Explorez les métriques du système ExtraHop pour étudier les défaillances du DNS

Publié: 2024-01-31

Le protocole DNS (système de nom de domaine) est essentiel pour prendre en charge le trafic Internet. Cela fonctionne souvent sans problème. Cependant, les serveurs DNS sont souvent mal configurés ou surchargés dans les environnements informatiques, ce qui peut affecter les performances Internet.

Il existe de nombreuses façons d'explorer les métriques DNS dans le système ExtraHop. Dans cette présentation pas à pas, nous allons vous montrer comment examiner les métriques DNS dans un tableau de bord, accédez aux pages du protocole DNS et explorez les indicateurs intéressants pour identifier les appareils potentiellement affectés.

Plus précisément, vous allez apprendre à répondre aux questions suivantes :

- Y a-t-il un problème de réseau ou de DNS qui affecte les performances d'Internet ?
- Quel est le nombre de défaillances DNS sur mon réseau ?
- Quels clients sont concernés par des problèmes de DNS ?

Des ressources supplémentaires sont disponibles pour interpréter le DNS :

- Découvrez comment interpréter les métriques DNS dans le système ExtraHop en consultant notre module de formation en ligne, Aperçu rapide : DNS.
- Découvrez les requêtes DNS problématiques et les erreurs que vous pouvez surveiller dans votre propre environnement en installant Ensemble DNS ExtraHop. Ce bundle contient un tableau de bord avec des graphiques préconfigurés et des explications détaillées sur les principales erreurs DNS.
- Apprenez comment créer un tableau de bord pour surveiller les erreurs DNS.

Prérequis

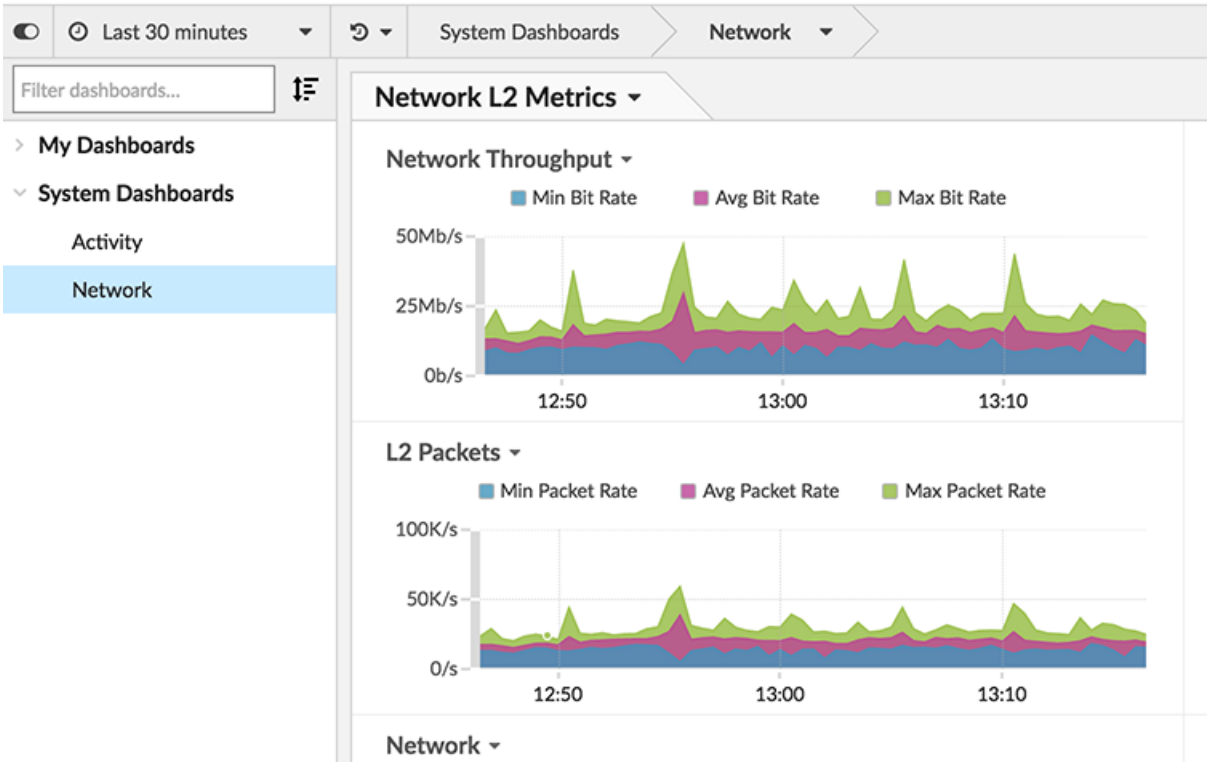
- Familiarisez-vous avec les concepts présentés dans cette procédure pas à pas en lisant le Référence des métriques du protocole et le FAQ sur les métriques.
- Vous devez avoir accès à un système ExtraHop avec du trafic de serveur DNS, ou vous pouvez effectuer cette procédure pas à pas dans Démo ExtraHop.

Identifiez les problèmes liés au DNS avec les tableaux de bord du système

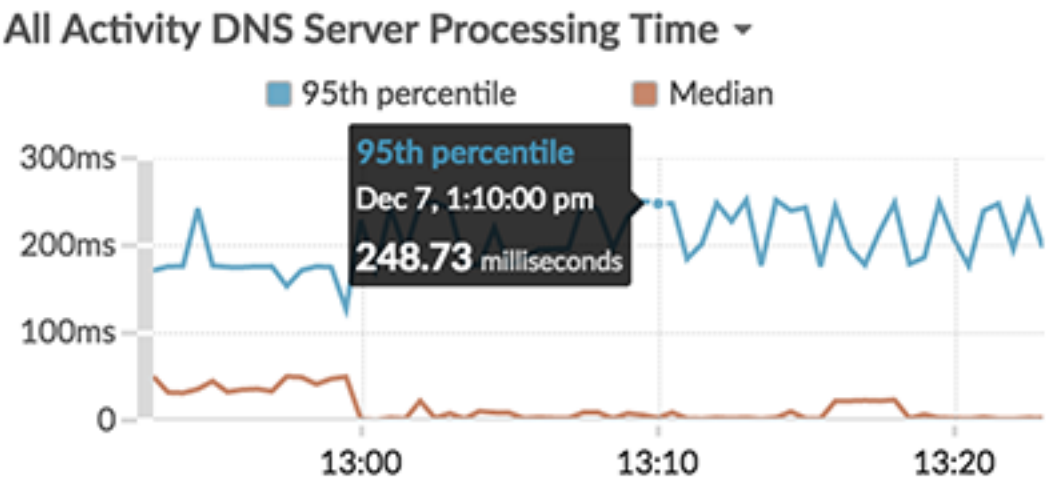
Si un problème de lenteur d'Internet est signalé, examinez les tableaux de bord du système pour déterminer s'il est lié au débit du réseau ou au protocole DNS.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur le sélecteur d'heure global dans la barre de navigation en haut à gauche, puis sélectionnez **Les 7 derniers jours**, puis cliquez sur **Enregistrer**.

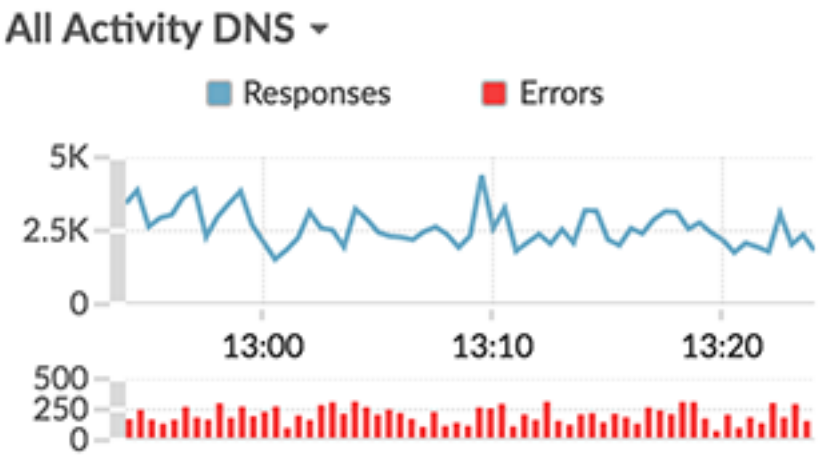
   Note: La modification de l'intervalle de temps global vous permet de voir le comportement du réseau et du protocole qui s'est produit avant la détection du problème.
3. Cliquez **Tableaux de bord**, puis cliquez sur **Réseau** dans le Tableaux de bord du système collection.
4. Confirmez que le Débit du réseau et Paquets L2 les graphiques montrent des pics normaux ou constants, comme dans la figure ci-dessous. Un écart important entre les débits maximaux et les débits moyens peut indiquer que des problèmes de réseau affectent les performances Internet. Dans le cas contraire, poursuivez votre investigation sur les métriques DNS.



5. Cliquez **Activité** dans le Tableaux de bord du système collection.
6. Faites défiler la page jusqu'au Durée de traitement du serveur DNS pour toutes les activités et DNS pour toutes les activités graphiques.
   a) Le Durée de traitement du serveur DNS pour toutes les activités Ce graphique indique le temps écoulé entre le dernier paquet d'une demande DNS d'un client et le premier paquet de réponse DNS du serveur. Passez le curseur sur la médiane pour comparer le temps de traitement au même moment. Une grande différence entre la valeur médiane et le 95e percentile indique que quelque chose ne va peut-être pas avec un serveur DNS de votre réseau.



   b) Le DNS pour toutes les activités le graphique met en corrélation les réponses et les erreurs. Un pic d'erreurs peut entraîner des délais de deux à quatre secondes pour les clients, les serveurs, les applications et les clients. Dans la figure ci-dessous, la proportion de réponses à des erreurs semble constante.



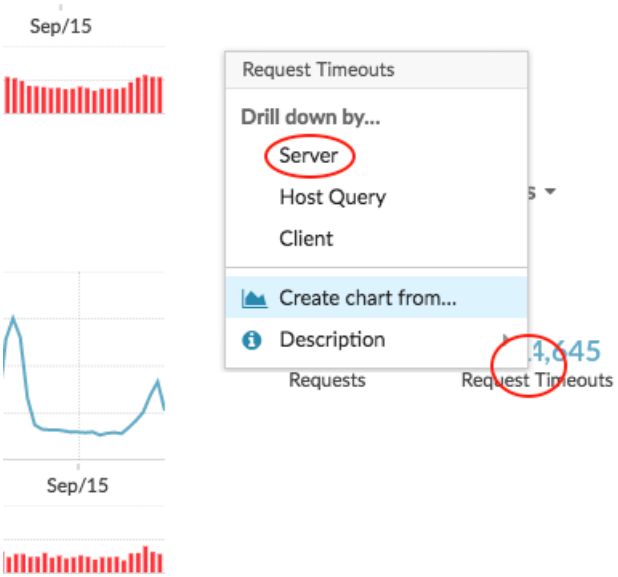
Sur la base de ces graphiques de tableau de bord, le débit du réseau semble correct, mais le temps de traitement du serveur DNS semble inhabituel. Ensuite, nous devrions étudier d'autres indicateurs du serveur DNS afin de déterminer la cause du ralentissement.

Afficher le nombre de délais d'expiration des requêtes DNS

La métrique DNS, Request Timeouts, indique l'échec du traitement d'une demande DNS. Les serveurs DNS qui ne répondent pas aux demandes peuvent avoir une incidence négative sur les performances des applications et d'Internet. Examinons le nombre total de délais d'expiration des requêtes pour les serveurs DNS de notre réseau sur une page de protocole. La page de protocole de l'application All Activity fournit un aperçu des indicateurs importants pour toutes les activités de votre réseau, y compris l'activité du protocole DNS. Nous pouvons ensuite effectuer une analyse détaillée pour voir quels serveurs DNS expirent.

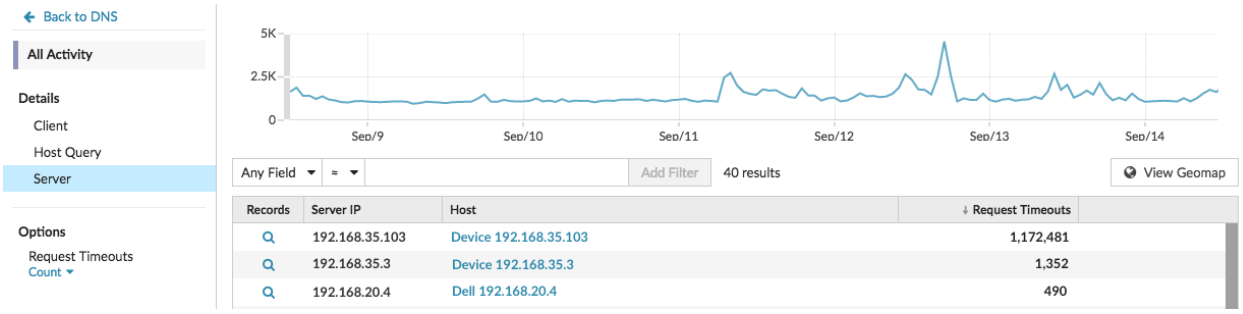
1. Dans le tableau de bord des activités, cliquez sur **DNS pour toutes les activités** titre du graphique.
2. Dans le Accédez à l'application... section du menu déroulant, cliquez sur **DNS pour toutes les activités**. La page de protocole All Activity apparaît.
3. Dans le volet de gauche, cliquez sur **DNS**.
4. Afficher le nombre de Délais d'expiration des demandes. Dans la figure ci-dessous, le chiffre est élevé (1 174 645) et mérite d'être étudié plus avant.

5. Cliquez sur la valeur métrique pour les délais d'expiration des demandes, puis sélectionnez **serveur**, comme le montre la figure ci-dessous.



Une page métrique détaillée apparaît qui affiche toutes les adresses IP des serveurs de votre réseau avec les délais d'expiration des demandes.

6. Notez quels appareils présentent le plus grand nombre de délais d'expiration des demandes. Dans la figure ci-dessous, il s'agit du périphérique 192.168.35.103.

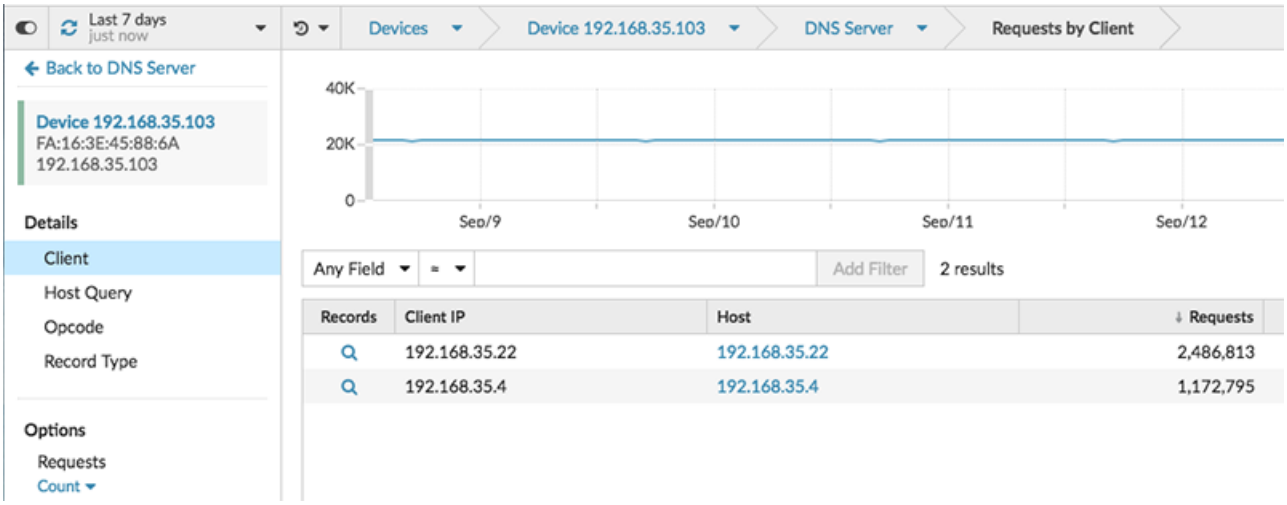


7. Dans le Hôte dans la colonne, cliquez sur le nom de l'équipement présentant le plus grand nombre de délais d'expiration des demandes.
Une nouvelle page de protocole apparaît, qui affiche les métriques spécifiques au périphérique 192.168.35.103. Nous pouvons maintenant examiner quels clients sont concernés par ce serveur DNS.

Trouvez les clients concernés par les délais d'expiration des requêtes DNS

Vous pouvez désormais identifier les clients qui ont envoyé des demandes à ce serveur DNS et qui sont susceptibles d'être affectés par les délais d'expiration des demandes DNS.

1. Sur la page de protocole du périphérique 192.168.35.103, cliquez sur **DNS** dans le Activité du serveur section dans le volet de gauche.
2. Dans le APPROFONDISSEZ section en haut de la page, cliquez sur **Clientèle**.



Une page métrique détaillée apparaît qui affiche toutes les adresses IP des clients ayant envoyé des demandes au serveur DNS.

Prochaines étapes
Sur cette page métrique détaillée, vous pouvez également découvrir les requêtes hôtes et les types d'enregistrement inclus dans les demandes en sélectionnant une option dans le Détails section du volet gauche. Vous pouvez également étudier les mesures associées pour chaque client en cliquant sur le lien dans le Hôte colonne.

Sur la base des données que vous avez collectées, vous pouvez désormais contacter l'équipe chargée de la maintenance de ce serveur DNS spécifique, car il est possible qu'il soit mal configuré ou qu'il rencontre d'autres problèmes.