Trouvez un équipement

Publié: 2023-11-21

Le système ExtraHop détecte automatiquement les appareils tels que les clients, les serveurs, les routeurs, les équilibreurs de charge et les passerelles qui communiquent activement avec d'autres appareils via le fil. Vous pouvez rechercher un équipement spécifique sur le système, puis consulter le trafic et les métriques du protocole sur une page de protocole.

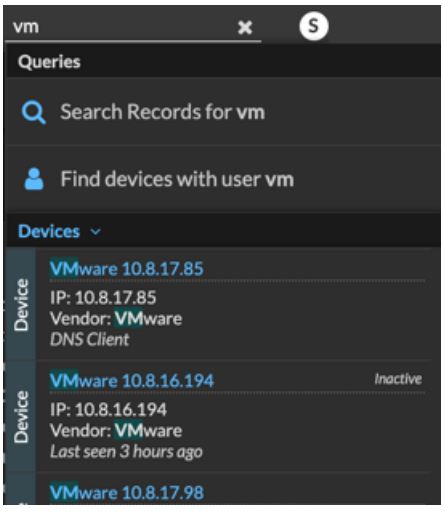
Il existe plusieurs méthodes pour rechercher un équipement :

- Trouvez un équipement à partir d'une recherche globale
- Rechercher un équipement par détails
- Recherche d'appareils par activité du protocole
- Rechercher les appareils auxquels un utilisateur spécifique a accédé
- Rechercher des appareils homologues

Trouvez un équipement à partir d'une recherche globale

Vous pouvez rechercher des appareils dans le champ de recherche global en haut de la page. La recherche globale compare un terme de recherche à plusieurs propriétés d'équipement, telles que le nom d'hôte, l'adresse IP, l'alias connu, le fournisseur, le tag, la description et le groupe de périphériques. Par exemple, si vous recherchez le terme `vm`, les résultats de la recherche peuvent afficher des appareils qui incluent `vm` dans le nom de l'équipement, le fournisseur de l'équipement ou l'étiquette de l'équipement.

1. Tapez un terme de recherche dans le champ de recherche globale en haut de la page.
2. Cliquez **N'importe quel type** puis sélectionnez **Appareils**.
   Les résultats de la recherche sont affichés dans une liste sous le champ de recherche. Cliquez **Plus de résultats** pour faire défiler la liste.



   Les appareils correspondants qui n'ont aucune activité pendant l'intervalle de temps spécifié portent le label Inactif.

   Conseil Les appareils inactifs depuis plus de 90 jours sont exclus des résultats de recherche globaux. Cependant, vous pouvez immédiatement exclure tous les appareils inactifs depuis moins de 90 jours via les paramètres d'administration.
3. Cliquez sur le nom d'un équipement pour ouvrir le Page de présentation de l'appareil et consultez les propriétés et les statistiques de l'équipement.

Rechercher un équipement par détails

Vous pouvez rechercher des appareils en fonction des informations observées sur le réseau, telles que l'adresse IP, l'adresse MAC, le nom d'hôte ou l'activité du protocole. Vous pouvez également rechercher des appareils à l'aide d'informations personnalisées telles que les étiquettes des appareils.

Le filtre de recherche à trois champs vous permet d'effectuer une recherche par plusieurs catégories à la fois. Par exemple, vous pouvez ajouter des filtres pour le nom de l'équipement, l'adresse IP et le rôle afin d'afficher les résultats des appareils qui répondent à tous les critères spécifiés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**.
3. Cliquez **Appareils** dans le volet de gauche, puis cliquez sur **Appareils actifs** graphique.
4. Dans le filtre à trois champs, cliquez sur **Nom** et sélectionnez l'une des catégories suivantes :

Option	Description
Nom	Filtre les appareils en fonction du nom de l'équipement découvert. Par exemple, le nom d'un équipement découvert peut inclure l'adresse IP ou le nom d'hôte.
Adresse MAC	Filtre les appareils en fonction de l'adresse MAC de l'équipement.
Adresse IP	Filtre les appareils par adresse IP au format de bloc IPv4, IPv6 ou CIDR.
Site	Filtre les appareils associés à un site connecté. Console uniquement.
Heure de découverte	Filtre les appareils détectés automatiquement par le système ExtraHop dans l'intervalle de temps spécifié. Pour plus d'informations, voir Création d'un groupe déquipements en fonction de l'heure de découverte.
Niveau d'analyse	Filtre les appareils par niveau d'analyse, ce qui détermine les données et les mesures collectées pour un appareil. Vous ne pouvez pas créer de groupe déquipements dynamique pour les appareils filtrés par niveau d'analyse.
Modèle	Filtre les appareils par marque et nom de modèle. Les conseils suivants peuvent vous aider à trouver le modèle d'équipement que vous souhaitez : • Sélectionnez l'opérateur de correspondance exact (=) pour afficher une liste déroulante des modèles et ensembles de modèles existants. • Sélectionnez l'opérateur de correspondance exact (=), puis sélectionnez **Modèles personnalisés** pour filtrer tous les appareils affectés à un ensemble de modèles personnalisé.

Option	Description
Activité	Filtre les appareils en fonction de l'activité du protocole associée à l'équipement. Par exemple, si vous sélectionnez Serveur HTTP, vous renvoyez les appareils avec des métriques de serveur HTTP et tout autre équipement dont le rôle d'équipement est défini sur Serveur HTTP. Filtre également les appareils qui ont accepté ou initié une connexion externe, ce qui peut vous aider à déterminer si les appareils sont impliqués dans des activités suspectes.
Compte cloud	Filtre les appareils en fonction du compte de service cloud associé à l'équipement.
ID d'instance Cloud	Filtre les appareils en fonction de l'ID d'instance cloud associé à l'équipement.
Type d'instance cloud	Filtre les appareils en fonction du type d'instance cloud associé à l'équipement.
Valeur élevée	Filtre les appareils considérés comme ayant une valeur élevée parce qu'ils fournissent des services d'authentification, prennent en charge des services essentiels sur votre réseau ou sont spécifiés par l'utilisateur comme ayant une valeur élevée.
Actuellement actif	Filtre les appareils en fonction de l'activité observée sur un équipement au cours des 30 dernières minutes.
Type de localité du réseau	Filtre les appareils en fonction de toutes les localisations du réseau interne ou externe.
Nom de la localité du réseau	Filtre les appareils par nom de localité du réseau.
Rôle	Filtre les appareils en fonction du rôle d'équipement attribué, tel que passerelle, pare-feu, équilibreur de charge et serveur DNS.
Logiciel	Filtre les appareils en fonction du logiciel du système d'exploitation détecté sur l'équipement.
Sous-réseau	Filtre les appareils en fonction du sous-réseau associé à l'équipement.
Balise	Filtre les appareils en fonction de balises d'équipement définies par l'utilisateur.
Fournisseur	Filtre les appareils en fonction du nom du fournisseur de l'équipement, tel que déterminé par la recherche de l'identifiant unique de l'organisation (OUI).
Cloud privé virtuel	Filtre les appareils en fonction du VPC associé à l'équipement.
VLAN	Filtre les appareils en fonction de la balise VLAN de l'équipement. Les informations VLAN sont extraites des balises VLAN, si le processus de

Option	Description
	mise en miroir du trafic les conserve sur le port miroir. Disponible uniquement si `devices_accross_vlans` le réglage est défini sur `False` dans le fichier de configuration en cours d'exécution.
Nom CDP	Filtre les appareils en fonction du nom CDP attribué à l'équipement.
Nom de l'instance Cloud	Filtre les appareils en fonction du nom d'instance cloud attribué à l'équipement.
Nom personnalisé	Filtre les appareils en fonction du nom personnalisé attribué à l'équipement.
Nom DHCP	Filtre les appareils en fonction du nom DHCP attribué à l'équipement.
Nom DNS	Filtre les appareils en fonction de tout nom DNS attribué à l'équipement.
Nom NetBIOS	Filtre les appareils en fonction du nom NetBIOS attribué à l'équipement.

5. Sélectionnez l'un des opérateurs suivants ; les opérateurs disponibles sont déterminés par la catégorie sélectionnée :

Option	Description
=	Filtre les appareils qui correspondent exactement au champ de recherche de la catégorie sélectionnée.
↓	Filtre les appareils qui ne correspondent pas exactement au champ de recherche.
≈	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.
≈/	Filtre les appareils qui excluent la valeur du champ de recherche pour la catégorie sélectionnée.
commence par	Filtre les appareils qui commencent par la valeur du champ de recherche pour la catégorie sélectionnée.
existe	Filtre les appareils dont la valeur correspond à la catégorie sélectionnée.
n'existe pas	Filtre les appareils qui n'ont pas de valeur pour la catégorie sélectionnée.
correspondre	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.

6. Dans le champ de recherche, tapez la chaîne à mettre en correspondance ou sélectionnez une valeur dans la liste déroulante. Le type de saisie est basé sur la catégorie sélectionnée.

   Par exemple, si vous souhaitez rechercher des appareils en fonction du nom, tapez la chaîne à rechercher dans le champ de recherche. Si vous souhaitez rechercher des appareils en fonction de leur rôle, sélectionnez-les dans la liste déroulante des rôles.

Conseil Selon la catégorie sélectionnée, vous pouvez cliquer sur l'icône Regex dans le champ de texte pour activer la correspondance par expression régulière.

7. Cliquez **Ajouter un filtre**.
   La liste des appareils est filtrée selon les critères spécifiés.

Prochaines étapes

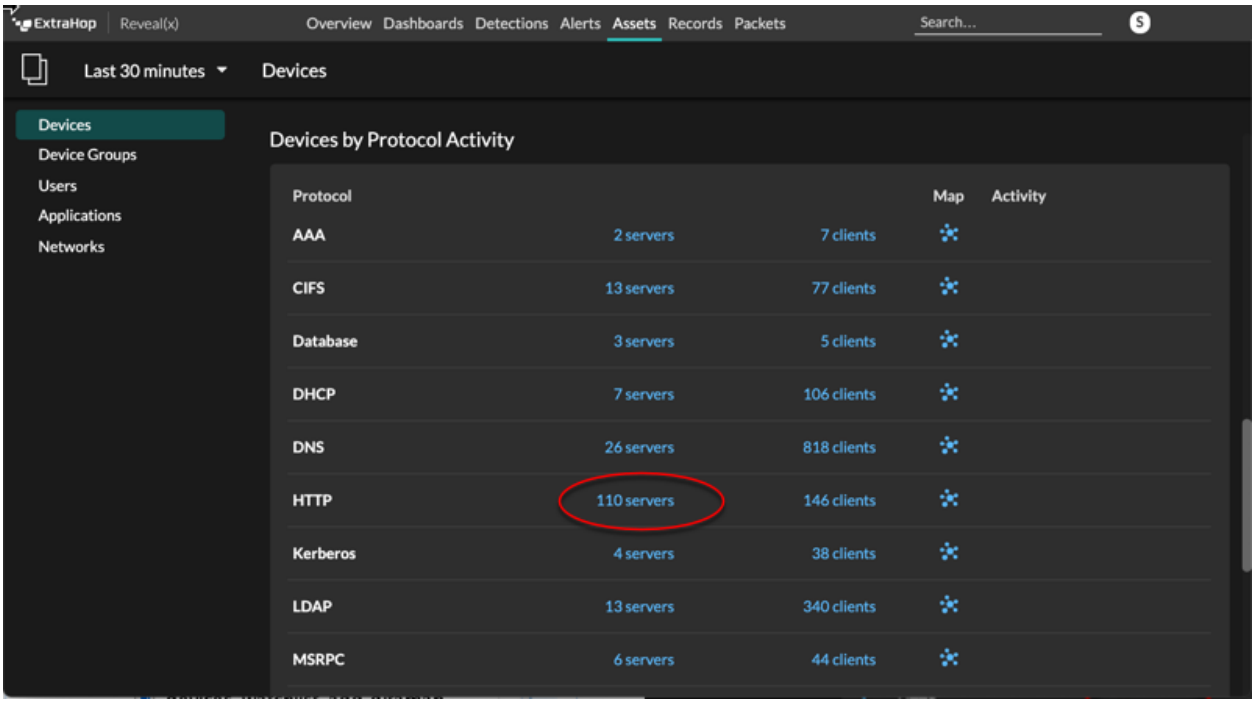
- Cliquez sur le nom d'un équipement pour afficher les propriétés et les statistiques de l'équipement sur le Page de présentation de l'appareil.
- Cliquez **Créer un groupe dynamique** depuis le coin supérieur droit vers créer un groupe d' équipements dynamiques en fonction des critères du filtre.
- Cliquez sur le menu de commande puis sélectionnez PDF ou CSV pour exporter la liste des équipements dans un fichier.

Recherche d'appareils par activité du protocole

La page Appareils affiche tous les protocoles qui communiquent activement sur le système ExtraHop pendant l'intervalle de temps sélectionné. Vous pouvez rapidement localiser un équipement associé à un protocole ou découvrir un équipement hors service qui communique toujours activement via un protocole.

Dans l'exemple suivant, nous vous montrons comment rechercher un serveur Web au sein du groupe de serveurs HTTP.

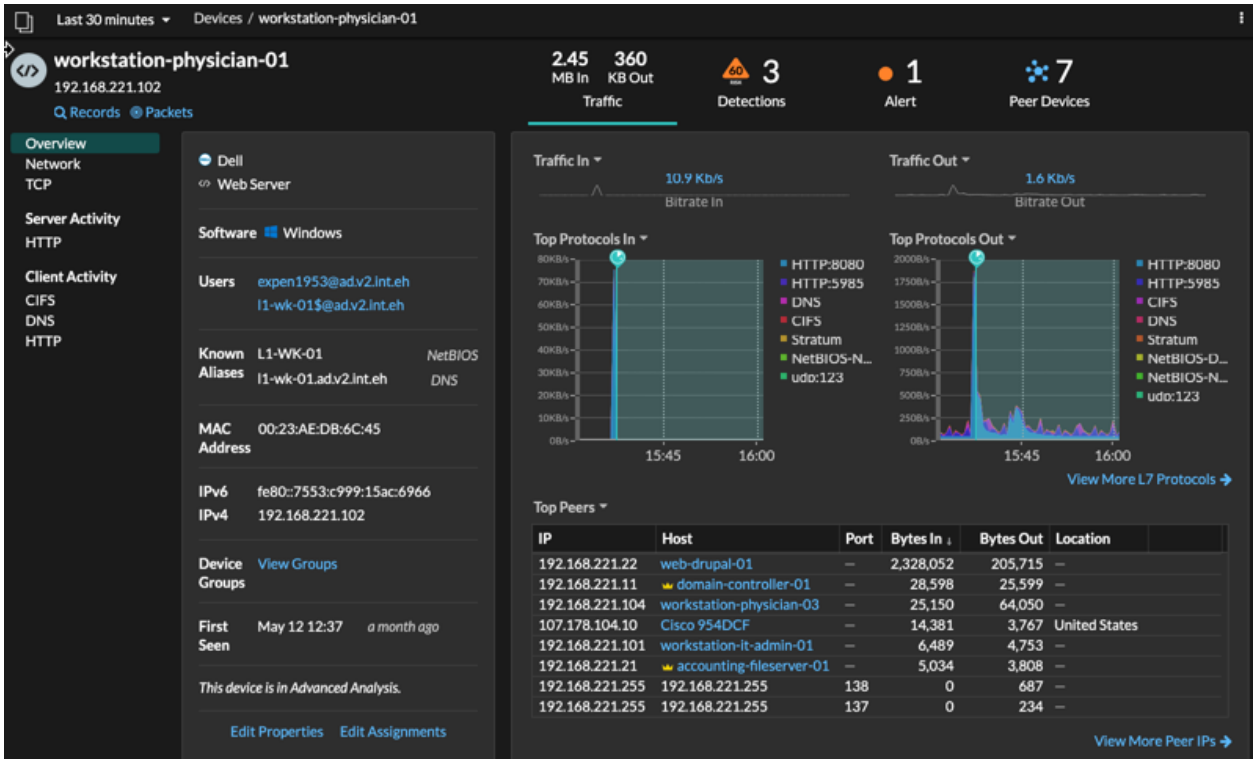
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**.
3. Dans le graphique Devices by Protocol Activity, cliquez sur le nombre de serveurs HTTP, comme illustré dans la figure suivante.



Note: Si vous ne voyez pas le protocole souhaité, le système ExtraHop n'a peut-être pas observé ce type de trafic de protocole sur le fil pendant l'intervalle de temps spécifié, ou le protocole peut nécessiter une licence de module. Pour plus d'informations, consultez le Je ne vois pas le trafic de protocole auquel je m'attendais ? section de la FAQ sur les licences.

La page affiche les mesures de trafic et de protocole associées au groupe de serveurs HTTP.

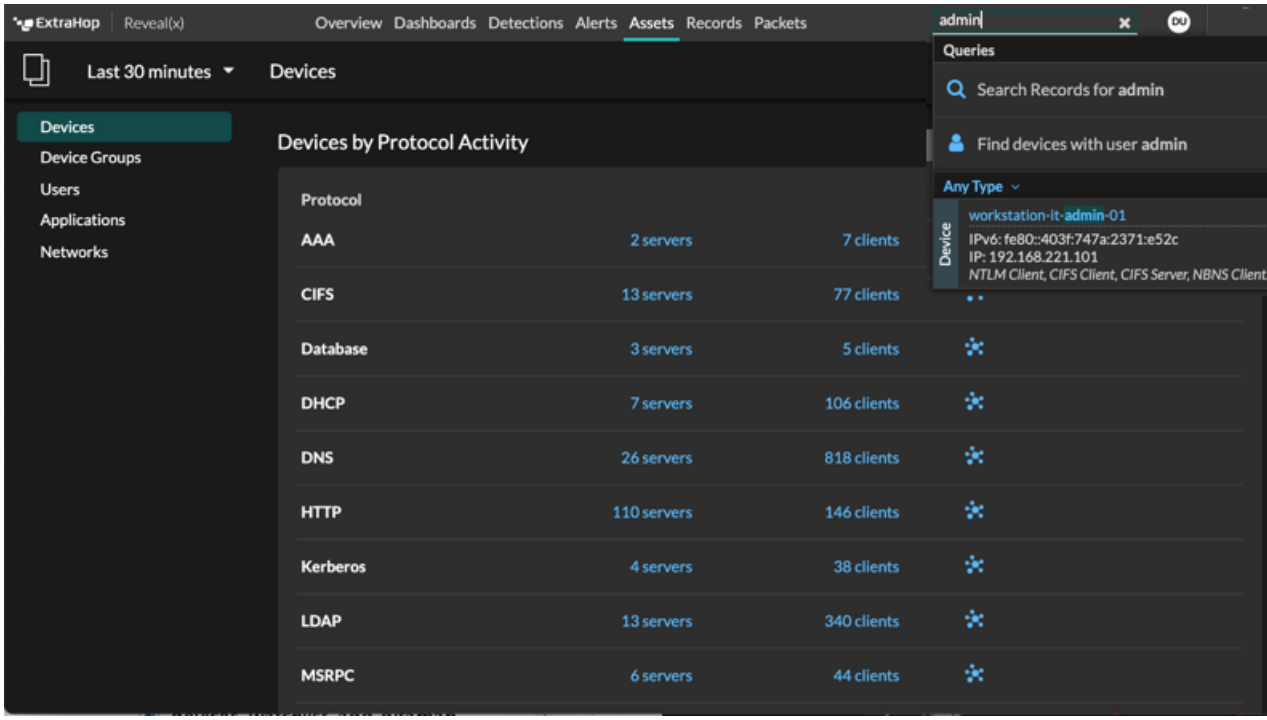
4. En haut de la page, cliquez sur **Membres du groupe**.
La page affiche un tableau répertoriant tous les appareils qui ont envoyé des réponses HTTP par câble pendant l'intervalle de temps sélectionné.
5. Dans le tableau, cliquez sur le nom d'un équipement.
La page affiche les métriques de trafic et de protocole associées à cet équipement, comme dans l'image suivante.



Rechercher les appareils auxquels un utilisateur spécifique a accédé

Sur la page Utilisateurs, vous pouvez voir les utilisateurs actifs et les appareils auxquels ils se sont connectés au système ExtraHop pendant l'intervalle de temps spécifié.

Conseil: Vous pouvez également rechercher des utilisateurs dans le champ de recherche global en haut de la page.



Cette procédure explique comment effectuer une recherche à partir de la page Utilisateurs.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**.
3. Cliquez **Utilisateurs** dans le volet de gauche.
4. Dans la barre de recherche, sélectionnez l'une des catégories suivantes dans la liste déroulante :

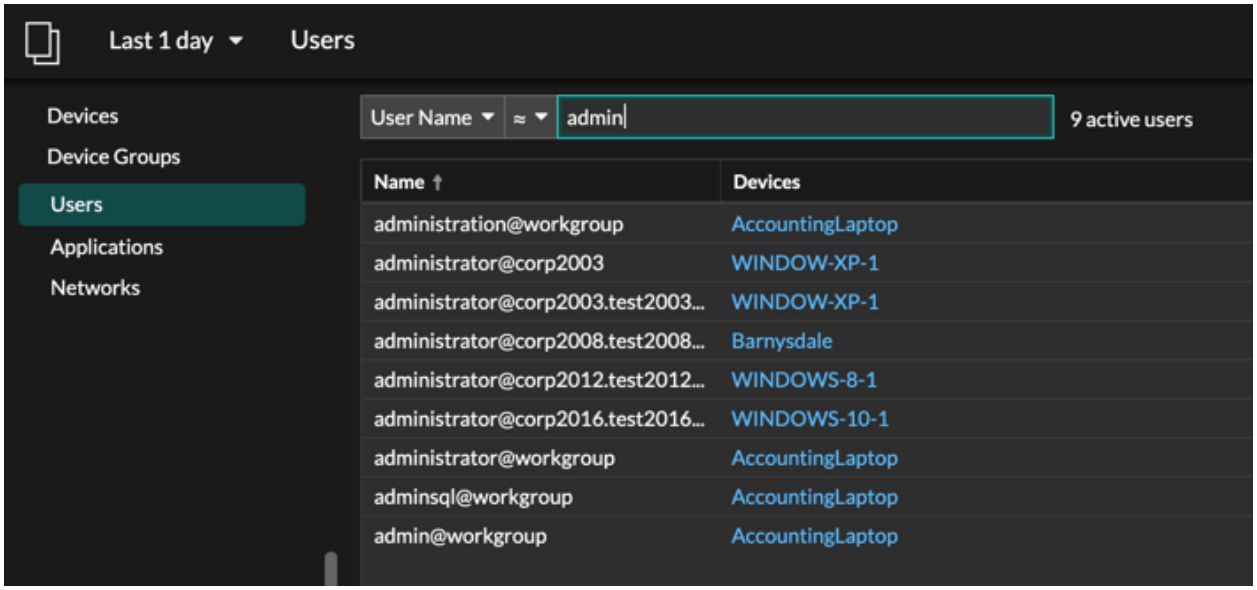
Option	Description
Nom d'utilisateur	Effectuez une recherche par nom d'utilisateur pour savoir à quels appareils l'utilisateur a accédé. Le nom d'utilisateur est extrait du protocole d'authentification, tel que LDAP ou Active Directory.
Protocole	Effectuez une recherche par protocole pour savoir quels utilisateurs ont accédé à des appareils communiquant via ce protocole.
Nom de l'appareil	Effectuez une recherche par nom d'équipement pour savoir quels utilisateurs ont accédé à l'équipement.

5. Sélectionnez l'un des opérateurs suivants dans la liste déroulante :

Option	Description
=	Recherchez un nom ou un équipement correspondant exactement au champ de texte.
↓	Recherchez des noms ou des appareils qui ne correspondent pas exactement au champ de texte.
≈ (par défaut)	Recherchez un nom ou un équipement qui inclut la valeur du champ de texte.

Option	Description
≈/	Recherchez un nom ou un équipement qui exclut la valeur du champ de texte.

6. Dans le champ de texte, saisissez le nom de l'utilisateur ou de l'équipement que vous souhaitez associer ou exclure.
La page Utilisateurs affiche une liste de résultats similaire à la figure suivante :



7. Cliquez sur le nom d'un équipement pour ouvrir le Page de présentation de l'appareil et visualisez tous les utilisateurs qui ont accédé à l'équipement pendant l'intervalle de temps spécifié.

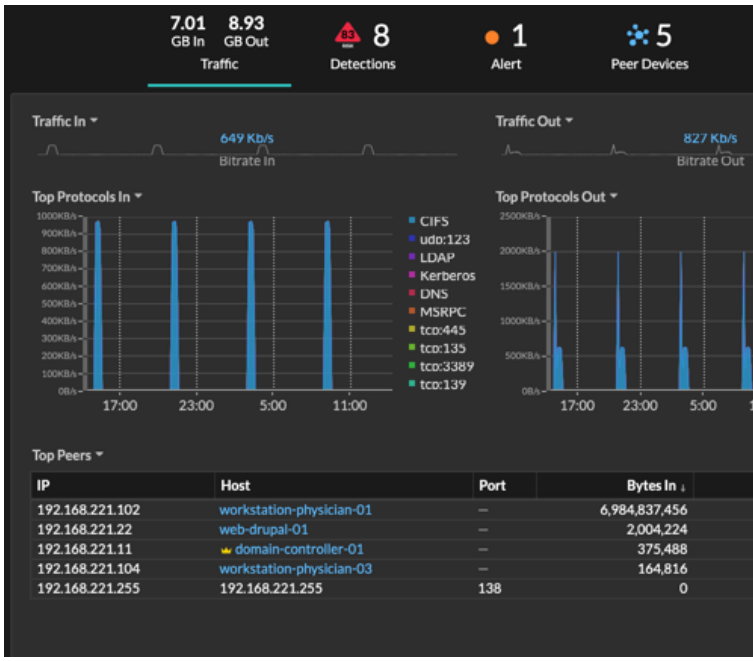
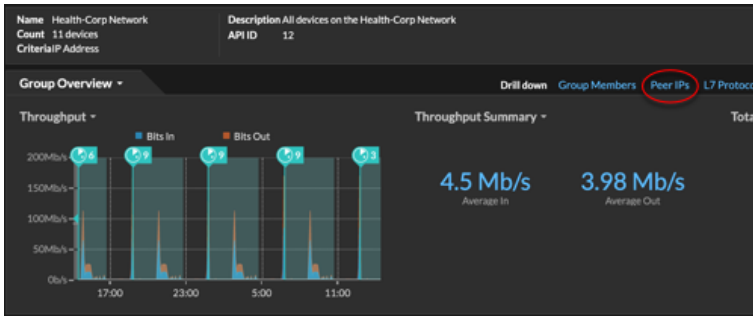
Rechercher des appareils homologues

Si vous souhaitez savoir quels appareils communiquent activement entre eux, vous pouvez effectuer une recherche par adresse IP homologue à partir de la page de protocole d'un équipement ou d'un groupe d'équipements.

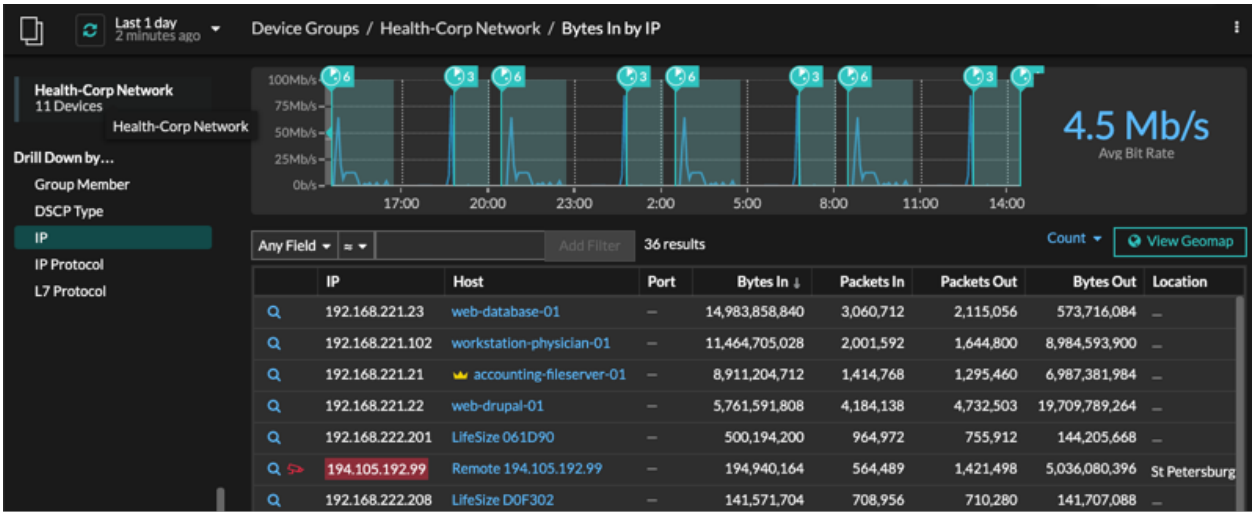
Lorsque vous approfondissez par adresse IP homologue, vous pouvez consulter une liste d'appareils homologues, consulter les mesures de performance ou de débit associées aux appareils homologues, puis cliquer sur le nom d'un équipement homologue pour afficher des mesures de protocole supplémentaires.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis sélectionnez **Appareil** ou **Groupe d'appareils** dans le volet de gauche.
3. Rechercher un équipement ou un groupe déquipements, puis cliquez sur le nom dans la liste des résultats.
4. Sur la page de présentation de l'équipement ou du groupe d'équipements sélectionné, cliquez sur l'un des liens suivants :

Option	Description
Pour les appareils	Cliquez **Afficher plus d'adresses IP homologues**, situé au bas du palmarès Top Peers.

Option	Description
	
Pour les groupes d'équipements	Cliquez **IP des pairs**, situé dans la section Détails dans le coin supérieur droit de la page. 

La liste des appareils homologues s'affiche, qui est ventilée par adresse IP. Vous pouvez examiner les informations relatives aux octets et aux paquets du réseau pour chaque équipement homologue, comme illustré dans la figure suivante.



View the peer device sending or receiving data from the source device. If available, click the hostname to learn about activity on that device.

View network throughput metrics for traffic associated with peer devices.