2) ou par leur adresse IP (découverte L3). La découverte L2 offre l'avantage de suivre les mesures d'un périphérique même si l'adresse IP est modifiée ou réattribuée par le biais d'une requête DHCP. Le système peut également découvrir automatiquement les clients VPN.

Avant de commencer
Découvrez le fonctionnement de la découverte de périphériques et de la découverte L2 dans le système ExtraHop. La modification de ces paramètres affecte la manière dont les métriques sont associées aux périphériques.

Note: Les courtiers en paquets peuvent filtrer les requêtes ARP. Le système ExtraHop s'appuie sur les requêtes ARP pour associer les adresses IP L3 aux adresses MAC L2.

Découvrir les appareils locaux

Si vous activez la découverte L3, les périphériques locaux sont suivis par leur adresse IP. Le système crée une entrée parent L2 pour l'adresse MAC et une entrée enfant L3 pour l'adresse IP. Au fil du temps, si l'adresse IP change pour un périphérique, vous pouvez voir une seule entrée pour un parent L2 avec une adresse MAC avec plusieurs entrées enfant L3 avec des adresses IP différentes.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Configuration du système, cliquez sur **Capture**.
3. Cliquez sur **Device Discovery (Découverte de** périphériques).
4. Dans la section Découverte de périphériques locaux, sélectionnez l'une des options suivantes :
   - Cochez la case **Activer la découverte de périphériques locaux** pour activer la découverte de L3.
   - Décochez la case **Activer la** découverte des périphériques locaux pour activer la découverte L2.
5. Cliquez sur **Enregistrer**.

Découverte de périphériques distants par adresse IP

Vous pouvez configurer le système ExtraHop pour qu'il découvre automatiquement des périphériques sur des sous-réseaux distants en ajoutant une plage d'adresses IP.

Note: Si votre système ExtraHop est configuré pour la découverte L2 et que vos périphériques distants demandent des adresses IP par l'intermédiaire d'un agent de relais DHCP, vous pouvez suivre les périphériques par leur adresse MAC et vous n'avez pas besoin de configurer la découverte L3 à distance.

Pour en

Note: savoir plus sur la

découverte de

Note: périphériques, consultez

les considérations importantes relatives à la découverte à distance de L3 :

- Les informations L2, telles que l'adresse MAC du périphérique et le trafic L2, ne sont pas disponibles si le périphérique se trouve sur un réseau différent de celui surveillé par le système ExtraHop. Ces informations ne sont pas transmises par les routeurs et ne sont donc pas visibles par le système ExtraHop.
- Soyez prudent lorsque vous spécifiez la notation CIDR. Un préfixe de sous-réseau /24 peut entraîner la découverte de 255 nouveaux périphériques par le système ExtraHop. Un préfixe de sous-réseau /16 large peut entraîner la découverte de 65 535 nouveaux périphériques, ce qui risque de dépasser votre limite de périphériques.
- Si une adresse IP est supprimée des paramètres de découverte de périphériques L3 distants, elle reste présente dans le système ExtraHop en tant que périphérique L3 distant tant qu'il existe des flux actifs pour cette adresse IP ou jusqu'à ce que la capture soit redémarrée.

  Si la même adresse IP est ajoutée ultérieurement par le biais du flux de données local, ce périphérique L3 distant peut devenir un périphérique L3 local, mais uniquement si le processus de capture est redémarré et que le paramètre Local Device Discovery (Découverte de périphériques locaux) est activé

  .

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Configuration du système, cliquez sur **Capture**.
3. Cliquez sur **Découverte de** périphériques.
4. Dans la section Découverte de périphériques à distance, saisissez l'adresse IP dans le champ Plages d'adresses IP. Vous pouvez spécifier une adresse IP ou une notation CIDR, telle que `192.168.0.0/24` pour un réseau IPv4 ou `2001:db8::/32` pour un réseau IPv6.

   Important: Chaque adresse IP distante communiquant activement et correspondant au bloc CIDR sera découverte en tant que périphérique unique dans le système ExtraHop. La spécification de préfixes de sous-réseaux larges tels que /16 peut entraîner la découverte de milliers de périphériques, ce qui risque de dépasser votre limite de périphériques.
5. Cliquez sur l'icône verte plus**(+**) pour ajouter l'adresse IP. Vous pouvez ajouter une autre adresse IP ou une autre plage d'adresses IP en répétant les étapes 5-6.

   Important: Le processus de capture doit être redémarré lorsque vous supprimez des plages d'adresses IP pour que les modifications soient prises en compte. Nous vous recommandons de supprimer toutes les entrées avant de redémarrer le processus de capture. Il n'est pas nécessaire de redémarrer le processus de capture lors de l'ajout de plages d'adresses IP.

Découvrir les clients VPN

Activez la découverte des adresses IP internes associées aux périphériques clients VPN.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Configuration du système, cliquez sur **Capture**.
3. Cliquez sur **Découverte de périphériques**.
4. Dans la section Découverte de clients V PN, sélectionnez l'une des options suivantes :
   - Cochez la case **Activer la découverte** des clients VPN pour activer la découverte des clients VPN.
   - Décochez la case **Activer la découverte** du client VPN pour désactiver la découverte du client VPN.
5. Cliquez sur **Enregistrer**.