Surveillez les nouveaux appareils de votre réseau

Publié: 2024-08-08

Chaque nouvel équipement connecté à votre réseau comporte des risques potentiels. Il est donc important d'identifier rapidement les appareils récemment découverts et de surveiller leur activité. Le système ExtraHop crée automatiquement un groupe déquipements pour les appareils découverts le jour précédent et la semaine dernière. Toutefois, ce groupe déquipements collecte des statistiques limitées par défaut et n'est pas visible sur le tableau de bord de votre système.

Dans cette présentation, nous allons d'abord prioriser le groupe d'appareils récemment découverts afin de recueillir des statistiques complètes, puis nous allons créer un tableau de bord pour surveiller l'activité des équipements, et enfin nous allons créer un rapport quotidien pour suivre les changements intéressants.

Une fois cette procédure pas à pas terminée, vous serez en mesure de répondre aux questions suivantes :

- Combien de nouveaux appareils sont apparus sur mon réseau la semaine dernière ?
- Quel est le volume de trafic entrant et sortant associé aux nouveaux appareils ?
- Quels sont les changements quotidiens liés à l'activité des nouveaux équipements ?
- Comment en savoir plus lorsque vous constatez une activité intéressante sur un équipement ?

Prérequis

- Familiarisez-vous avec les concepts présentés dans cette procédure pas à pas en lisant le FAQ sur la découverte des appareils, Classer les groupes par ordre de priorité pour l'Analyse avancée, le FAQ sur les métriques et le Référence des métriques du protocole sujets.
- Vous devez avoir accès à un console avec des privilèges d'administration du système et des accès pour planifier un rapport.

Prioriser les nouveaux appareils pour une Analyse avancée

Tout d'abord, nous allons donner la priorité au groupe diciels récemment découvert afin de recueillir des statistiques complètes via Analyse avancée. En donnant la priorité à votre groupe pour l'Analyse avancée, vous vous assurez que le système ExtraHop collecte les métriques L2-L7 pour les nouveaux appareils.

Si votre console n'est pas gestion des priorités d'analyse pour vos capteurs, vous pouvez effectuer cette procédure pas à pas à partir d'un capteur à la place et omettre la dernière section. (Les rapports planifiés ne peuvent être créés qu'à partir d'un console).

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système, puis sur **Priorités d'analyse**.
3. Dans le Pour une Analyse avancée section, cliquez sur **ajout d'un groupe** pour ajouter un groupe initial ou **Ajouter un groupe** pour ajouter des groupes supplémentaires.
4. Tapez `new devices` dans le **GROUPE** liste déroulante, puis sélectionnez **Nouveaux appareils (7 derniers jours)**.
5. En haut de la page, cliquez sur **Enregistrer**.

Créons maintenant un tableau de bord pour surveiller l'activité des nouveaux équipements.

Création d'un tableau de bord

En créant un tableau de bord pour votre groupe, vous pouvez visualiser l'activité des équipements en un coup d'œil.

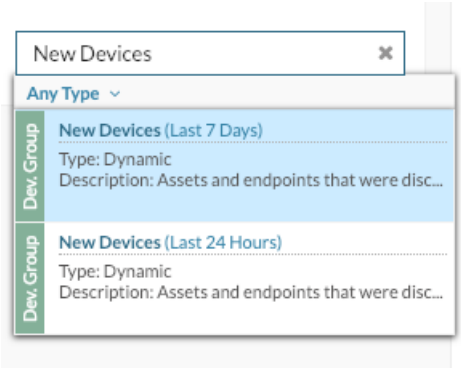
1. En haut de la page, cliquez sur **Tableaux de bord**.
2. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit et sélectionnez **Nouveau tableau de bord** pour créer un tableau de bord vide.
3. Entrez le nom de votre tableau de bord dans le **Titre** champ. Pour cette procédure pas à pas, tapez `Nouveaux appareils`.
4. Cliquez **Créez**.
   Lorsque vous créez un nouveau tableau de bord, un espace de travail s'ouvre dans un mode de mise en page modifiable. Cet espace de travail contient une seule région et deux widgets vides : un graphique et une zone de texte.
5. Supprimez la zone de texte en effectuant les étapes suivantes :
   a) Cliquez sur le menu de commande ⋮ dans le coin supérieur droit du widget de zone de texte et sélectionnez **Supprimer**.
   b) Cliquez **Supprimer le widget**.
   Les widgets de zone de texte peuvent inclure un texte explicatif personnalisé concernant un tableau de bord ou un graphique. Pour cette procédure pas à pas, nous n'ajouterons toutefois pas de texte.

Ajoutons ensuite des graphiques à notre tableau de bord qui indiquent quels nouveaux appareils ont été découverts la semaine dernière et ce qu'ils ont fait sur le réseau.

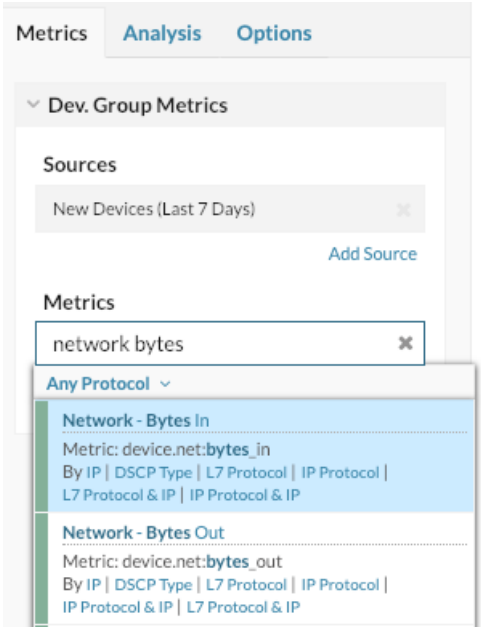
Ajoutez un graphique qui montre le débit du trafic pour les nouveaux appareils

Au cours de cette étape, nous allons créer un tableau répertoriant tous les appareils découverts au cours des sept derniers jours. Le volume de trafic entrant et sortant observé au cours de la semaine dernière s'affiche à côté de chaque équipement. À partir de ce tableau de bord, vous pouvez connaître le volume de trafic généré par chaque nouvel équipement.

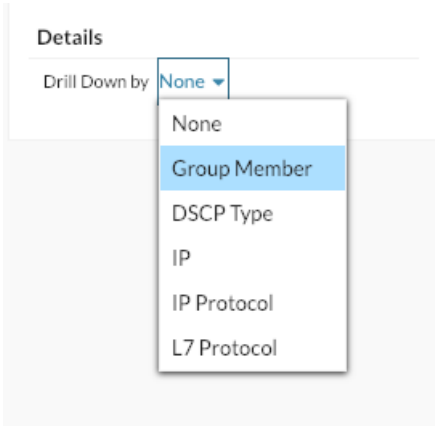
1. Cliquez sur le widget graphique vide dans le tableau de bord que vous venez de créer pour ouvrir l'explorateur de métriques.
2. Cliquez **Ajouter une source**.
3. Dans le champ Sources, tapez `New Devices` pour filtrer les résultats, puis sélectionnez **Nouveaux appareils (7 derniers jours)** pour une sonde connectée.



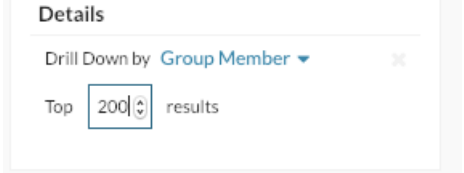
4. Dans le champ Métriques, tapez `network bytes` pour filtrer les résultats à partir de toutes les mesures disponibles, puis cliquez sur **Octets réseau entrants**.



5. Cliquez **Ajouter une métrique**, tapez `network bytes`, puis sélectionnez **Octets réseau en sortie**.
6. Au bas de la fenêtre, cliquez sur **Tableau**.
7. Dans le Détails section, cliquez **Aucune**, puis cliquez sur **Membre du groupe**.

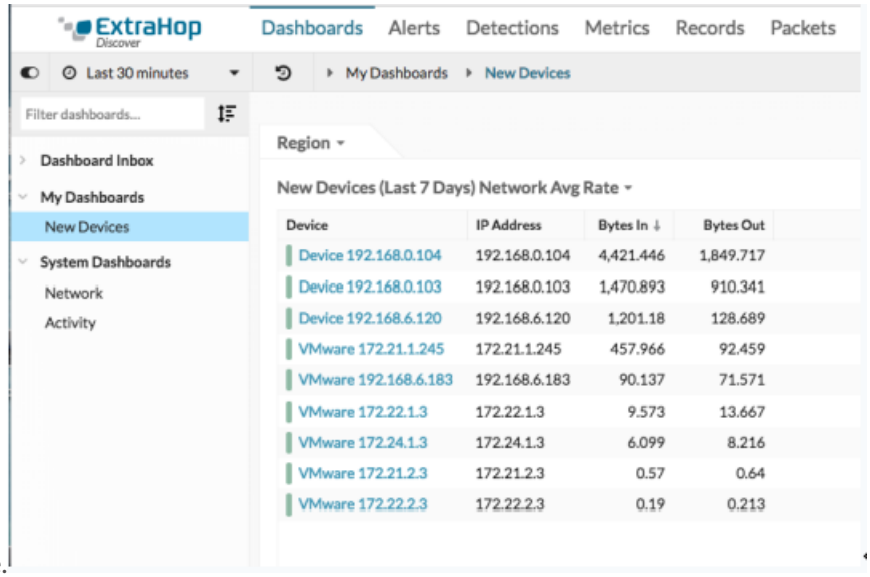


8. Optionnel : Cliquez sur **Des options** onglet. Dans le Unités section, cliquez **Convertir des octets en bits**.
   Le débit s'affiche désormais en bits par seconde.
9. Optionnel : Sous la métrique, cliquez sur **Taux moyen** puis cliquez sur **Compter**.
   Le débit total s'affiche désormais au lieu d'un nombre moyen de débit par seconde.
10. Dans le champ Meilleurs résultats, cliquez sur **5**, tapez `200`, puis appuyez sur `Entrez`.



11. Cliquez **Enregistrer**.
12. Cliquez **Quitter le mode Layout**.

Le tableau indique désormais tous les appareils récemment découverts au cours de la semaine dernière et leur débit, comme le montre la figure suivante.



Configurons maintenant un rapport quotidien pour surveiller les nouveaux appareils.

Planifiez un rapport quotidien

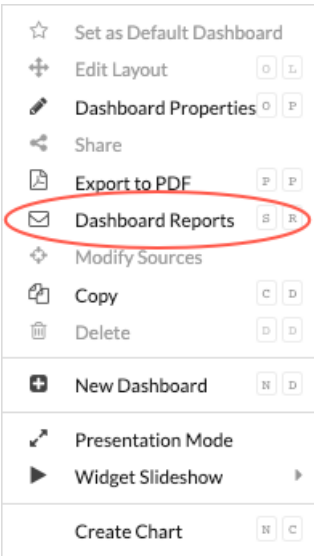
Après avoir créé votre tableau de bord des nouveaux appareils, vous pouvez planifier un rapport quotidien sur l'activité des nouveaux appareils au cours de la dernière journée. Ce rapport est un fichier PDF du tableau de bord, qui peut être envoyé par e-mail à n'importe quel destinataire. Les rapports planifiés ne peuvent être créés qu'à partir d'un console.

Dans les étapes suivantes, nous allons vous montrer comment planifier un rapport quotidien qui sera diffusé à 7h00.

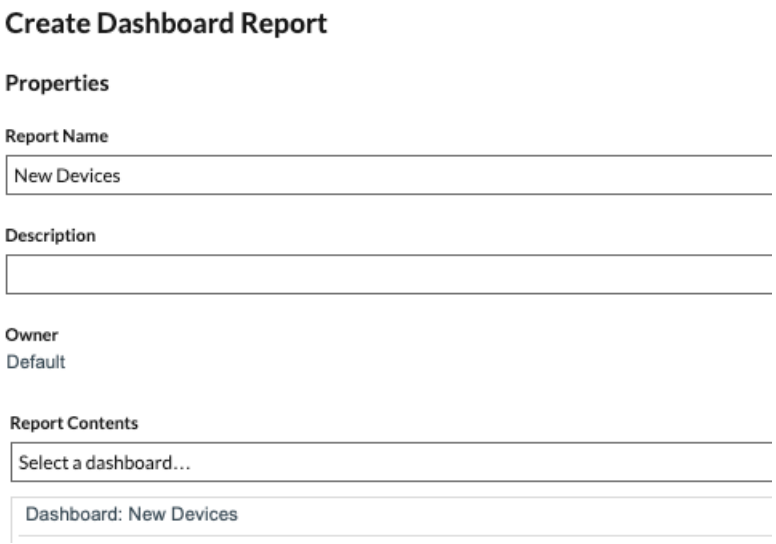
1. À partir du console, cliquez **Tableaux de bord** en haut de la page, puis cliquez sur **Nouveaux appareils** tableau de bord dans le volet de gauche.

   Note: Chaque rapport ne peut être lié qu'à un seul tableau de bord. Vous pouvez créer un rapport pour n'importe quel tableau de bord qui vous appartient ou qui a été partagé avec vous.

2. Dans le coin supérieur droit de la page du tableau de bord, cliquez sur le menu de commande ⋮, puis cliquez sur **Rapports de tableau de bord**.

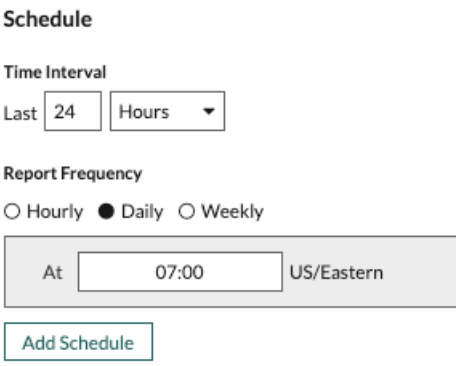


3. Une page de rapports planifiés s'affiche et affiche tous les rapports stockés sur console.
   Si aucun rapport n'a été créé, cette page est vide.
4. Dans le coin supérieur droit, cliquez sur **Créez**.
5. Dans le **Nom du rapport** champ, le nom du tableau de bord s' affiche, comme illustré dans la figure suivante.



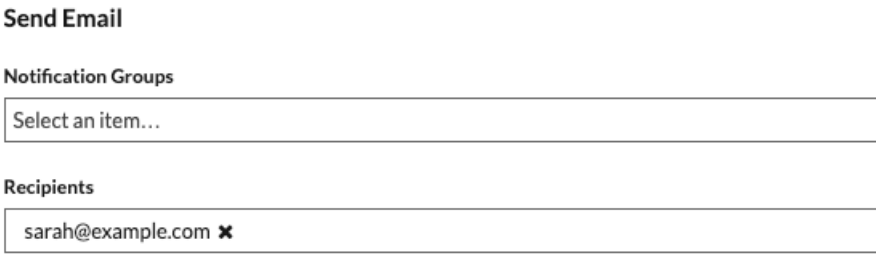
6. Faites défiler l'écran vers le bas jusqu'à Intervalle de temps section. Laissez le réglage par défaut de **Les 10 derniers jours**. Le rapport inclura le trafic de nouveaux équipements survenu au cours de la journée précédente.

   Note: Pour plus d'informations sur la configuration de chaque champ, voir Création d'un rapport planifié.
7. Dans le Fréquence des rapports section, cliquez sur **À** dans la liste déroulante, puis cliquez sur 07:00 pour envoyer un e-mail quotidien à 7:00



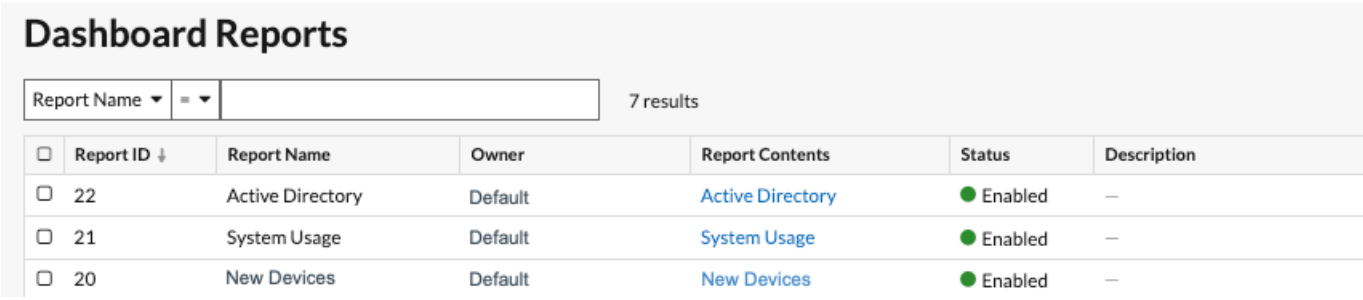
Note: L'heure système définie pour votre console détermine le fuseau horaire affiché lors de la configuration de votre rapport. Pour plus d'informations sur la configuration du fuseau horaire de votre console via les paramètres d' administration d'ExtraHop, voir Configurer l'heure du système.

8. Tapez votre adresse e-mail dans le champ Destinataires.



Note: Le système ExtraHop ne stocke pas les adresses e-mail des comptes utilisateurs ExtraHop. Toutefois, si votre système ExtraHop RevealX Enterprise est configuré avec un groupe de messagerie, vous pouvez sélectionner un groupe de notifications à envoyer par e-mail. RevealX 360 ne prend pas en charge les groupes de notifications par e-mail.

9. Optionnel : Cliquez **Envoyer maintenant** pour envoyer un e-mail de test au destinataire.
10. Cliquez **Terminé**. Votre rapport planifié apparaît désormais sur la page Rapports du tableau de bord, comme le montre la figure suivante.



11. Dans le coin inférieur droit de la page, cliquez sur **Terminé** à nouveau pour revenir à votre tableau de bord.

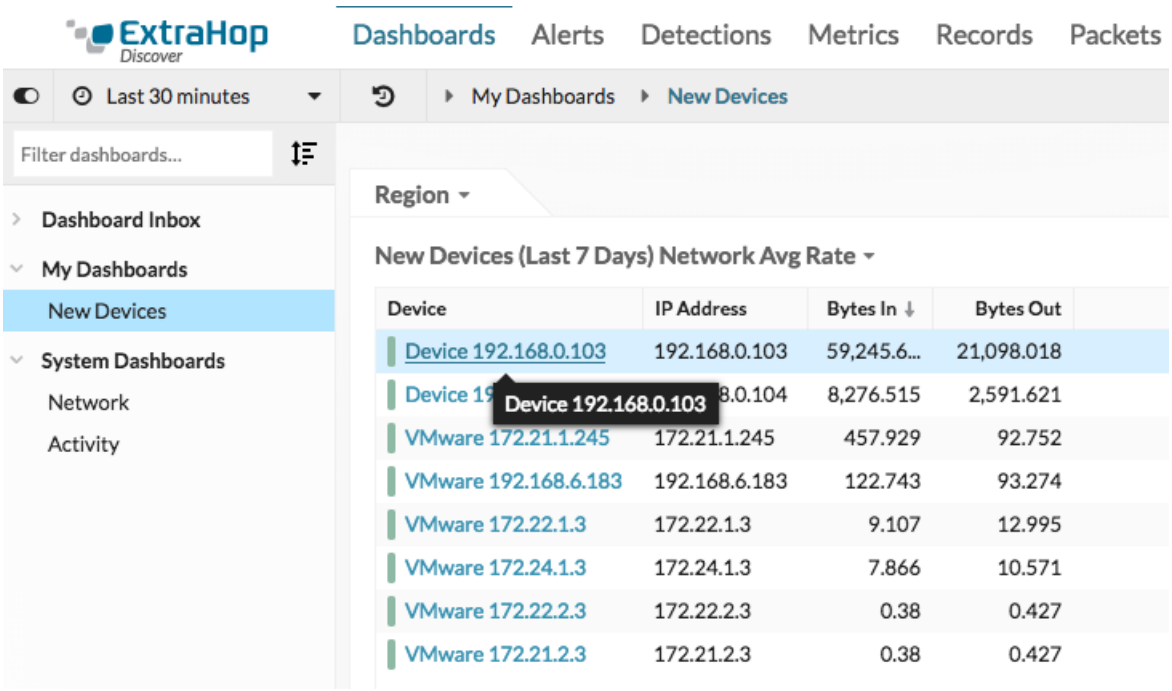
Lorsque vous recevez le fichier PDF envoyé par e-mail, cliquez sur **Voir le rapport sur ExtraHop** pour accéder au tableau de bord qui a généré le rapport. Pour les utilisateurs d'ExtraHop, le lien ouvre la console et le tableau de bord est réglé sur l'intervalle de temps indiqué dans le rapport.

Dans la section suivante, nous examinerons certaines des manières dont vous pouvez étudier les appareils présentant une activité inhabituelle.

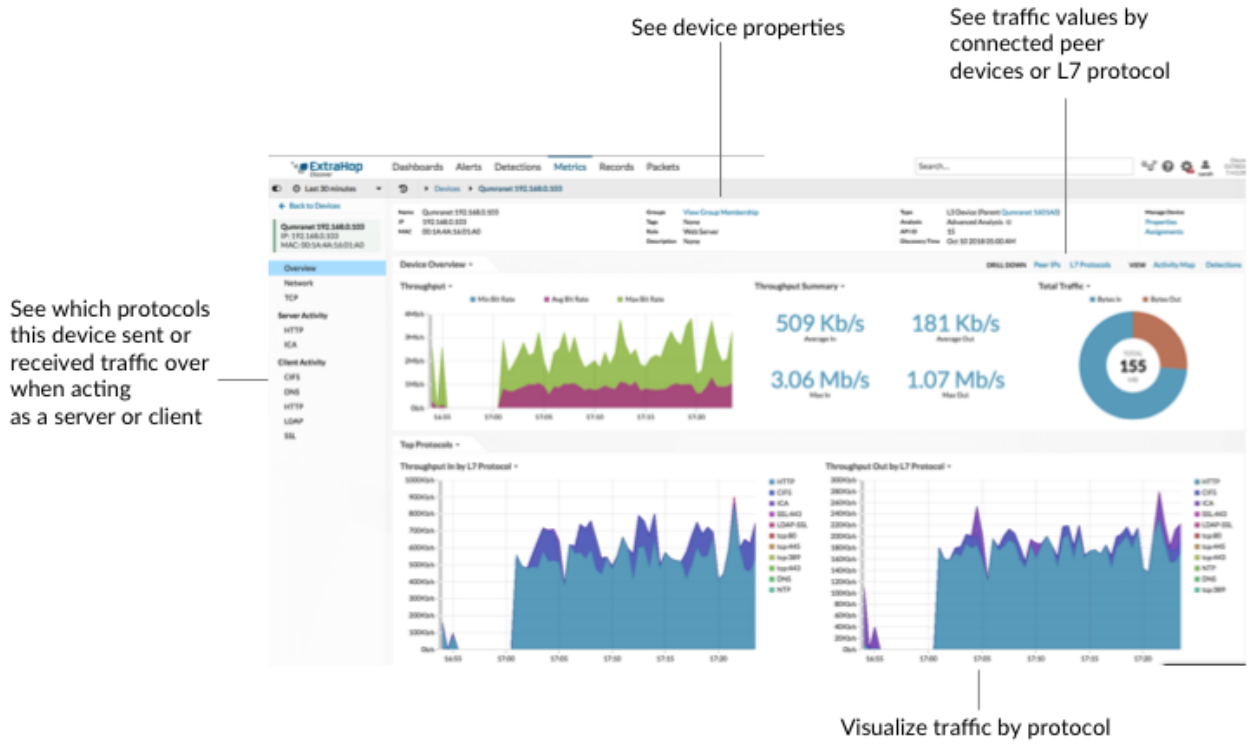
Prochaines étapes : étudier un nouvel équipement

Si vous constatez qu'un nouvel équipement envoie un volume important de trafic sur votre réseau, vous pouvez consulter une page de protocole pour savoir ce que fait l'équipement.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Cliquez sur le **Nouveaux appareils** tableau de bord dans le volet gauche, puis cliquez sur le nom de l'équipement, comme illustré dans la figure suivante.



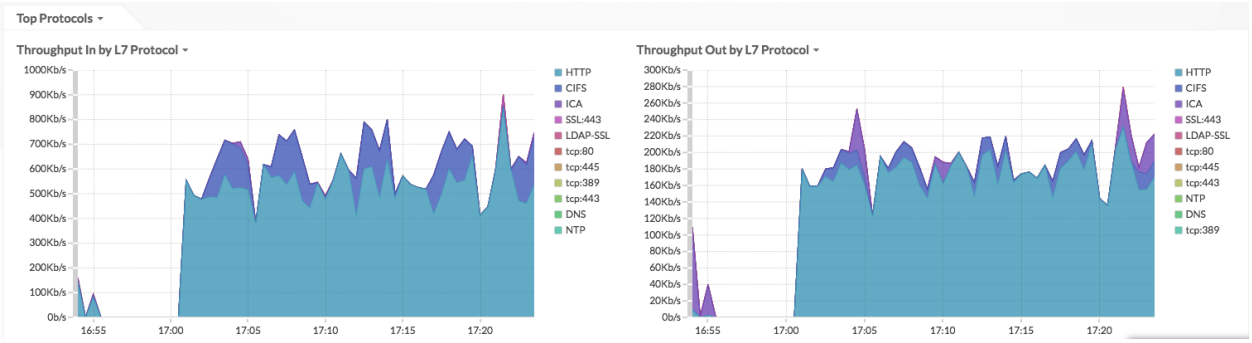
Une page de protocole s'affiche, qui contient les données métriques associées à cet équipement.



Sur la page de protocole, vous pouvez répondre aux questions suivantes.

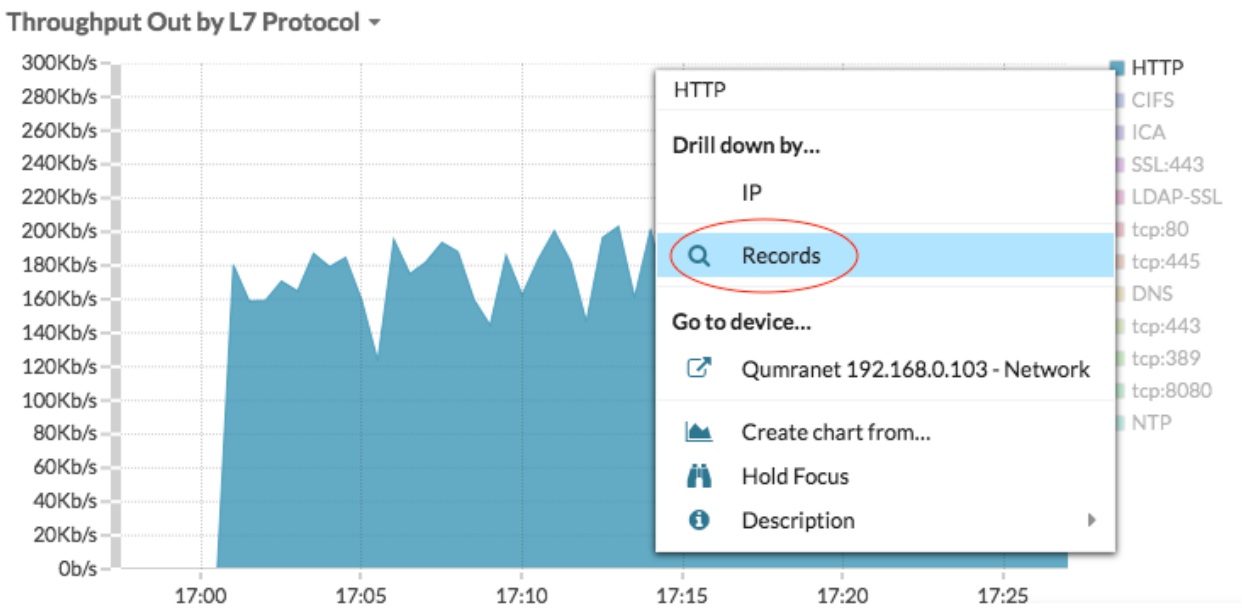
Quel est le principal type d'activité de cet équipement ?

Consultez les graphiques du débit entrant par protocole L7 et du débit sortant par protocole L7. Le volume de trafic est ventilé par protocoles au niveau de l'application (L7). Dans l'exemple ci-dessous, nous pouvons voir que les transactions HTTP constituent le principal type de trafic pour cet équipement.

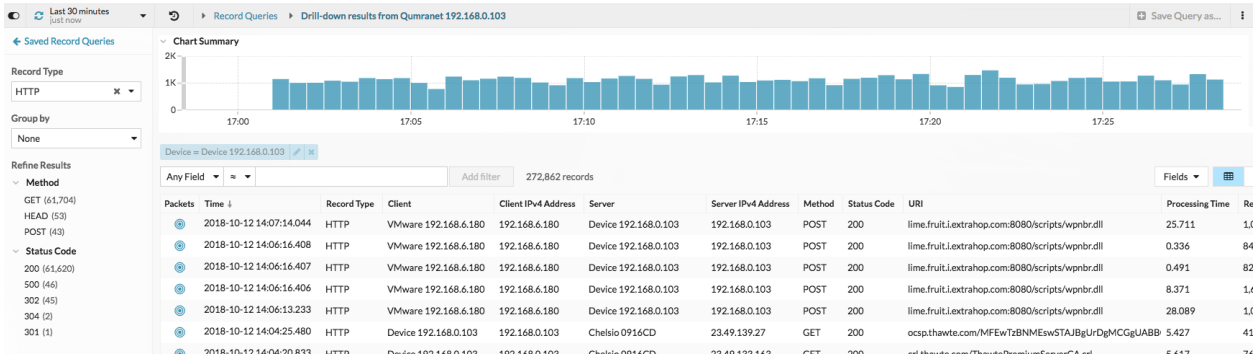


Quelles sont les transactions associées aux volumes élevés de trafic ?

Si vous avez un espace de stockage des enregistrements connecté, cliquez sur une étiquette de protocole dans le graphique, puis sur **Enregistrements**.



Tu peux voir au niveau de la transaction détails.

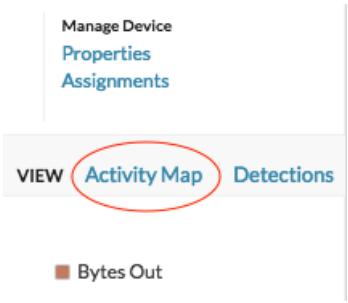


Quels appareils homologues sont connectés à ce nouvel équipement ?

Il existe deux manières de voir quels appareils réseau sont connectés à votre équipement.

- Dans le APPROFONDISSEZ section, cliquez **IP des pairs** pour voir la liste des valeurs de trafic des appareils homologues connectés.

- Dans le VUE section, cliquez **Carte des activités** pour visualiser les connexions avec des appareils homologues en fonction de l'activité du protocole.


Manage Device
Properties
Assignments
VIEW
Activity Map
Detections
Bytes Out