Appareils

Publié: 2025-01-05

Le système ExtraHop découvre et classe automatiquement les appareils, également appelés points de terminaison, qui communiquent activement sur votre réseau, tels que les clients, les serveurs, les routeurs, les équilibreurs de charge et les passerelles. Chaque équipement bénéficie du plus haut niveau d'analyse disponible, en fonction de la configuration de votre système.

Le système ExtraHop peut découvrir et suivre les appareils par leur adresse MAC (L2 Discovery) ou par leur adresse IP (L3 Discovery). L'activation de L2 Discovery offre l'avantage de suivre les métriques d'un équipement, même si l' adresse IP est modifiée ou réattribuée via une requête DHCP. Si L3 Discovery est activé, il est important de savoir que les appareils peuvent ne pas avoir de corrélation biunivoque avec les périphériques physiques de votre environnement. Par exemple, si un seul équipement physique possède plusieurs interfaces réseau actives, ce périphérique est identifié comme plusieurs appareils par le système ExtraHop.

Une fois qu'un équipement est découvert, le système ExtraHop commence à collecter des métriques en fonction de niveau d'analyse configuré pour cet équipement. Le niveau d'analyse détermine les types de métriques qui sont générés et les fonctionnalités disponibles pour organiser les données métriques.

Appareils de navigation

Cliquez **Actifs** depuis le menu supérieur pour afficher les options de recherche et les graphiques qui fournissent des informations sur les appareils actifs découverts sur votre réseau au cours de l'intervalle de temps sélectionné :

Assistant de recherche AI (nécessite l'accès au module NDR)

Vous permet de rechercher des appareils avec des questions écrit dans un langage naturel et courant. Assistant de recherche IA doit être activé par l'administrateur ExtraHop.

champ de recherche standard

Fournit un filtre pour ajouter des critères rechercher des appareils spécifiques. Cliquez sur le filtre pour modifier les critères de recherche.

Propositions de recherche

Fournit des suggestions de recherches qui tirent parti des filtres de recherche qui ont été créés.

Appareils actifs

Affiche le nombre total d'appareils découverts par le système ExtraHop au cours de l'intervalle de temps sélectionné. Cliquez sur le numéro pour afficher la liste de tous les appareils découverts. À partir de la liste des appareils actifs, vous pouvez rechercher des appareils spécifiques ou cliquez sur le nom d'un appareil pour afficher les détails de l'équipement sur Page de présentation de l'appareil.

Nouveaux appareils

Affiche le nombre d'appareils découverts au cours des cinq derniers jours. Cliquez sur le numéro pour afficher la liste de tous ces appareils.

Appareils par rôle

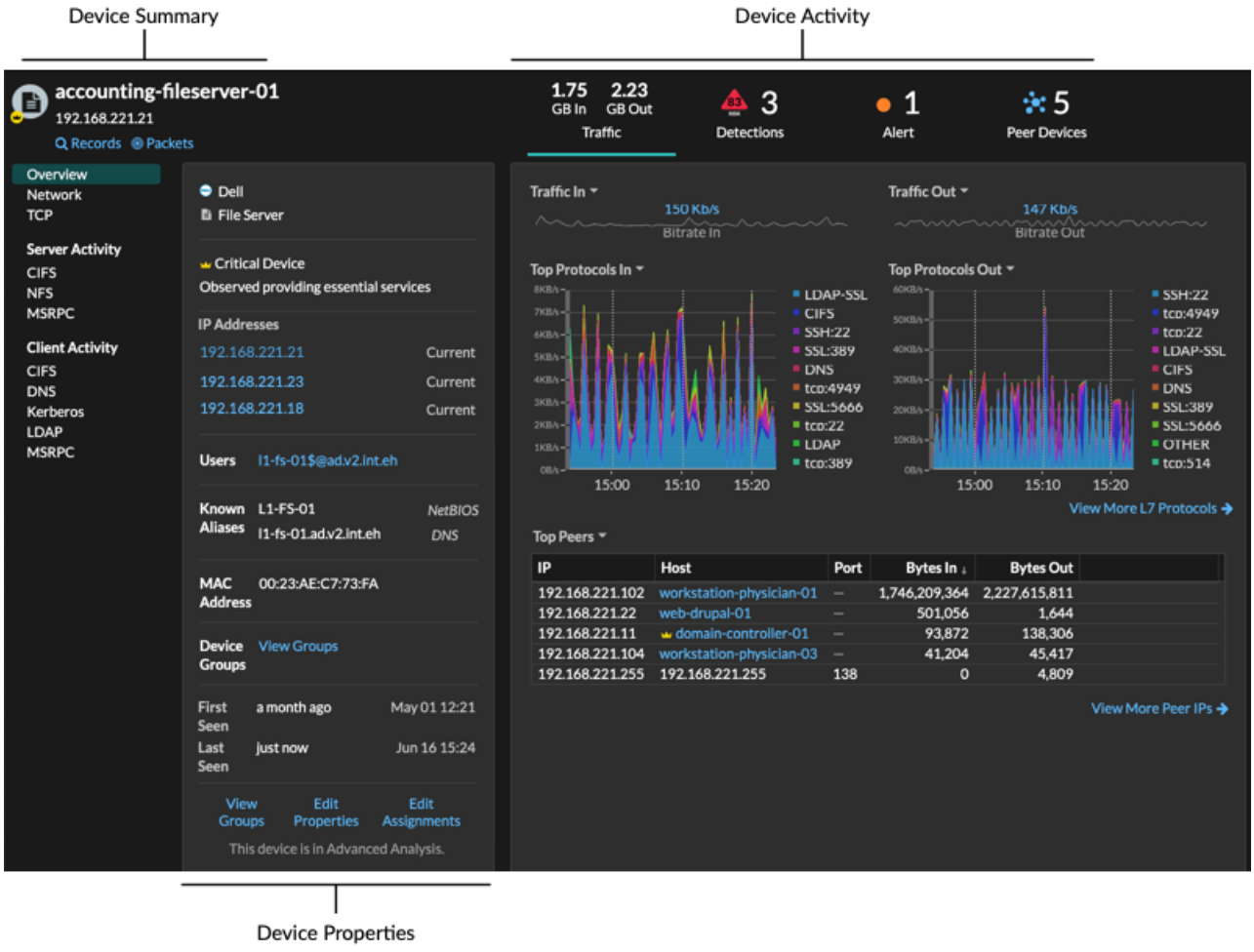
Affiche chaque rôle d'équipement et le nombre d'appareils affectés à chaque rôle actif pendant l'intervalle de temps spécifié. Cliquez sur un rôle d'équipement pour afficher une page intégrée de présentation du groupe d'appareils qui inclut les données métriques, les adresses IP homologues et l'activité du protocole pour ce groupe d'appareils. Vous pouvez également ajouter des critères de filtre supplémentaires et enregistrer le groupe en tant que nouveau groupe dynamique d'équipements.

Appareils par activité de protocole

Affiche la liste des activités de protocole détectées sur votre réseau. Cliquez sur le nom d'un protocole ou sur le nombre d'équipements pour afficher une page de présentation des groupes d'appareils intégrée contenant des graphiques métriques spécifiques concernant cette activité de protocole. Cliquez sur une carte d'activités pour voir toutes les connexions d'appareil à appareil. Vous pouvez également ajouter des critères de filtre supplémentaires et enregistrer le groupe en tant que nouveau groupe dynamique d'équipements.

Page de présentation de l'appareil

En cliquant sur le nom d'un équipement, vous pouvez consulter toutes les informations découvertes à son sujet par le système ExtraHop sur la page Aperçu de l'appareil. La page de présentation de l'appareil est divisée en trois sections : un résumé de niveau supérieur, un panneau des propriétés et un panneau d'activité.



Résumé de l'appareil

Le résumé de l'équipement fournit des informations telles que le nom de l'équipement, l' adresse IP ou l'adresse MAC actuelle et le rôle attribué à l'équipement. Si vous regardez depuis console, le nom du site associé à l'équipement s'affiche également.

- Cliquez **Disques** pour démarrer un requête d'enregistrement qui est filtré par cet équipement.
- Cliquez **Paquets** pour démarrer un requête de paquet qui est filtré par cet équipement.

Propriétés de l'appareil

La section des propriétés de l'équipement fournit les attributs et attributions connus suivants pour l'appareil.

Marque et modèle

La marque (ou le fabricant) de l'équipement et le modèle de l'appareil, le cas échéant.

Le système ExtraHop observe le trafic réseau sur les appareils pour déterminer automatiquement la marque et le modèle, ou vous pouvez attribuer manuellement une nouvelle marque et un nouveau modèle.

Rôle de l'appareil

Le système ExtraHop attribue automatiquement un rôle de l'équipement, comme une passerelle, un serveur de fichiers, une base de données ou un équilibreur de charge, en fonction du type de trafic associé à l'équipement ou à son modèle. Vous pouvez manuellement modifier le rôle d'un équipement.

Appareil de grande valeur

Une icône à valeur élevée apparaît si le système ExtraHop a détecté l'équipement fournissant l'authentification ou les services essentiels ; vous pouvez également spécifier manuellement un équipement comme valeur élevée. Les scores de risque sont augmentés pour les détections sur des appareils à valeur élevée.

Logiciel

Système d'exploitation principal ou logiciel exécuté sur l'équipement.

Conseil : (Intégration à CrowdStrike (sur RevealX 360 uniquement) Vous pouvez cliquer sur des liens depuis des appareils exécutant le logiciel CrowdStrike pour afficher les détails de l'équipement dans CrowdStrike Falçon et initier le confinement des appareils CrowdStrike qui participent à une détection de sécurité.

Adresses IP

Liste des adresses IP observées sur l'équipement à tout moment pendant l'intervalle de temps sélectionné. Si Découverte L2 est activée, la liste peut afficher à la fois les adresses IPv4 et IPv6 qui sont observées simultanément sur l'équipement, ou la liste peut afficher plusieurs adresses IP attribuées via des requêtes DHCP à des moments différents. Un horodateur indique la date à laquelle l'adresse IP a été observée pour la dernière fois sur l'équipement. Cliquez sur une adresse IP pour afficher les autres appareils sur lesquels l'adresse IP a été consultée.

Adresses IP associées

Liste des adresses IP, généralement en dehors du réseau, associées à l'équipement à tout moment pendant l'intervalle de temps sélectionné. Par exemple, un client VPN de votre réseau peut être associé à une adresse IP externe sur l'Internet public. Un horodateur indique la date à laquelle l'adresse IP a été associée pour la dernière fois à l'équipement. Cliquez sur une adresse IP associée pour afficher des détails tels que la localisation géographique et les autres appareils auxquels l'adresse IP a été associée.

Propriétés de l'instance Cloud

Les propriétés d'instance cloud suivantes apparaissent pour l'équipement lorsque vous configurez les propriétés via l'API REST :

- Compte Cloud
- Type d'instance cloud
- Cloud privé virtuel (VPC)
- Sous-réseau
- Nom de l'instance Cloud (apparaît dans la propriété Known Alias)
- Description de l'instance Cloud (les métadonnées de l'instance apparaissent automatiquement pour les appareils dans Flow Analysis)

Voir Ajoutez des propriétés d'instance cloud via l'explorateur d'API ExtraHop pour plus d' informations.

Utilisateurs

Liste des utilisateurs authentifiés connectés à l'équipement. Cliquez sur un nom d'utilisateur pour accéder à la page Utilisateurs et voir à quels autres appareils l'utilisateur est connecté.

Pseudonymes connus

Une liste d'alternatives noms des équipements et le programme ou protocole source.

Note: Plusieurs noms DNS sont pris en charge.

Balises

Le tags attribués à l'équipement. Cliquez sur le nom d'une étiquette pour afficher les autres appareils auxquels la balise est attribuée.

Vu pour la première et la dernière fois

Les horodatages entre la première découverte de l'équipement et la date à laquelle l'activité a été observée pour la dernière fois sur l'appareil. NOUVEAU apparaît si l' équipement a été découvert au cours des cinq derniers jours

Analyse

Le niveau d' analyse que cet équipement reçoit.

Voici quelques moyens d'afficher et de modifier les propriétés de l'équipement :

- Cliquez **Afficher les groupes** pour consulter le groupe d'équipements adhésion à l'équipement.
- Cliquez **Modifier les propriétés** pour afficher ou modifier les propriétés de l'équipement , telles que rôle de l'équipement, des adhésions à des groupes ddevices-équipements, ou étiquettes d'équipement.
- Cliquez **Modifier les devoirs** pour afficher ou modifier lequel alertes et déclencheurs sont attribués à l' équipement.

Activité de l'appareil

La section sur l'activité de l'équipement fournit des informations sur la manière dont l'équipement communique avec d'autres appareils et sur les détections et les alertes associées à l'appareil.

- Cliquez **Trafic** pour afficher les graphiques des protocoles et des données homologues, puis forer vers le bas sur les métriques des graphiques de trafic.

  Note: Les graphiques de trafic ne sont pas disponibles si le niveau d'analyse de l'équipement est en mode découverte. Pour activer les cartes de trafic pour l'appareil, placez l'appareil à Analyse avancée ou Analyse standard.
- Cliquez **Détections** pour afficher la liste des détections, puis cliquez sur le nom d'une détection pour afficher les détails de détection.
- Cliquez **Appareils similaires** pour afficher la liste des appareils présentant un comportement de trafic réseau similaire observé par une analyse d'apprentissage automatique. Des appareils similaires peuvent vous aider à mieux comprendre le comportement normal de l'équipement lors de la recherche de menaces. Cet onglet ne s'affiche que si des appareils similaires sont associés à l'équipement.
- (L'accès au module NPM est requis.) Cliquez **Alertes** pour afficher la liste des alertes, puis cliquez sur le nom d'une alerte pour afficher les détails de l' alerte. Cet onglet ne s'affiche que si des alertes sont associées à l' équipement.
- Cliquez **Appareils homologues** pour consulter une carte dqu`activités, qui est une représentation visuelle de l'activité du protocole L4-L7 entre les appareils de votre réseau. À modifier la carte dqu`activités avec des filtres et des étapes supplémentaires, cliquez sur **Ouvrir la carte des activités**.

Conseil: Vous pouvez ajouter la page Aperçu de l'appareil à un affichage d'activité spécifique à vos favoris en réglant `tab` Paramètre d'URL à l'une des valeurs suivantes :

- `tab=traffic`
- `tab=detections`

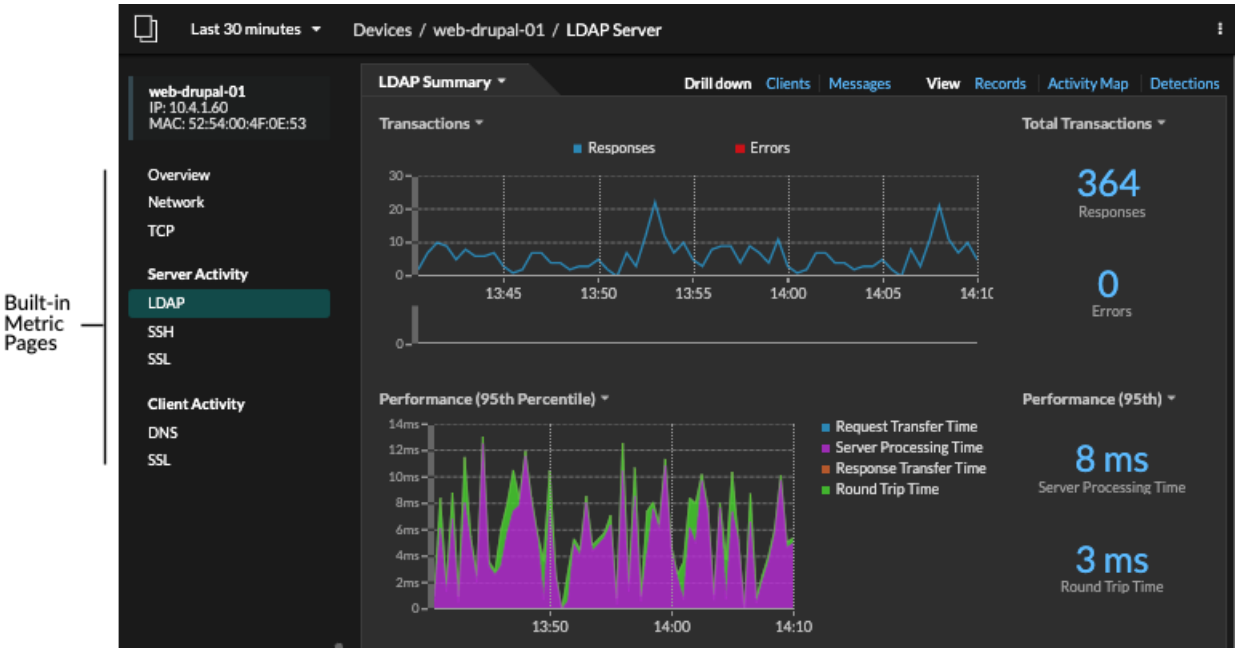
- `tab=alerts`
- `tab=peers`

Par exemple, l'URL suivante affiche toujours l'activité de détection pour l'équipement spécifié :

```
https://example-eda/extrahop/#/metrics/devices//0026b94c03810000/
overview/&tab=detections
```

Métriques de l'appareil

Les métriques sont des mesures en temps réel du trafic de votre réseau que le système ExtraHop calcule à partir des données du réseau ou des flux. Les mesures collectées à partir du trafic des équipements peuvent être consultées dans des tableaux et des graphiques intégrés à partir d'une page d'équipement.



Cliquez sur une page métrique intégrée dans le volet de gauche pour afficher le niveau supérieur métriques relatives à l'équipement ou client et serveur métriques par protocole. Cliquez sur un graphique pour Afficher les pages métriques détaillées, qui affichent les valeurs métriques d'une clé spécifique (telle qu'une adresse IP de client ou de serveur).

Outre les pages intégrées au réseau et au protocole TCP, les appareils affichent des pages métriques intégrées pour les services cloud associés si des données sont disponibles. Voir le Référence des métriques du protocole pour plus d'informations sur les données disponibles sur les pages d'équipement intégrées.

Le système ExtraHop fournit des milliers de métriques intégrées. Voici quelques moyens d' obtenir des informations supplémentaires sur vos appareils

- Création d'un graphique pour visualiser des indicateurs spécifiques et enregistrer le graphique dans un tableau de bord.
- Création d'une carte dactivitiés pour afficher les relations entre les équipements homologues sur des protocoles spécifiés.
- Écrire un déclencheur pour créer métriques personnalisées ou créez un application conteneur pour collecter des métriques pour des appareils spécifiques.

Détails de l'adresse IP

Tapez une adresse IP dans le champ de recherche global ou cliquez sur le lien d'une adresse IP depuis une page de présentation des appareils pour afficher les détails d'une adresse IP.

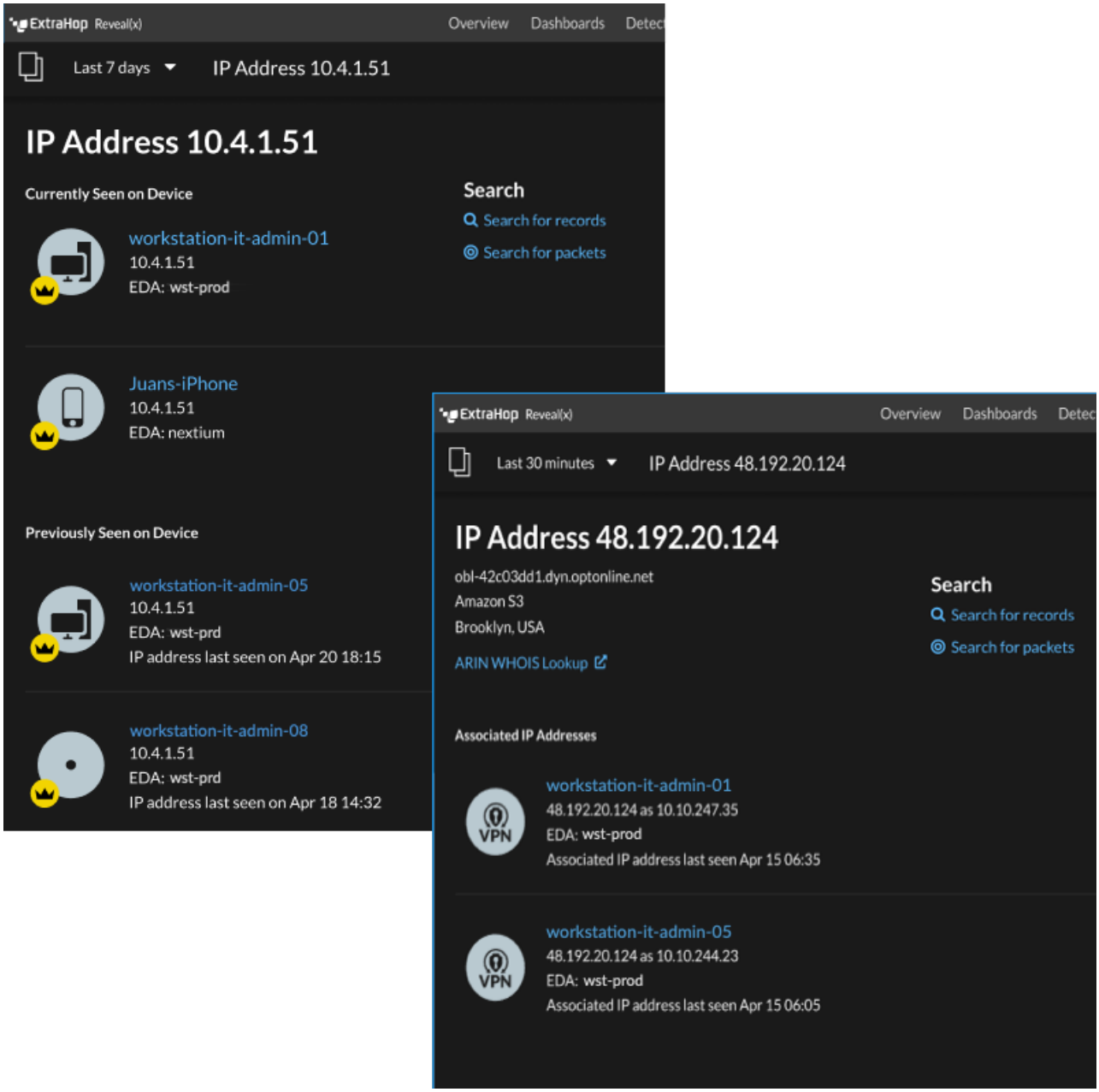
Les informations suivantes s'affichent pour une adresse IP affichée sur un équipement :

- Chaque équipement sur lequel l'adresse IP est actuellement observée, quel que soit l'intervalle de temps sélectionné.
- Chaque équipement sur lequel l'adresse IP a été précédemment observée au cours de l' intervalle de temps sélectionné, y compris l'horodateur depuis la dernière fois que l'adresse IP a été vue sur l'équipement.

Si Découverte L2 est activé, les adresses IPv4 et IPv6 peuvent être observées simultanément sur l'équipement, ou différentes adresses IP peuvent être attribuées à l'équipement par DHCP au fil du temps.

Les informations suivantes s'affichent pour une adresse IP associée à un équipement :

- La géolocalisation de l'adresse IP et des liens vers le site web ARIN Whois.
- Chaque équipement dont l'adresse IP associée a été vue en dehors du réseau à tout moment pendant l'intervalle de temps sélectionné. Par exemple, un client VPN de votre réseau peut être associé à une adresse IP externe sur l'Internet public.
- Tous les services cloud associés à l'adresse IP.
- L'adresse IP de l'équipement telle qu'elle est vue par le système ExtraHop de votre réseau.
- L'horodateur auquel l'adresse IP associée a été vue pour la dernière fois sur l'équipement.



Voici quelques moyens de consulter des informations supplémentaires sur l'adresse IP et l'équipement :

- Passez la souris sur le nom d'un équipement pour afficher ses propriétés.
- Cliquez sur le nom d'un équipement pour afficher la page de présentation de l'appareil.
- Cliquez **Rechercher des enregistrements** pour démarrer un requête d'enregistrement qui est filtré par l'adresse IP .
- Cliquez **Rechercher des paquets** pour démarrer un requête de paquet qui est filtré par cet équipement.

Regroupement d'appareils

Les appareils personnalisés et les groupes d'appareils vous permettent d'agréger les statistiques de vos appareils. Les appareils personnalisés sont des appareils créés par l'utilisateur qui collectent des mesures en fonction de critères spécifiques, tandis que les groupes d'appareils collectent des mesures pour tous les appareils spécifiés d'un groupe. Avec les groupes d'appareils, vous pouvez toujours consulter les statistiques

de chaque appareil ou membre du groupe. Les statistiques d'un équipement personnalisé sont collectées et affichées comme s'il s'agissait d'un seul appareil. Vous ne pouvez pas consulter les mesures individuelles des appareils .

Les groupes d'appareils et les appareils personnalisés peuvent agréger dynamiquement les métriques en fonction des critères que vous avez spécifiés. Nous vous recommandons de sélectionner des critères fiables, tels que l'adresse IP, l'adresse MAC, le VLAN, la balise ou le type de l'équipement. Bien que vous puissiez sélectionner les appareils par leur nom, si le nom DNS n'est pas découvert automatiquement, l'équipement n'est pas ajouté.

	Groupes d'appareils	Appareils personnalisés
Critères	Comprend : • Noms et alias des appareils • adresse IP, adresse MAC, sous-réseau • Port source et port de destination • L'heure de la découverte • Criticité de l'appareil • Rôle de l'appareil • Activité protocolaire • Connexions externes • Fournisseur, modèle, logiciel • Propriétés de l'instance Cloud • VLAN • Étiquettes d'appareils	• adresse IP • Trafic sortant, entrant ou bidirectionnel • adresse IP homologue • Port source • Port de destination • VLAN
Coût de performance	Relativement faible. Étant donné que les groupes d'équipements ne combinent que des métriques déjà calculées, l'effet sur la collecte des métriques est relativement faible. Cependant, le traitement d'un grand nombre de groupes d' appareils comportant un grand nombre d'appareils et des critères complexes prendra plus de temps.	Relativement élevé. Étant donné que les statistiques relatives aux appareils personnalisés sont agrégées en fonction de critères définis par l'utilisateur, un grand nombre d'appareils personnalisés, ou des appareils personnalisés avec des critères extrêmement larges, nécessitent un traitement plus important. Les appareils personnalisés augmentent également le nombre d' objets système pour lesquels les métriques sont validées.
Afficher les statistiques de chaque équipement	Oui	Non
Contrôle d'édition pour les utilisateurs à écriture limitée	Oui Utilisateurs avec privilèges d'écriture limités peut créer et modifier des groupes d'équipements. Cette politique de privilèges globale doit être activée dans les paramètres d'administration.	Non

	Groupes d'appareils	Appareils personnalisés
Meilleures pratiques	Créez pour les appareils locaux sur lesquels vous souhaitez afficher et comparer les statistiques dans un seul graphique. Les groupes d'appareils peuvent être définis en tant que source métrique.	Créez pour les appareils situés en dehors de votre réseau local ou pour les types de trafic que vous souhaitez organiser en tant que source unique. Par exemple, vous souhaiterez peut-être définir toutes les interfaces physiques d'un serveur comme un seul équipement personnalisé afin de mieux visualiser les statistiques de ce serveur dans son ensemble.

Appareils personnalisés

Les appareils personnalisés vous permettent de collecter des statistiques pour les appareils qui se trouvent en dehors de votre réseau local ou lorsque vous disposez d'un groupe d'appareils pour lesquels vous souhaitez regrouper les mesures en tant qu' équipement unique. Ces appareils peuvent même être des interfaces physiques différentes situées sur le même équipement ; l'agrégation des métriques de ces interfaces peut permettre de comprendre plus facilement le niveau de charge de vos ressources physiques dans leur ensemble, plutôt que par interface.

Tu pourrais créer un équipement personnalisé pour suivre des appareils individuels en dehors de votre domaine de diffusion local ou pour collecter des statistiques sur plusieurs adresses IP ou blocs CIDR connus à partir d'un site distant ou d'un service cloud. Tu peux collecter des statistiques de sites distants pour des appareils personnalisés pour découvrir comment les sites distants consomment les services et pour obtenir une visibilité sur le trafic entre les sites distants et un centre de données. Consultez les Référence des métriques du protocole pour obtenir la liste complète des statistiques et des descriptions des sites distants.

Une fois que vous avez créé un équipement personnalisé, toutes les mesures associées aux adresses IP et aux ports sont agrégées dans un seul équipement qui collecte les mesures L2-L7. Un seul équipement personnalisé compte comme un seul appareil dans le cadre de votre capacité sous licence pour Analyse avancée ou analyse standard, qui vous permet de ajouter un équipement personnalisé à la liste de surveillance. Tous les déclencheurs ou alertes sont également attribués à l'équipement personnalisé en tant qu' appareil unique.

Alors que les appareils personnalisés regroupent les métriques en fonction de leurs critères définis, les calculs de métriques ne sont pas traités de la même manière que pour les appareils découverts. Par exemple, un déclencheur peut être attribué à un équipement personnalisé qui valide des enregistrements dans un espace de stockage des enregistrements. Cependant, l'équipement personnalisé n'apparaît ni en tant que client ni en tant que serveur dans aucun enregistrement de transaction. Le système ExtraHop renseigne ces attributs avec l'équipement correspondant à la conversation sur les données filaires.

Les appareils personnalisés peuvent affecter les performances globales du système. Vous devez donc éviter les configurations suivantes :

- Évitez de créer plusieurs appareils personnalisés pour les mêmes adresses IP ou les mêmes ports. Les appareils personnalisés configurés selon des critères qui se chevauchent peuvent dégrader les performances du système.
- Évitez de créer un équipement personnalisé pour un large éventail d'adresses IP ou de ports, car cela pourrait dégrader les performances du système.

Si un grand nombre de périphériques personnalisés affectent les performances de votre système, vous pouvez supprimer ou désactiver un équipement personnalisé. L' ID de découverte unique de l'équipement personnalisé reste toujours dans le système. Voir Créez un équipement personnalisé pour surveiller le trafic des bureaux distants pour vous familiariser avec les appareils personnalisés.

Groupes d'appareils

Un groupe déquipements est un ensemble défini par l'utilisateur qui peut vous aider à suivre les métriques de plusieurs appareils, généralement regroupés selon des attributs partagés tels que l'activité du protocole.

Tu peux créer un groupe dcessaires d'équipements qui vous oblige à ajouter ou à supprimer manuellement un équipement du groupe. Ou, tu peux créer un groupe dcesséquipements dynamique qui inclut des critères qui déterminent quels appareils sont automatiquement inclus dans le groupe. Par exemple, vous pouvez créer un groupe dcessaires dynamique en fonction de l'heure de découverte des équipements qui ajoute des appareils découverts au cours d'un intervalle de temps spécifique.

Par défaut, la page Groupe d'appareils inclut les groupes d'équipements dynamiques suivants que vous pouvez remplacer ou supprimer :

Nouveaux appareils (dernières 24 heures)

Comprend les actifs et les points de terminaison qui ont été vus pour la première fois par le système ExtraHop au cours des dernières 24 heures.

Nouveaux appareils (7 derniers jours)

Comprend les actifs et les points de terminaison qui ont été vus pour la première fois par le système ExtraHop au cours des 7 derniers jours.

Le système ExtraHop inclut également des groupes d'équipements dynamiques intégrés par rôle et par protocole. Vous pouvez attribuer des groupes d'équipements intégrés en tant que source métrique pour des objets tels que des graphiques, des alertes, des déclencheurs et des cartes d'activité. Vous ne pouvez pas remplacer ou supprimer un groupe d'appareils intégré, mais vous pouvez ajouter des critères de filtre et l'enregistrer en tant que nouveau groupe d'appareils.

Sur la page Appareils, cliquez sur le nombre d'équipements correspondant à un rôle ou à un protocole, tel que le contrôleur de domaine ou les clients SMB, pour afficher la page de présentation des groupes d'appareils. En cliquant sur le filtre en haut de la page, vous pouvez ajouter des critères supplémentaires et mettre à jour les données de la page à la demande au lieu de devoir créer un groupe dcessaires d'équipements.

La collecte de métriques auprès de groupes d'équipements n'a aucun impact sur les performances. Nous vous recommandons toutefois de donner la priorité à ces groupes par leur importance pour s'assurer que les bons appareils reçoivent le plus haut niveau d'analyse.

Les groupes d'appareils constituent un bon choix lorsque vous avez des appareils que vous souhaitez appliquer collectivement en tant que source. Par exemple, vous pouvez collecter et afficher des statistiques pour tous vos serveurs Web de production prioritaires dans un tableau de bord.

En créant un groupe d'appareils, vous pouvez gérer tous ces appareils comme une seule source métrique au lieu de les ajouter à vos graphiques en tant que sources individuelles. Notez toutefois que tous les déclencheurs ou alertes attribués sont attribués à chaque membre du groupe (ou à chaque équipement individuel).

Noms et rôles des appareils

Après la découverte d'un équipement, le système ExtraHop suit l'ensemble du trafic associé à l'équipement afin de déterminer le nom et le rôle de l'équipement.

Noms des appareils

Le système ExtraHop découvre les noms des équipements en surveillant passivement les protocoles de dénomination, notamment DNS, DHCP, NETBIOS et Cisco Discovery Protocol (CDP).

Si aucun nom n'est découvert par le biais d'un protocole de dénomination, le nom par défaut est dérivé des attributs de l' équipement, tels que les adresses MAC et IP. Pour certains appareils découverts lors du flux capteurs, le système ExtraHop attribue des noms en fonction du rôle de l'équipement, comme Internet

Gateway ou Amazon DNS Server. Vous pouvez également créer un nom personnalisé ou définir un nom d'instance cloud pour un équipement.

Un équipement peut être identifié par plusieurs noms, qui apparaissent sous la forme d'alias connus sur la page de présentation de l'appareil. Si un équipement porte plusieurs noms, l'ordre de priorité d'affichage est spécifié dans les paramètres d'administration. Vous pouvez effectuer une recherche par n'importe quel nom pour trouver un équipement.

Note: Les noms personnalisés ne sont pas synchronisés entre les systèmes ExtraHop connectés. Par exemple, un nom personnalisé créé sur une sonde n'est pas disponible sur une console connectée.

Si le nom d'un équipement n'inclut pas de nom d'hôte, le système ExtraHop n'a pas encore observé le trafic du protocole de dénomination associé à cet équipement. Le système ExtraHop n' effectue pas de recherches DNS pour les noms d'équipement.

Rôles des appareils

En fonction du type de trafic associé à l'appareil ou à son modèle, le système ExtraHop attribue automatiquement un rôle à l'équipement, tel qu'une passerelle, un serveur de fichiers, une base de données ou un équilibreur de charge. Le rôle Autre est attribué aux appareils qui ne peuvent pas être identifiés.

Un équipement ne peut se voir attribuer qu'un seul rôle à la fois. Vous pouvez manuellement modifier le rôle d'un équipement, ou le système ExtraHop peut réattribuer un rôle différent si le trafic observé et le comportement changent. Par exemple, si un PC a été transformé en serveur Web, vous pouvez modifier le rôle immédiatement, ou le changement peut être observé au fil du temps et le rôle mis à jour par le système.

Le système ExtraHop identifie les rôles suivants :

Icône	Rôle	Descriptif
	Appareil personnalisé	Un équipement créé par l'utilisateur qui collecte des métriques en fonction de critères spécifiques. Le système ExtraHop attribue automatiquement ce rôle lorsque vous créer un équipement personnalisé. Vous ne pouvez pas attribuer manuellement le rôle personnalisé à un équipement.
	Simulateur d'attaque	Un équipement qui exécute un logiciel de simulation de brèches et d'attaques (BAS) pour simuler des attaques sur un réseau.
	Base de données	Un équipement qui héberge principalement une instance de base de données.
	Serveur DHCP	Un équipement qui traite principalement l'activité du serveur DHCP.

Icône	Rôle	Descriptif
	Serveur DNS	Un équipement qui traite principalement l'activité du serveur DNS.
	Contrôleur de domaine	Un équipement qui fait office de contrôleur de domaine pour l'activité des serveurs Kerberos, SMB et MSRPC.
	Serveur de fichiers	Un équipement qui répond aux demandes de lecture et d'écriture de fichiers via les protocoles NFS et SMB.
	Pare-feu	Un équipement qui surveille le trafic réseau entrant et sortant et bloque le trafic conformément aux règles de sécurité. Le système ExtraHop n'attribue pas automatiquement ce rôle aux appareils.
	Passerelle	Un équipement qui fait office de routeur ou de passerelle. Le système ExtraHop recherche les appareils associés à un grand nombre d'adresses IP uniques (au-delà d' un certain seuil) lors de l'identification des passerelles. Les noms des équipements de passerelle incluent le nom du routeur, tel que Cisco B1B500. Contrairement à d'autres Appareils parents L2, vous pouvez ajouter un équipement de passerelle à la liste de surveillance pour une analyse avancée.
	Caméra IP	Un équipement qui envoie des données d'image et de vidéo via le réseau. Le système ExtraHop attribue ce rôle en fonction du modèle d'équipement.
	Équilibreur de charge	Un équipement qui agit comme un proxy inverse pour distribuer le trafic sur plusieurs serveurs.

Icône	Rôle	Descriptif
	Dispositif médical	Un équipement conçu pour les besoins de santé et les environnements médicaux. Le système ExtraHop peut attribuer ce rôle si un équipement est d'une marque et d'un modèle médicaux connus ou s'il traite du trafic DICOM.
	Appareil mobile	Un équipement sur lequel un système d'exploitation mobile est installé, tel qu'iOS ou Android.
	Passerelle NAT	Un équipement qui fait office de passerelle de traduction d'adresses réseau (NAT). Le système ExtraHop peut attribuer ce rôle si un équipement est associé à au moins quatre familles d'empreintes digitales de système d'exploitation ou à au moins quatre marques et modèles de matériel ou de fournisseurs. Une fois ce rôle attribué à un appareil, les propriétés du logiciel, de la marque et du modèle du matériel et des utilisateurs authentifiés n'apparaissent plus pour l'appareil.
	PC	Un équipement tel qu'un ordinateur portable, un ordinateur de bureau, une machine virtuelle Windows ou un appareil macOS qui traite le trafic des clients DNS, HTTP et TLS.
	Imprimante	Un équipement qui permet aux utilisateurs d'imprimer du texte et des graphiques à partir d'autres appareils connectés. Le système ExtraHop attribue ce rôle en fonction du modèle d' équipement ou du trafic observé sur mDNS (DNS multicast).
	Téléphone VoIP	Un équipement qui gère les appels téléphoniques de voix sur IP (VoIP).

Icône	Rôle	Descriptif
	Client VPN	Un équipement interne qui communique avec une adresse IP distante. Si La découverte des clients VPN est activée, le système ExtraHop attribue automatiquement ce rôle aux appareils internes communiquant avec des adresses IP distantes via une passerelle VPN. Vous ne pouvez pas attribuer manuellement le rôle de client VPN à un équipement.
	Passerelle VPN	Un équipement qui connecte deux ou plusieurs appareils ou réseaux VPN ensemble pour relier des connexions distantes. Le système ExtraHop attribue ce rôle aux appareils dotés d'un grand nombre de pairs VPN externes si la classification automatique de ce rôle est activée dans le fichier de configuration en cours d'exécution.
	Scanner de vulnérabilité	Un équipement qui exécute des programmes d'analyse de vulnérabilités.
	Serveur proxy Web	Un équipement qui traite les requêtes HTTP entre un équipement et un autre serveur.
	Serveur Web	Un équipement qui héberge principalement des ressources Web et répond aux requêtes HTTP.
	Point d'accès Wi-Fi	Un équipement qui crée un réseau local sans fil et projette un signal de réseau sans fil vers une zone désignée. Le système ExtraHop attribue ce rôle en fonction du modèle d'équipement.