Créez un équipement personnalisé pour surveiller le trafic des bureaux distants

Publié: 2024-04-10

Après avoir déployé le système ExtraHop dans votre centre de données, des informations sur votre réseau apparaissent rapidement. À mesure que le système ExtraHop détecte automatiquement les appareils qui communiquent sur votre réseau, vous pouvez commencer à identifier les goulots d'étranglement du trafic ou à résoudre les problèmes de lenteur des services. Mais comment recueillir des informations sur le trafic important pour les sites distants situés en dehors de votre centre de données ?

Par création d'un équipement personnalisé, vous pouvez facilement découvrir comment les sites distants consomment les services et les applications. Les appareils personnalisés collectent des métriques à partir du trafic réseau en fonction de critères que vous spécifiez, tels qu' un sous-réseau d'adresses IP, une plage de ports ou un réseau local virtuel (VLAN). Avec un équipement personnalisé, vous pouvez surveiller les types de trafic suivants :

- Trafic de sites distants, tels que les succursales, les magasins et les cliniques.
- Trafic de partenaires commerciaux tiers, tels que les processeurs de cartes de crédit et les chronométreurs.
- « Internet », où vous pouvez collecter du trafic à partir d'une gamme d' adresses IP publiques connues, telles que 8.0.0.0/7.

Vous pouvez ajouter un équipement personnalisé à un tableau de bord en tant que source métrique pour surveiller facilement le trafic sur l'équipement. Un équipement personnalisé peut également être sélectionné comme source métrique pour les déclencheurs et les alertes.

Un équipement personnalisé ne compte que comme un seul appareil dans le cadre de votre limite d'équipements sous licence, ce qui est utile pour réduire le nombre d'appareils. Mais il est important de noter que les appareils personnalisés affectent les performances du système s'ils ne sont pas correctement configurés.

Cette procédure pas à pas vous explique comment créer un équipement personnalisé et surveiller le trafic des bureaux distants en suivant les étapes suivantes :

- Créez un équipement personnalisé pour un sous-réseau d'appareils de succursales.
- Créez un tableau de bord pour surveiller la bande passante et la latence du trafic des succursales.

Prérequis

Vous devez disposer d'un compte utilisateur doté de droits d'écriture complets ou d'un système complet.

Voici quelques directives relatives à la configuration d'appareils personnalisés :

- Évitez de créer plusieurs appareils personnalisés pour les mêmes adresses IP ou ports. Le chevauchement d'appareils personnalisés peut affecter les performances du système.
- Lorsque vous configurez un équipement personnalisé à partir d'un console, vous devez spécifier une sonde. L'équipement personnalisé n'est disponible que pour la sonde spécifiée.

Création d'un équipement personnalisé

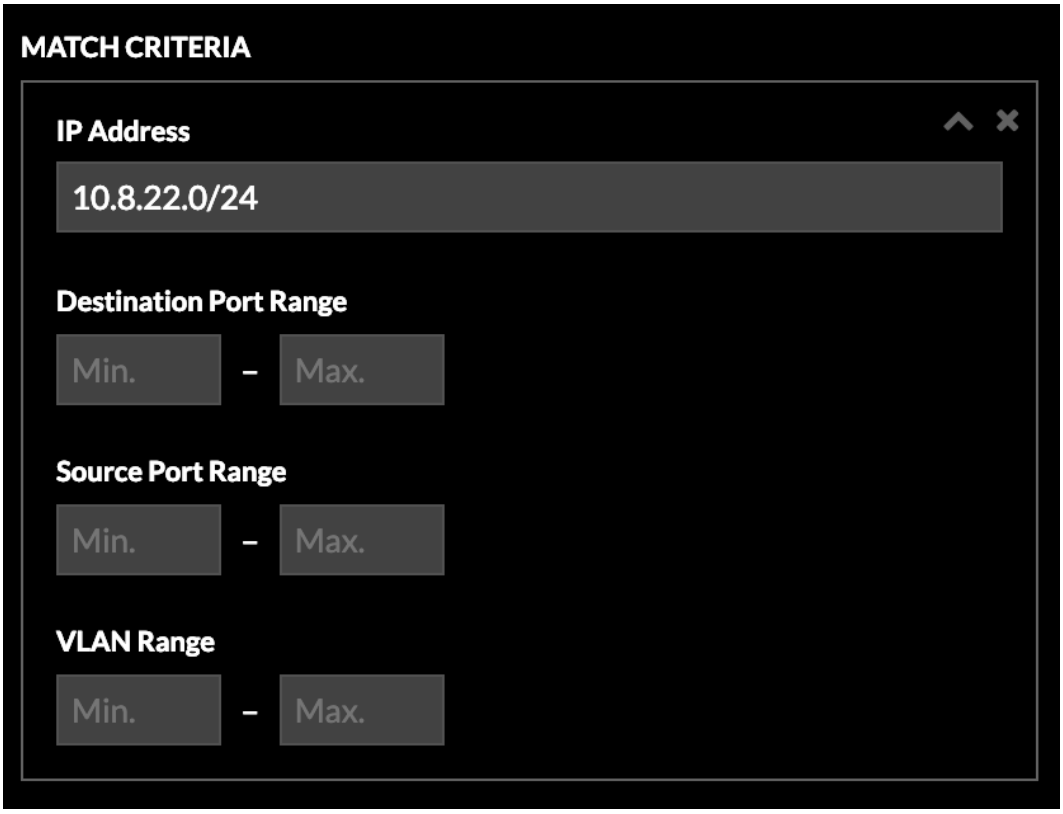
Commençons par créer un équipement personnalisé pour notre succursale de Seattle.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système dans le coin supérieur droit de la page, puis cliquez sur **Appareils personnalisés**.

3. En haut de la page, cliquez sur **Créez**.
4. Dans le **Nom** dans ce champ, saisissez le nom de votre équipement. Par exemple, nommez votre équipement avec la région de la succursale. Dans cet exemple, vous allez nommer l'équipement `Seattle`.
5. Dans le **Identifiant Discovery** dans ce champ, saisissez un identifiant unique pour l'équipement, tel qu'un numéro de magasin ou de bureau. Dans cet exemple, vous allez taper `Store_09045` pour le Discovery ID.

Conseil: Si ce champ est laissé vide, le Discovery ID est généré à partir du nom de l' équipement personnalisé. Le Discovery ID ne peut pas contenir d'espaces et ne peut pas être modifié une fois l'équipement personnalisé enregistré.

6. Dans le **Descriptif** champ, saisissez des informations qui aideront à identifier ce réseau distant lors de recherches futures. Par exemple, saisissez l'adresse de la succursale afin de pouvoir rechercher cet équipement personnalisé par ville ou code postal.
7. (Console uniquement) À partir du **capteur** dans la liste déroulante, sélectionnez la sonde que vous souhaitez associer à l'équipement personnalisé.
8. Cliquez **Ajouter des critères** pour spécifier les adresses IP des appareils pour lesquels vous collecterez des métriques.
9. Dans le **Adresse IP** dans le champ, saisissez une notation CIDR pour le sous-réseau de la succursale de Seattle. Pour cet exemple, vous allez taper `10,8,22,0/24`. Vous pouvez laisser les champs de port et de VLAN vides.



10. Cliquez **Enregistrer**.

Votre équipement personnalisé est créé ! Il faudra quelques minutes à l'équipement personnalisé pour détecter les appareils sur le réseau distant. Au fur et à mesure que le système ExtraHop observe le trafic répondant aux critères de correspondance (par exemple, le sous-réseau 10.8.22.0/24), les métriques seront disponibles pour cet équipement personnalisé.

Ensuite, créons un tableau de bord pour surveiller facilement les indicateurs personnalisés des équipements.

Création d'un tableau de bord

Vous pouvez créer un tableau de bord pour afficher des graphiques et des données spécifiques pour l'équipement personnalisé que vous avez créé.

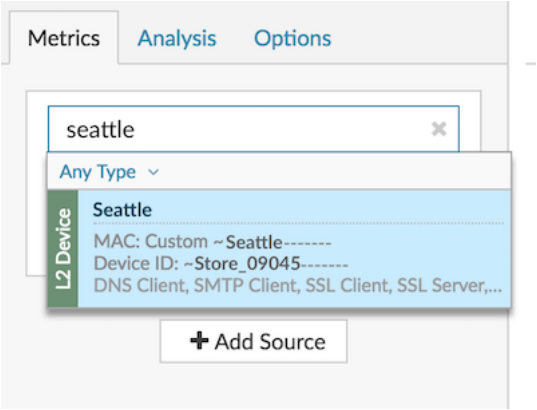
1. En haut de la page, cliquez sur **Tableaux de bord**.
2. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit et sélectionnez **Nouveau tableau de bord** pour créer un tableau de bord vide.
3. Tapez le nom de votre tableau de bord dans **Titre** champ. Pour cette procédure pas à pas, tapez `Trafic des succursales de Seattle`.
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. Les widgets de zone de texte peuvent inclure un texte explicatif personnalisé concernant un tableau de bord ou un graphique. Toutefois, pour cette procédure pas à pas, vous n'ajouterez pas de texte. 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 cliquez sur **Supprimer**.
   b) Cliquez **Supprimer le widget**.

Vous allez ensuite ajouter des mesures de débit relatives aux volumes de trafic au graphique vide.

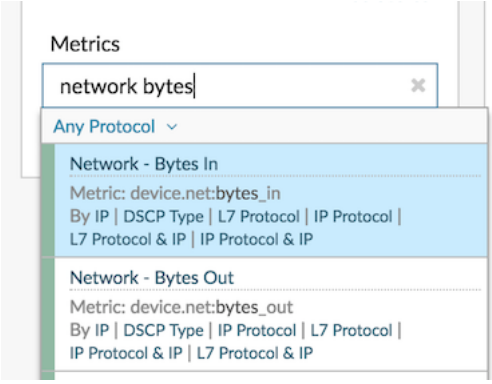
Ajoutez le débit du réseau à votre tableau de bord

Surveillons le nombre d'octets du réseau entrant et sortant du réseau distant.

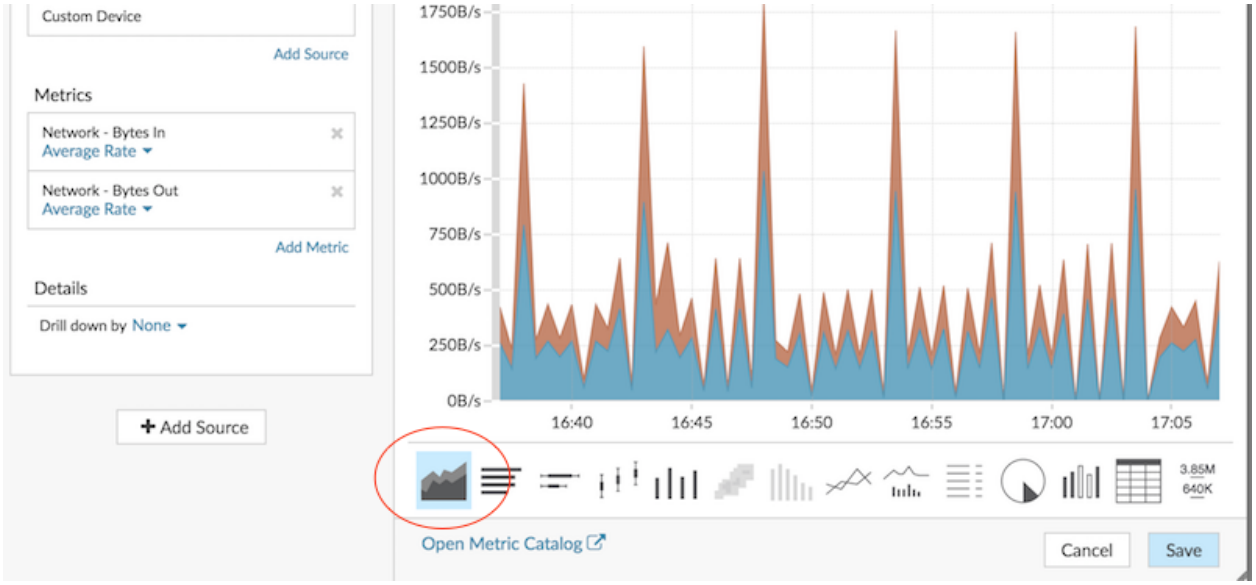
1. Cliquez sur le widget graphique vide dans le tableau de bord que vous venez de créer pour ouvrir l' explorateur de métriques.
2. Cliquez **Ajouter une source**.
3. Dans le Les sources champ, type `Seattle`, puis sélectionnez cet équipement personnalisé dans les résultats, comme indiqué dans l' exemple suivant.



4. Dans le Métriques champ, type `octets du réseau`, puis sélectionnez **Réseau - Octets entrants** à partir des résultats, comme indiqué dans l'exemple suivant.



5. Cliquez **Ajouter une métrique**, tapez `octets du réseau`, puis sélectionnez **Réseau - Octets sortants** à partir des résultats.
6. Cliquez sur **Région** graphique.



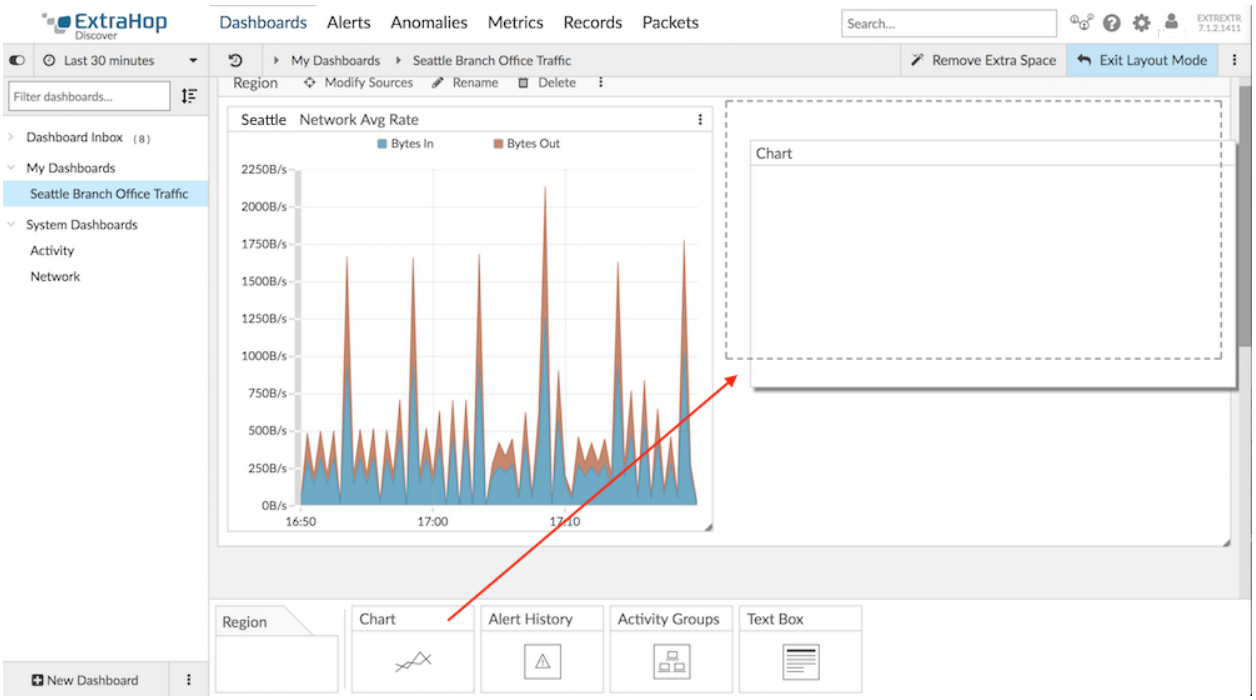
7. Cliquez **Enregistrer**.

Vous allez ensuite ajouter la métrique du temps d'aller-retour pour surveiller la latence du réseau.

Ajoutez la latence du réseau à votre graphique

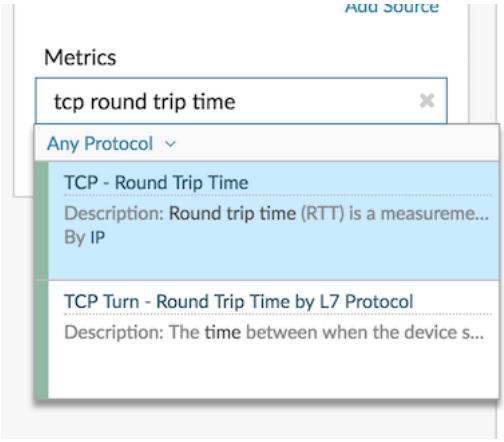
Voyons maintenant si la latence du réseau affecte le réseau distant.

1. Au bas de la page Tableaux de bord, cliquez et faites glisser un widget graphique dans l'espace vide à côté du premier graphique, comme illustré dans l'exemple suivant.

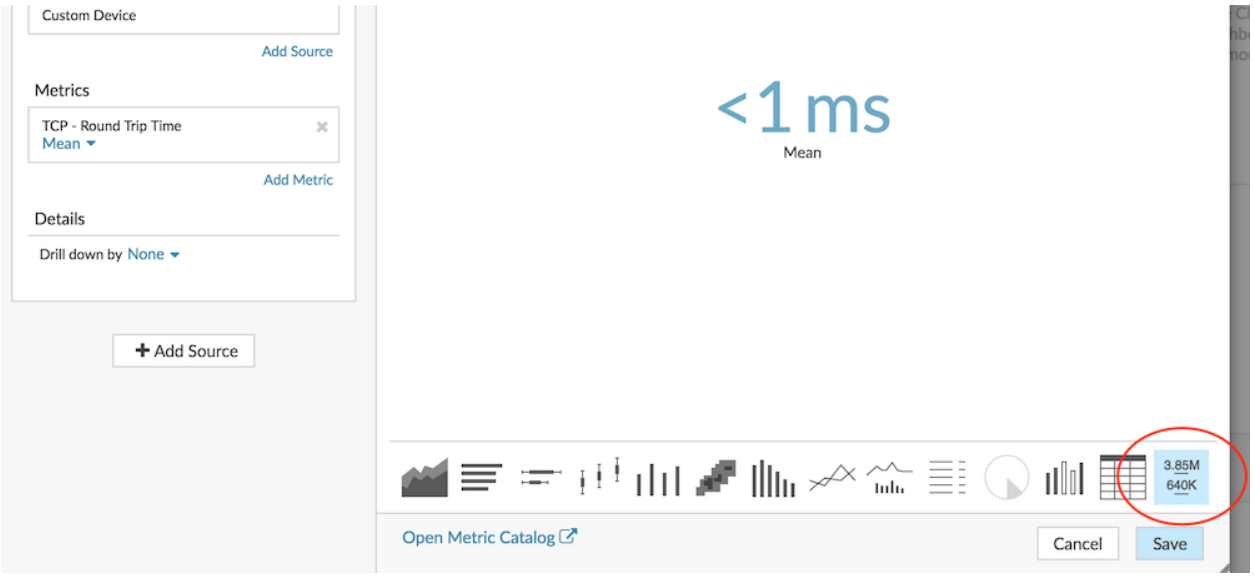


2. Cliquez sur le graphique vide.
3. Cliquez **Ajouter une source**, tapez `Seattle`, puis sélectionnez **Seattle** à partir des résultats.

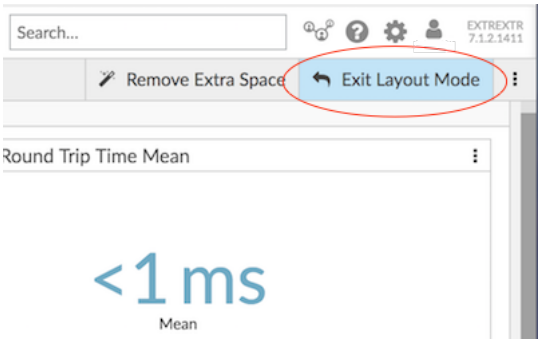
4. Dans le Métriques champ, type `temps d'aller-retour TCP`, puis sélectionnez **TCP - Durée du trajet aller-retour** à partir des résultats, comme indiqué dans l'exemple suivant.



5. Cliquez sur le **Valeur** graphique.



6. Cliquez **Enregistrer**.
7. Dans le coin supérieur droit de la page, cliquez sur **Quitter le mode Layout**.



Votre tableau de bord est terminé ! Vous pouvez désormais surveiller les performances du réseau en effectuant les tâches suivantes :

- Partager un tableau de bord
- Ajouter une ligne de base dynamique à un graphique

Résoudre les problèmes

Vous avez maintenant quelques graphiques à consulter lorsque des performances réseau lentes sont signalées. Le tableau suivant contient des suggestions pour interpréter les données du graphique, puis résoudre les problèmes.

Problème potentiel	Action de suivi
Une augmentation soudaine du trafic	Examinez les données des graphiques du tableau de bord pour comprendre ce qui contribue au trafic. Vous pouvez également examiner les données des pages de protocole. Cliquez sur le titre du graphique , puis sur le nom de l'équipement personnalisé dans Allez à... section. Une page de protocole pour l'équipement personnalisé s'affiche. Création d'une carte dactivitiés pour voir les connexions des équipements et le volume de trafic entre les connexions. Vous pouvez également comparer deux intervalles de temps à partir de différentes heures ouvrables pour voir la différence entre les valeurs métriques.
Application lente	Déterminez si la lenteur de l'application est liée à un problème côté client dans la succursale ou si le problème est lié aux serveurs du centre de données local. Cliquez sur le titre du graphique, puis sur le nom de l'équipement personnalisé dans Allez à... section. Une page de protocole pour l'équipement personnalisé s'affiche. Dans la section Activité du client du volet de gauche, cliquez sur **HTTP**, **Base de données**, **DNS**, ou **ICA** (Citrix) pour étudier les mesures d'erreur côté client. Dans la section Activité du serveur, cliquez sur Protocoles et examinez des indicateurs tels que les erreurs et le temps de traitement du serveur. Ces statistiques indiquent que les serveurs sont peut-être à l'origine du problème.
Augmentation du volume de trafic au fil du temps	Ajouter une ligne de base dynamique à un graphique pour visualiser les tendances des données de trafic au fil du temps. Notez que le système ExtraHop commence à créer une ligne de base dynamique après son ajout au graphique. Vous ne pouvez pas consulter une base de données historiques.
Augmentation de la congestion du réseau ou autres problèmes de transmission de données	Examinez les métriques TCP pour voir comment le réseau affecte les performances des applications.

Problème potentiel	Action de suivi
	Cliquez sur le titre du graphique, puis sur l'équipement personnalisé dans Allez à... section du menu déroulant. Une page de protocole pour l'équipement personnalisé s'affiche. Recherchez des valeurs élevées pour les mesures suivantes : • Délais de retransmission (entrée/sortie RTOS) en cas de congestion du réseau • Temps d'aller-retour (RTT) pour la latence du réseau • Recevez Window Throttling et Zero Windows pour les problèmes de transmission de données