Percer vers le bas

Publié: 2024-04-10

Une métrique intéressante soulève naturellement des questions sur les facteurs associés à cette valeur métrique. Par exemple, si vous constatez un grand nombre de délais d'expiration des requêtes DNS sur votre réseau, vous vous demandez peut-être quels clients DNS rencontrent ces délais. Dans le système ExtraHop, vous pouvez facilement effectuer une recherche vers le bas à partir d'une métrique de niveau supérieur pour afficher les appareils, les méthodes ou les ressources associés à cette métrique.

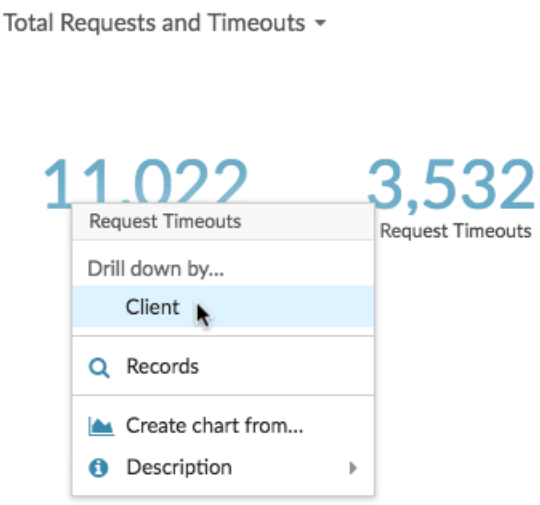
Lorsque vous parcourez une métrique à l'aide d'une clé (telle qu'une adresse IP client, une méthode, un URI ou une ressource), le système ExtraHop calcule un topnset d'un maximum de 1 000 paires clé-valeur. Vous pouvez ensuite étudier ces paires clé-valeur, appelées mesures détaillées, pour savoir quels facteurs sont liés à l'activité intéressante.

Exploration vers le bas à partir d'un tableau de bord ou d'une page de protocole

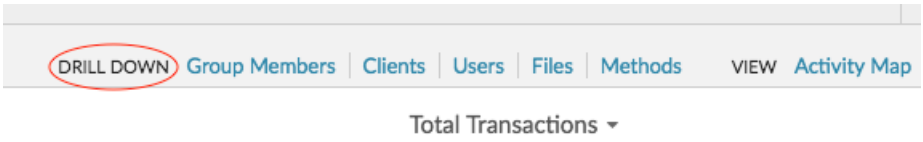
En cliquant sur une métrique dans un graphique ou une légende, vous pouvez voir quelle clé, telle que l' adresse IP du client, l'adresse IP du serveur, la méthode ou la ressource, a contribué à cette valeur.

Les étapes suivantes vous montrent comment localiser une métrique, puis comment effectuer une hiérarchisation vers le bas :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Trouvez une métrique intéressante en effectuant l'une des étapes suivantes :
   - Cliquez **Tableau de bord**, puis sélectionnez un tableau de bord dans le volet de gauche. Un tableau de bord contenant des métriques apparaît.
   - Cliquez **Actifs**, cliquez **Appareil**, **Groupe d'appareils**, ou **Demande** dans le volet de gauche. Sélectionnez ensuite un équipement, un groupe ou une application. Une page de protocole contenant des métriques apparaît.
   - Cliquez **Actifs**, cliquez **Réseaux** dans le volet gauche, puis sélectionnez un réseau de flux. Une page de protocole contenant des métriques apparaît.
3. Cliquez sur une valeur métrique ou sur une étiquette métrique dans la légende du graphique, comme illustré dans la figure suivante. Un menu apparaît.



Conseil: Sur une page de protocole, vous pouvez également cliquer sur un bouton de raccourci déroulant dans le Exploration vers le bas section, située dans le coin supérieur droit de la page. Le type de boutons de raccourci varie en fonction du protocole.



4. Dans le Profilez vers le bas par... section, sélectionnez une clé. Une page de statistiques détaillées avec un topnset des valeurs métriques par clé s'affiche. Vous pouvez consulter jusqu'à 1 000 paires clé-valeur sur cette page.

   Conseil: Si disponible, cliquez sur **Afficher plus** lien au bas d'un graphique pour accéder à la métrique affichée dans le graphique.

Prochaines étapes

- Étudiez les indicateurs de détail

Approfondissez la capture du réseau et les métriques VLAN

Cliquez sur une métrique de niveau supérieur intéressante concernant l'activité du réseau sur un Réseau capture ou VLAN page permettant d'identifier les appareils liés à cette activité.

Note: Pour plus d'informations sur la manière d'explorer les métriques à partir d'un réseau de flux ou d'une page d'interface de réseau de flux, consultez le Exploration vers le bas à partir d'un tableau de bord ou d'une page de protocole section.

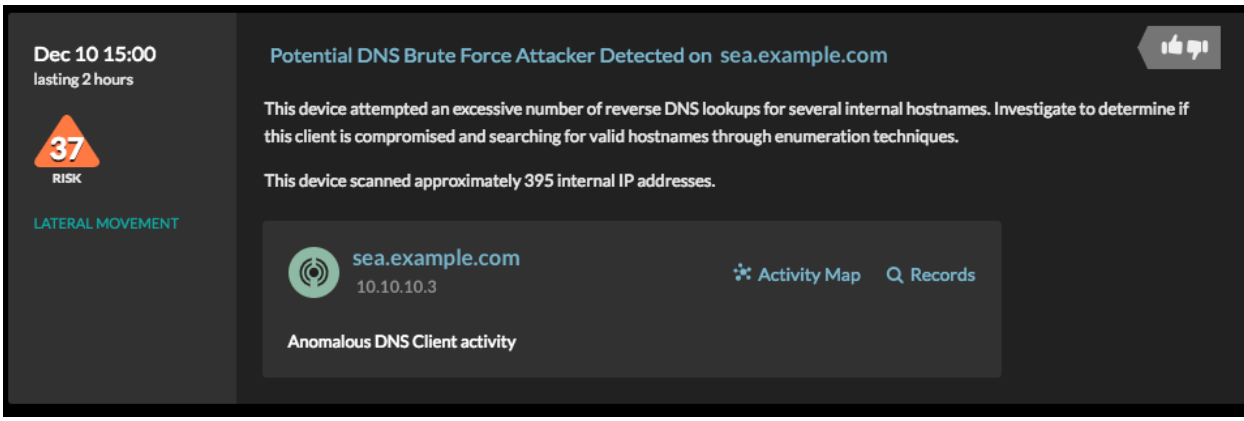
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs**.
3. Cliquez **Réseaux** dans le volet de gauche.
4. Cliquez sur le nom d'une capture réseau ou d'une interface VLAN.
5. Cliquez sur une couche réseau dans le volet de gauche, telle que **L3** ou **Protocoles L7**. Les graphiques qui affichent les valeurs métriques pour l'intervalle de temps sélectionné apparaissent. Pour la plupart des protocoles et mesures, un Appareil le tableau apparaît également au bas de la page.
6. Cliquez sur les données du graphique pour mettre à jour la liste afin d'afficher uniquement les appareils associés aux données.
7. Cliquez sur le nom d'un équipement. UN Appareil une page apparaît, qui affiche le trafic et l'activité du protocole associés à l'équipement sélectionné.

Exploration vers le bas à partir d'une détection

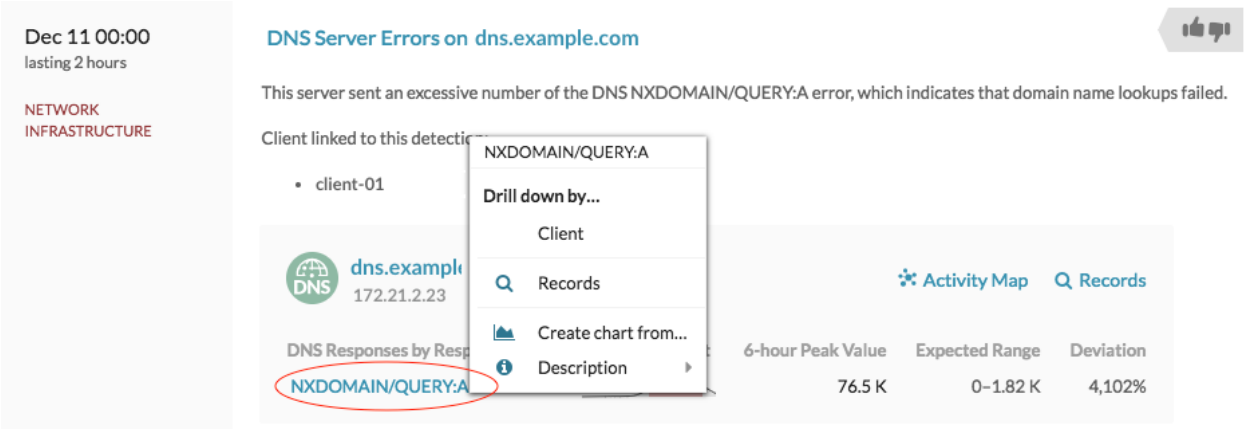
Pour certaines détections, vous pouvez effectuer une analyse détaillée de la métrique ou de la clé à l'origine du comportement inhabituel. Le nom ou la clé métrique apparaît sous forme de lien au bas d'une détection individuelle.

Note: Les détections comportant des mesures ou des clés ne comportant pas de mesures détaillées n'incluent pas d'option d'exploration vers le bas. Les détections qui n'affichent qu'une activité anormale du protocole au lieu d'une métrique n'incluent pas non plus d'option d'exploration des métriques. Par exemple, vous ne pouvez pas effectuer une analyse détaillée d'une détection d'activité anormale d'un client DNS, comme le montre la figure ci-dessous. Cliquez plutôt sur les liens correspondant au nom de l'équipement ou de

l'application, **Carte des activités**, ou **Enregistrements** pour en savoir plus sur cette activité anormale.



1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Détections** en haut de page.
3. Trouvez une détection intéressante associée à une métrique et cliquez sur le nom ou la clé de la métrique. Dans la figure suivante, en cliquant sur le code de réponse, nous pouvons afficher tous les clients qui ont reçu des réponses DNS avec NXDOMAIN/QUERY:A.



4. Dans le Profilez vers le bas par... section, cliquez sur une touche telle que **Cliente**.
Une page métrique détaillée apparaît, dans laquelle vous pouvez étudier les métriques répertoriées par clé.

Analyse détaillée à partir d'une alerte

Cliquez sur le nom de la métrique ou sur la clé dans une alerte de seuil pour voir quelle clé, telle que le client, le serveur, la méthode ou la ressource, a contribué à la valeur de la métrique ou à un comportement inhabituel.

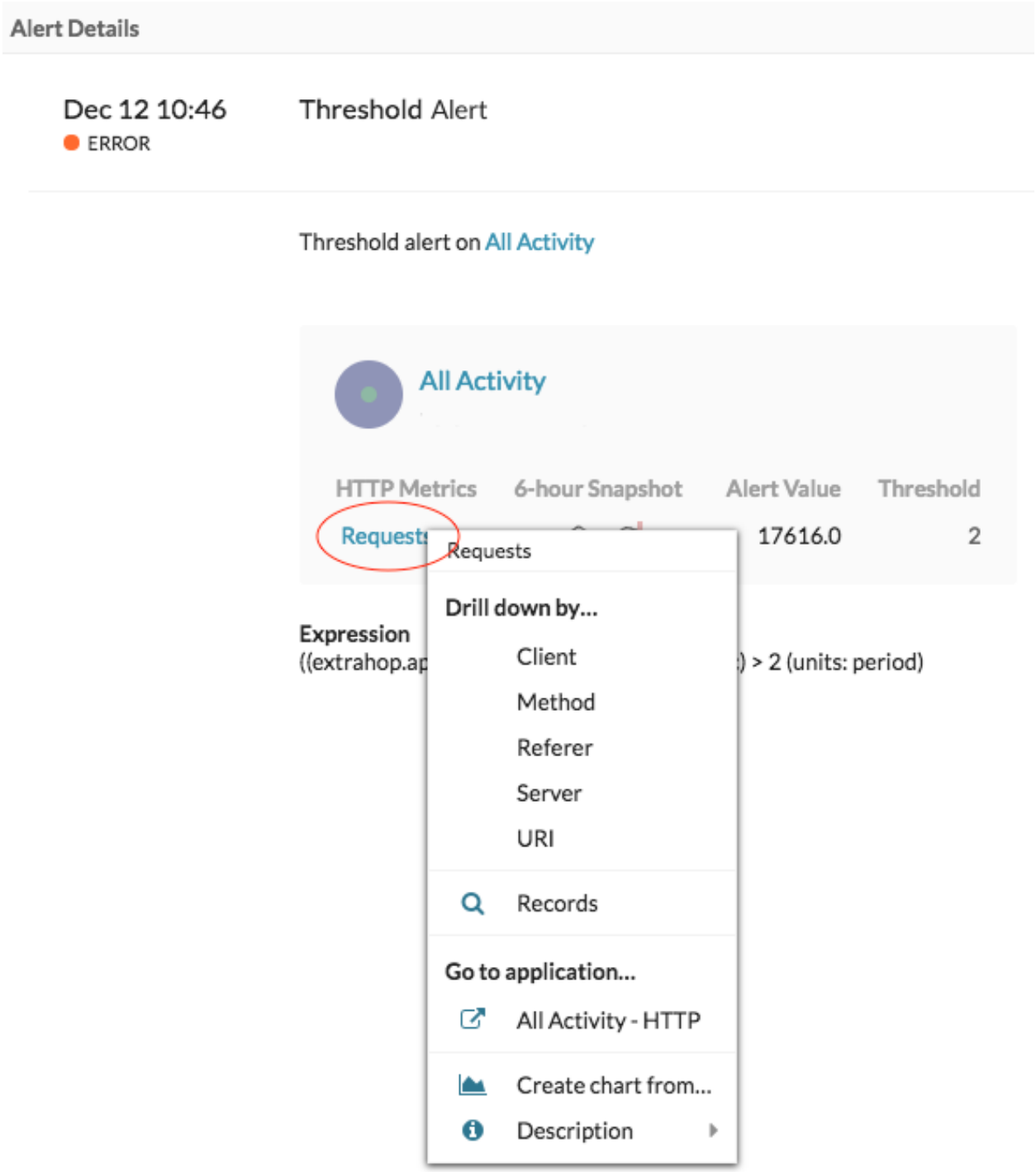
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Alertes** en haut de page.

Note: Vous pouvez également accéder aux alertes à partir d'un widget d'alerte sur un tableau de bord ou au bas des pages de protocole suivantes :

- Page de présentation de l'application

- Page de présentation des groupes d'appareils
- Page de présentation du réseau

3. Cliquez sur le nom d'une alerte de seuil.
   Les détails de l'alerte apparaissent.
4. Cliquez sur le nom ou la clé d'une métrique, comme illustré dans la figure suivante.



5. Dans le Profiler vers le bas par section, cliquez sur une touche, telle que **Cliente**, **Méthode**, **Référent**, **serveur**, ou **URI**.

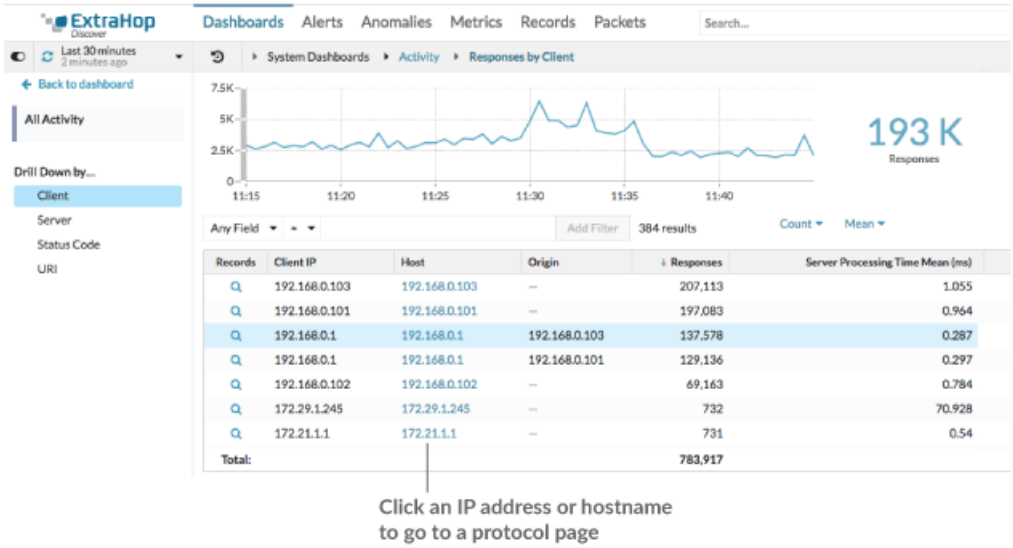
Une page métrique détaillée apparaît, dans laquelle vous pouvez étudier les métriques répertoriées par clé.

Étudiez les indicateurs de détail

Après avoir exploré une métrique depuis un tableau de bord, une page de protocole, une détection ou une alerte, vous pouvez examiner les valeurs métriques par clé sur une page de métrique détaillée. Filtrez les données métriques ou sélectionnez différentes clés, telles que des codes d'état ou des URI, pour afficher les données sous différents angles.

La figure suivante montre comment filtrer, faire pivoter, trier ou exporter des données sur une page métrique détaillée.

Si vous avez effectué une recherche approfondie sur une métrique par IP, client ou serveur, les adresses IP et les noms d'hôtes (s'ils sont observés à partir du trafic DNS) apparaissent dans le tableau. Des options supplémentaires s'offrent désormais à vous. Par exemple, vous pouvez accéder directement à la page de protocole d'un client ou d'un serveur, comme illustré dans la figure suivante.



Filtrer les résultats

Une page détaillée peut contenir jusqu'à 1 000 paires clé-valeur. Il existe deux manières de rechercher des résultats spécifiques à partir de données : filtrer les résultats ou cliquez sur une touche du tableau pour créer un autre filtre d'exploration.

Pour filtrer les résultats, cliquez sur **N'importe quel domaine**, puis sélectionnez un champ qui varie en fonction de la touche. Par exemple, vous pouvez sélectionner **Localité du réseau** pour les clés client ou serveur. Sélectionnez ensuite l'un des opérateurs suivants :

- Sélectionnez **=** pour effectuer une correspondance de chaîne exacte.
- Sélectionnez **≈** pour effectuer une correspondance de chaînes approximative. L' opérateur ≈ prend en charge les expressions régulières.

  Note: Pour exclure un résultat, entrez une expression régulière. Pour plus d'informations, voir Création de filtres d'expressions régulières.
- Sélectionnez **#** pour exclure une correspondance de chaîne approximative de vos résultats.
- Sélectionnez **>** ou **≥** pour effectuer une correspondance pour des valeurs supérieures (ou égales à) une valeur spécifiée.
- Sélectionnez **<** ou **≤** pour effectuer une correspondance pour des valeurs inférieures (ou égales) à une valeur spécifiée.
- Cliquez **Ajouter un filtre** pour enregistrer les paramètres du filtre. Vous pouvez enregistrer plusieurs filtres pour une seule requête. Les filtres enregistrés sont effacés si vous sélectionnez une autre clé dans la section Détails du volet de gauche.

Pour terminer le filtre, entrez ou sélectionnez la valeur selon laquelle vous souhaitez filtrer les résultats, puis cliquez sur **Ajouter un filtre**.

Étudier les données relatives aux renseignements sur les menaces (ExtraHop Reveal (x) Premium et Ultra uniquement)

Cliquez sur l'icône rouge de la caméra pour visionner renseignements sur les menaces des informations sur un hôte, une adresse IP ou un URI suspect trouvées dans des données métriques détaillées.

Mettez en surbrillance une valeur métrique dans le graphique supérieur

Sélectionnez une ligne individuelle ou plusieurs lignes pour modifier les données du graphique dans le graphique supérieur de la page des mesures métriques détaillées. Passez la souris sur les points de données du graphique pour afficher plus d'informations sur chaque point de données.

Passez à un plus grand nombre de données par clé

Cliquez sur le nom des touches dans Détails section pour voir des valeurs métriques plus détaillées, ventilées par d'autres clés. Pour l'adresse IP ou les clés d'hôte, cliquez sur le nom d'un équipement dans le tableau pour accéder à Appareil page de protocole, qui affiche le trafic et l'activité protocolaire associés à cet équipement.

Ajustez l'intervalle de temps et comparez les données de deux intervalles de temps

En modifiant l'intervalle de temps, vous pouvez consulter et comparer les données métriques de différentes périodes dans le même tableau. Pour plus d'informations, voir Comparez les intervalles de temps pour trouver le delta métrique.

Note: L'intervalle de temps global situé dans le coin supérieur gauche de la page comprend une icône d'actualisation bleue et un texte gris qui indique la date à laquelle les mesures d'exploration vers le bas ont été interrogées pour la dernière fois. Pour recharger les mesures pour l'intervalle de temps spécifié, cliquez sur l'icône d'actualisation dans l'affichage du sélecteur de temps global. Pour plus d'informations, voir Afficher les dernières données pour un intervalle de temps.

Trier les données métriques en colonnes

Cliquez sur l'en-tête de colonne pour effectuer un tri par métrique afin de voir quelles clés sont associées aux valeurs métriques les plus grandes ou les plus petites. Par exemple, triez en fonction du temps de traitement pour voir quels clients ont connu les temps de chargement de leur site Web les plus longs.

Calcul des données de modification pour les métriques

Modifiez les calculs suivants pour les valeurs métriques affichées dans le tableau :

- Si vous avez une métrique de comptage dans le tableau, cliquez sur **Compter** dans le Options section dans le volet de gauche, puis sélectionnez **Taux moyen**. Pour en savoir plus, consultez le Afficher un taux ou un nombre dans un graphique sujet.
- Si le tableau contient une métrique de jeu de données, cliquez sur **Moyenne** dans le Options section dans le volet de gauche, puis sélectionnez **Résumé**. Lorsque vous sélectionnez **Résumé**, vous pouvez consulter la moyenne et l'écart type.

Exporter des données

Cliquez avec le bouton droit sur une valeur métrique dans le tableau pour télécharger un fichier PDF, CSV ou Excel.

Profilez une seconde fois vers le bas à l'aide d'un filtre clé

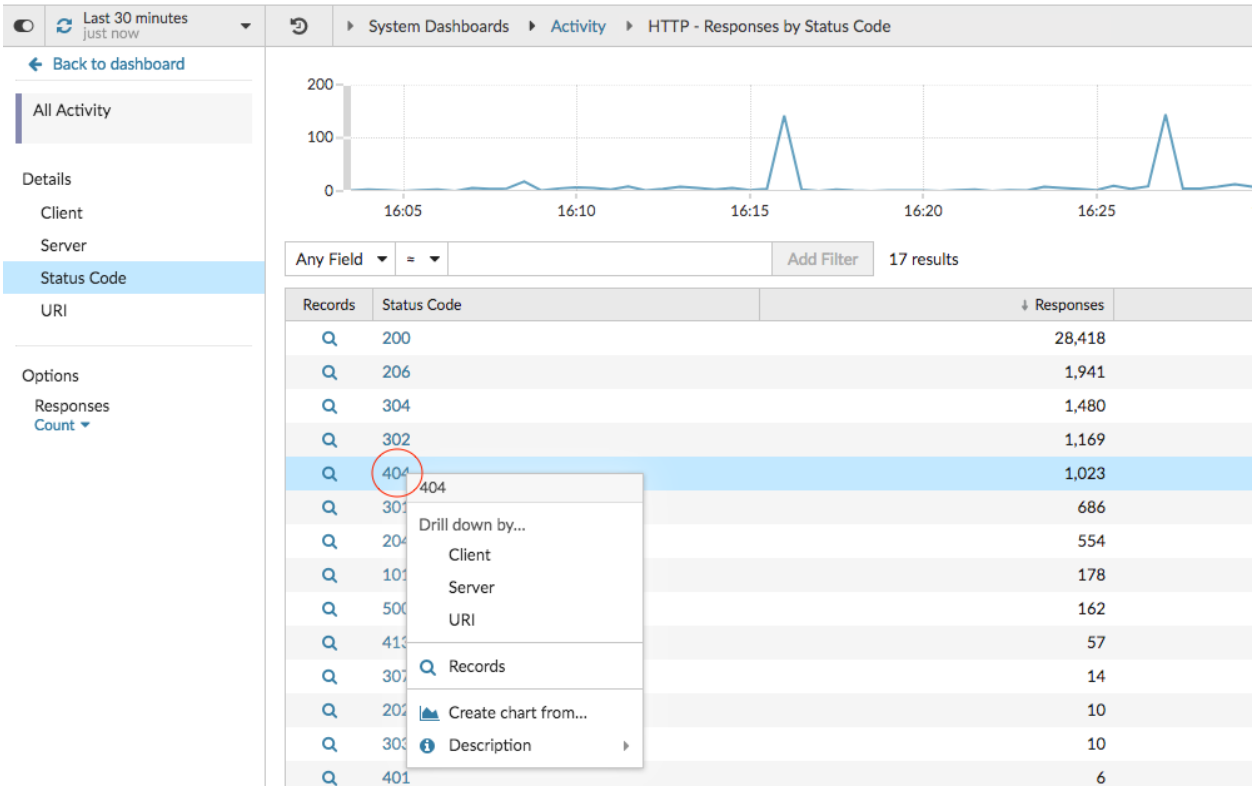
Après avoir exploré une métrique de niveau supérieur par touche pour la première fois, une page détaillée apparaît avec un topnset de valeurs métriques ventilées par cette clé. Vous pouvez ensuite créer un filtre pour effectuer une seconde exploration vers le bas à l'aide d'une autre touche. Par exemple, vous pouvez parcourir les réponses HTTP par code d'état, puis effectuer une nouvelle exploration vers le bas en fonction du code d'état 404 pour trouver plus d'informations sur les serveurs, les URI ou les clients associés à ce code d'état.

Note: L'option d'exploration vers le bas une deuxième fois n'est disponible que pour certains topnsets.

Les étapes suivantes vous montrent comment effectuer une hiérarchisation descendante à partir d'un graphique, puis une nouvelle exploration vers le bas à partir d'une page métrique détaillée :

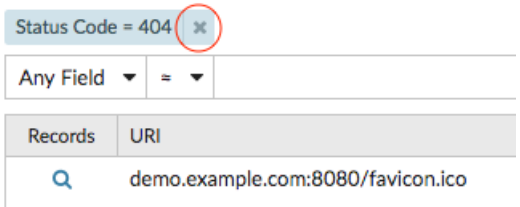
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Accédez à un tableau de bord ou à une page de protocole.
3. Cliquez sur une valeur métrique ou une étiquette.
4. Dans le Profilez vers le bas par... section, sélectionnez une clé.
   Une page détaillée s'affiche.
5. Cliquez sur une clé du tableau, telle qu'un code d'état ou une méthode. (La clé ne doit pas être une adresse IP ou un nom d'hôte.)

6. Dans le Profilez vers le bas par... section, sélectionnez une clé, comme indiqué dans la figure suivante.

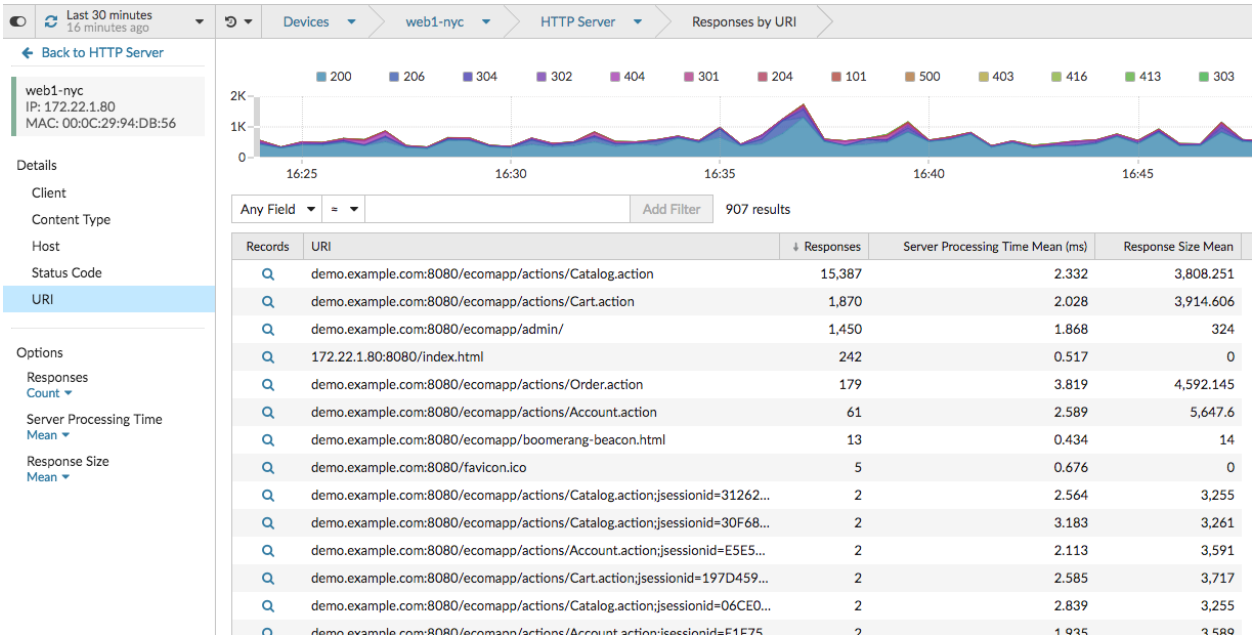


Le filtre principal apparaît au-dessus du tableau. Vous pouvez désormais consulter toutes les mesures détaillées associées à cette clé unique.

7. Pour supprimer ce filtre du tableau, puis l'appliquer au graphique supérieur, cliquez sur le **x** icône, comme illustré dans la figure suivante.



Le filtre du graphique persiste lorsque vous sélectionnez d'autres clés dans la section Détails.



Ajouter des mesures détaillées à un graphique

Si vous souhaitez surveiller rapidement un ensemble de mesures détaillées dans un tableau de bord, sans effectuer à plusieurs reprises les mêmes étapes de hiérarchisation, vous pouvez effectuer une analyse détaillée sur une métrique lorsque vous modifiez un graphique dans explorateur de métriques. La plupart des graphiques peuvent afficher jusqu'à 20 des valeurs métriques les plus détaillées, ventilées par clé. Une clé peut être l'adresse IP d'un client, un nom d'hôte, une méthode, un URI, un référent, etc. Les widgets de tableau et de liste peuvent afficher jusqu' à 200 valeurs métriques détaillées les plus élevées.

Par exemple, un tableau de bord destiné à surveiller le trafic Web peut contenir un graphique affichant le nombre total de requêtes et de réponses HTTP. Vous pouvez modifier ce graphique pour effectuer une analyse détaillée de chaque métrique par adresse IP afin de voir les principaux intervenants.

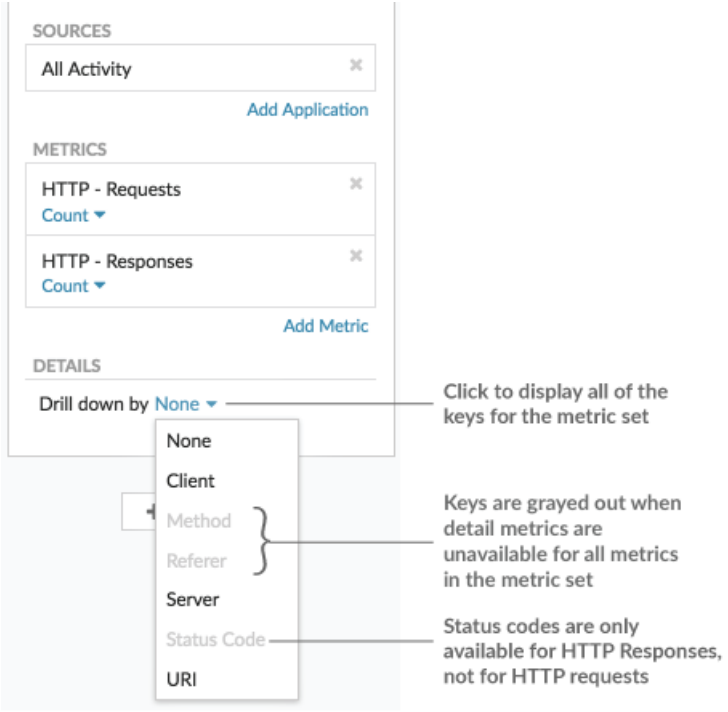
Les étapes suivantes vous montrent comment modifier un graphique existant, puis comment effectuer un défilement vers le bas pour afficher les mesures détaillées :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Accédez à un tableau de bord ou à une page de protocole.
3. Cliquez sur le titre du graphique, puis sélectionnez **Modifier**.
4. Dans le Détails section, cliquez **Profilez vers le bas par *<None>*** , où *<None>* est le nom de la clé métrique détaillée actuellement affichée dans votre graphique.
5. Sélectionnez une clé dans la liste déroulante.

Note: Si vous en avez plusieurs source sélectionnées dans votre ensemble métrique, par exemple deux appareils, les sources sont automatiquement combinées dans un groupe de sources ad hoc au fur et à mesure que vous effectuez une analyse descendante. Vous ne pouvez pas désélectionner le **Combiner les sources** case à cocher. Pour afficher les métriques détaillées pour chaque source, vous devez supprimer une source de l'ensemble de mesures, puis cliquer sur **Ajouter une source** pour créer un nouvel ensemble de mesures.

Si les données métriques détaillées d'une clé commune sont disponibles pour toutes les mesures d'un ensemble de mesures, la clé de la métrique détaillée apparaît automatiquement dans la liste déroulante, comme illustré dans la figure suivante. Si une clé de la liste est grisée, la métrique détaillée associée à cette clé n'est pas disponible pour toutes les métriques de cet ensemble de mesures ci-dessus. Par

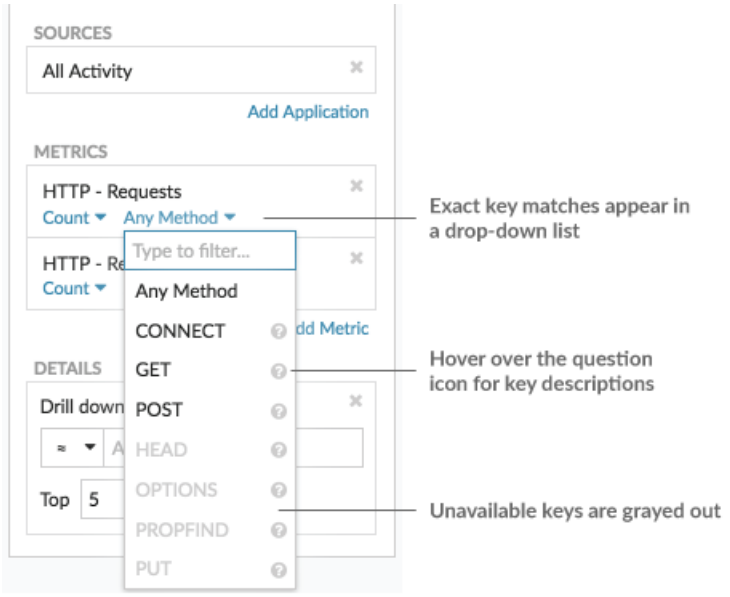
exemple, les données du client, du serveur et de l'URI sont disponibles pour les métriques de requêtes HTTP et de réponses HTTP dans l' ensemble de métriques.



6. Vous pouvez filtrer les clés avec une correspondance approximative, expression régulière (regex), ou une correspondance exacte en suivant l'une des étapes suivantes :
   - Dans le Filtre champ, sélectionnez le **≈** opérateur pour afficher les touches selon une correspondance approximative ou avec une expression régulière. Vous devez omettre les barres obliques avec regex dans le filtre de correspondance approximative.

     Note: Le **#** l'option de filtrage pour exclure les résultats n'est disponible que sur pages de détails. Si vous souhaitez exclure les résultats d'un graphique de tableau de bord, créez un expression régulière (regex).
   - Dans le Filtre champ, sélectionnez le **=** opérateur pour afficher les touches selon une correspondance exacte.
7. Optionnel : Dans le champ des meilleurs résultats, entrez le nombre de clés que vous souhaitez afficher. Ces clés auront les valeurs les plus élevées.
8. Pour supprimer une sélection déroulante, cliquez sur **x** icône.

   Note: Vous pouvez afficher une correspondance clé exacte par métrique, comme illustré dans la figure suivante. Cliquez sur le nom de la métrique détaillée (tel que **Toutes les méthodes**) pour sélectionner une clé métrique détaillée spécifique (telle que `GET`) dans la liste déroulante. Si une touche apparaît en gris (telle que `PROPFIND`), les données métriques détaillées ne sont pas disponibles pour cette clé spécifique. Vous pouvez également saisir une clé qui ne figure pas dans la liste déroulante.


SOURCES
All Activity
Add Application
METRICS
HTTP - Requests
Count
Any Method
Type to filter...
Any Method
CONNECT
GET
POST
HEAD
OPTIONS
PROPFIND
PUT
Exact key matches appear in a drop-down list
Hover over the question icon for key descriptions
Unavailable keys are grayed out