

Configurer Device Discovery

Publié: 2024-09-26

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

Avant de commencer

Découvrez comment [découverte d'équipements](#) et [Découverte de la L2](#) fonctionne dans le système ExtraHop. La modification de ces paramètres affecte la manière dont les métriques sont associées aux appareils.



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

Découvrez les appareils locaux

Si vous activez L3 Discovery, les appareils locaux sont suivis en fonction de 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 d'un équipement change, vous pouvez voir apparaître une seule entrée pour un parent L2 avec une adresse MAC avec plusieurs entrées L3 enfants 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 le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Découverte d'appareils**.
4. Dans le Découverte d'appareils locaux section, sélectionnez l'une des options suivantes :
 - Sélectionnez le **Activer la découverte des équipements locaux** case à cocher pour activer L3 Discovery.
 - Effacez le **Activer la découverte des équipements locaux** case à cocher pour activer L2 Discovery.
5. Cliquez **Enregistrer**.

Découvrez les appareils distants par adresse IP

Vous pouvez configurer le système ExtraHop pour détecter automatiquement les appareils sur les sous-réseaux distants en ajoutant une plage d'adresses IP.



Note: Si votre système ExtraHop est configuré pour L2 Discovery et que vos appareils distants demandent des adresses IP via un agent relais DHCP, vous pouvez suivre les appareils en fonction de leur adresse MAC et vous n'avez pas besoin de configurer Remote L3 Discovery. En savoir plus sur [découverte d'équipements](#).

Considérations importantes concernant Remote L3 Discovery :

- Les informations L2, telles que l'adresse MAC de l'équipement et le trafic L2, ne sont pas disponibles si l'équipement 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 pour 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 étendu peut entraîner la découverte de 65 535 nouveaux périphériques, ce qui peut dépasser la limite de votre équipement.

- Si une adresse IP est supprimée des paramètres de découverte d'appareils L3 distants, elle sera conservée dans le système ExtraHop en tant qu'équipement L3 distant tant qu'il existe des flux actifs pour cette adresse IP ou jusqu'à ce que la capture soit redémarrée. Après un redémarrage, l'équipement est répertorié comme un équipement distant L3 inactif.

Si la même adresse IP est ajoutée ultérieurement via le flux de données local, cet équipement L3 distant peut passer à un équipement L3 local, mais uniquement si le processus de capture est redémarré et que le paramètre Local Device Discovery est activé.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Découverte d'appareils**.
4. Dans le Découverte d'appareils à distance section, dans la Plages d'adresses IP dans le champ, saisissez l'adresse 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 qui correspond au bloc CIDR sera découverte en tant qu'équipement unique dans le système ExtraHop. La spécification de préfixes de sous-réseau étendus tels que `/16` peut entraîner la découverte de milliers de périphériques, ce qui peut dépasser la limite de votre équipement.

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 4 et 5.

- ⚠ **Important:** Le processus de capture doit être redémarré lors de la suppression de plages d'adresses IP avant que les modifications ne prennent effet. 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.

Découvrez les clients VPN

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

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