Surveiller les erreurs DNS dans un tableau de bord

Publié: 2024-04-10

Le système de noms de domaine (DNS) est un service essentiel pour résoudre les noms d'hôtes en adresses IP. Tout système ayant besoin de localiser et de communiquer avec d'autres systèmes dépend du DNS.

Bien que le DNS soit généralement un service résilient dont vous ne vous inquiétez pas trop, les erreurs du serveur DNS peuvent avoir des conséquences désastreuses sur l'expérience de l'utilisateur final en matière de courrier électronique, de systèmes d'authentification, de sites Web et de bases de données.

Pour surveiller quand et où les erreurs DNS se produisent sur votre réseau, nous vous recommandons de créer un tableau de bord dans le système ExtraHop. Les tableaux de bord incluent plusieurs types de graphiques qui révèlent différents types d'informations sur une même métrique, ce qui peut aider à mettre en lumière la cause sous-jacente des erreurs DNS.

Cette procédure pas à pas vous explique comment créer un tableau de bord pour répondre aux questions suivantes :

- Combien d'erreurs DNS ai-je ?
- Quel est le pourcentage d'erreurs DNS sur mon réseau ?
- Quand les erreurs DNS se sont-elles produites ?
- Quelles requêtes sont à l'origine d'erreurs DNS ?
- Quels serveurs DNS renvoient les erreurs ?
- Les erreurs DNS affectent-elles les performances de mes autres serveurs (tels que la base de données ou les applications) ?

Prérequis

- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de privilèges d'écriture limités ou complets.
- Votre système ExtraHop doit également disposer de données réseau avec du trafic DNS.
- Familiarisez-vous avec les concepts présentés dans cette procédure pas à pas en lisant le Tableaux de bord sujet.

Si vous n'avez pas accès aux données du serveur DNS ou si vous ne disposez pas des privilèges appropriés, vous pouvez effectuer cette procédure pas à pas dans Démo ExtraHop.

Création d'un tableau de bord

Pour créer votre propre tableau de bord afin d'afficher les métriques DNS, procédez comme suit :

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 menu de commande ⋮ dans le coin supérieur droit et sélectionnez **Nouveau tableau de bord** pour créer un tableau de bord vide.
4. Entrez le nom de votre tableau de bord dans le **Titre** champ. Pour cette procédure pas à pas, tapez `Erreurs DNS`.
5. 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.

6. 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. 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**.

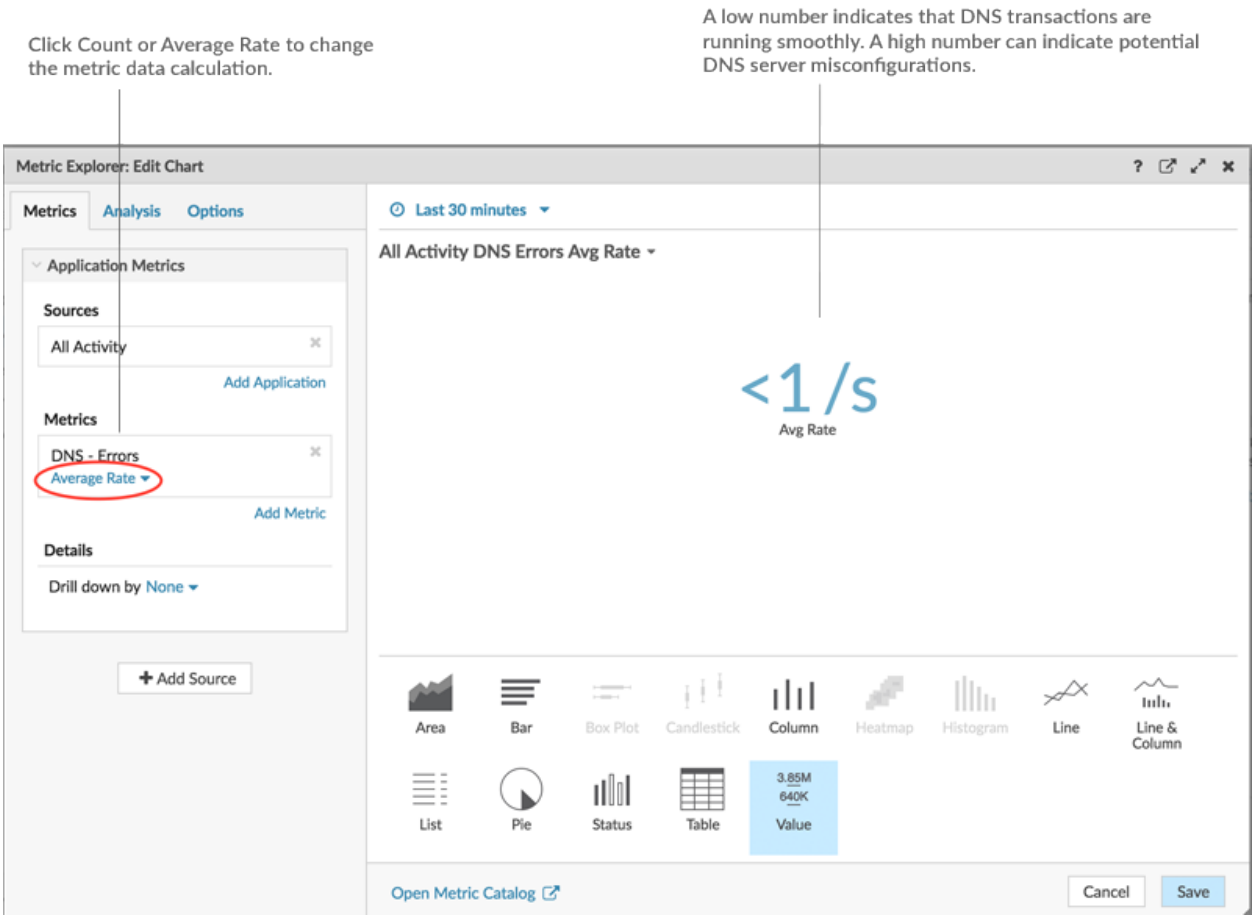
Prochaines étapes
Ajoutons les métriques d'erreur DNS au graphique vide.

Combien d'erreurs ai-je ?

Ces étapes vous montrent comment créer un graphique pour afficher le taux d'erreur DNS pendant un intervalle de temps spécifié.

Pour créer des graphiques de tableau de bord dans cette procédure pas à pas, vous allez sélectionner l' application All Activity comme source. All Activity est une source métrique disponible par défaut pour tous les utilisateurs et qui contient des métriques relatives à tous les appareils découverts sur votre réseau.

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 `Toutes les activités` pour filtrer les résultats, puis sélectionnez **Toutes les activités**.
4. Dans le champ Métriques, tapez `Erreurs DNS` pour filtrer les résultats à partir de toutes les mesures disponibles, puis sélectionnez **Erreurs DNS**.
5. Au bas de la page, cliquez sur **Valeur** graphique.
6. Cliquez **Compter** et sélectionnez **Taux moyen**.



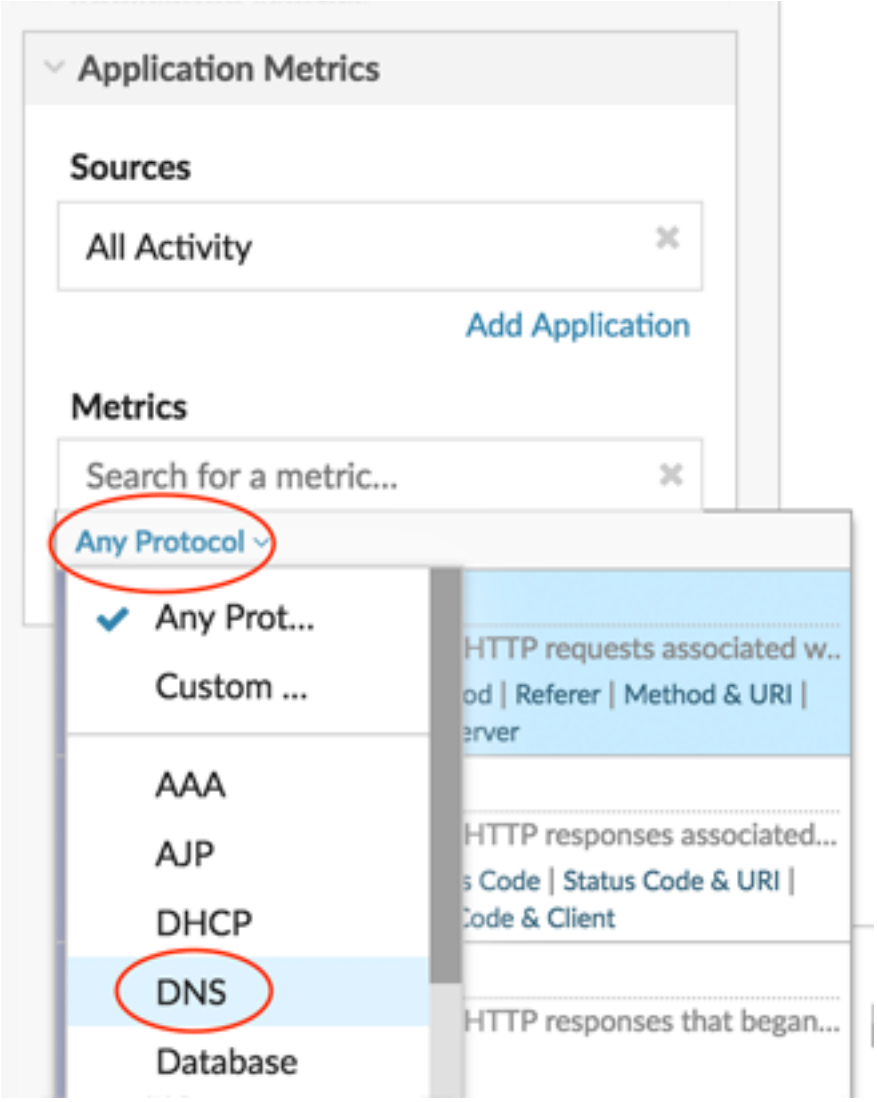
7. Cliquez **Enregistrer** pour revenir à votre tableau de bord.

Prochaines étapes
Continuons à ajouter d'autres tableaux d'erreurs DNS pour avoir une vue d'ensemble des erreurs DNS sur votre réseau.

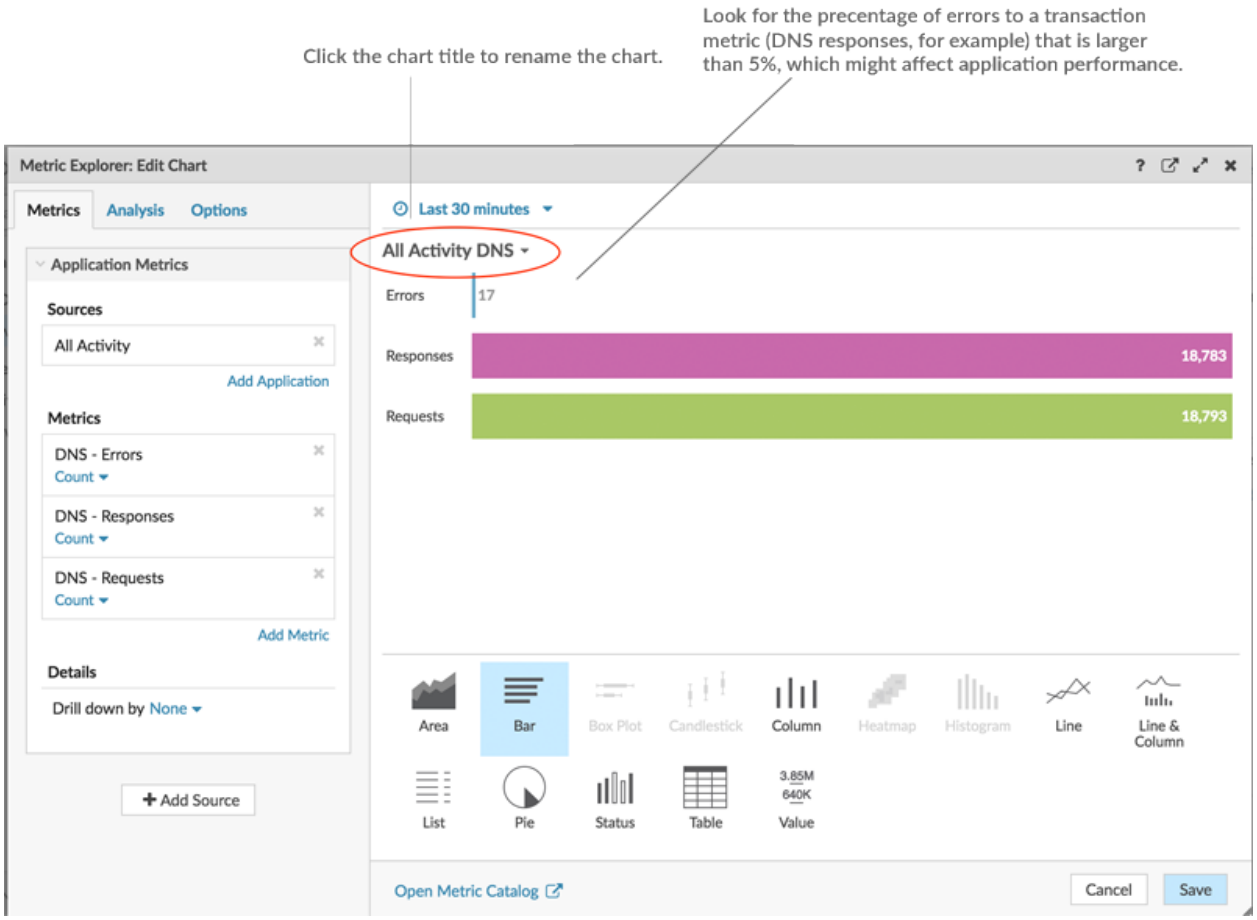
Quel est le pourcentage d'erreurs survenant sur mon réseau ?

La comparaison du nombre d'erreurs DNS au nombre de transactions DNS (demandes et réponses) peut vous aider à évaluer l'ampleur des problèmes de DNS sur votre réseau.

1. Au bas de la page, cliquez et faites glisser un widget graphique dans l'espace vide à côté du graphique des taux d'erreur DNS.
2. Cliquez sur le graphique.
3. Cliquez **Ajouter une source** et sélectionnez **Toutes les activités**.
4. Dans le champ Métriques, cliquez sur **N'importe quel protocole** et sélectionnez **DNS**. Ce raccourci peut vous aider à affiner votre recherche de métriques par protocole.



5. Type `erreurs` pour filtrer les résultats, puis sélectionner **Erreurs DNS**.
6. Au bas de la page, cliquez sur **Bar** graphique.
7. Cliquez **Ajouter une métrique**.
8. Cliquez **Tous les protocoles** et sélectionnez **DNS** depuis le menu déroulant.
9. Type `réponses` et sélectionnez **Réponses DNS**.
10. Cliquez **Ajouter une métrique**.
11. Cliquez **Tous les protocoles** et sélectionnez **DNS** depuis le menu déroulant.
12. Type `demandes` et sélectionnez **Requêtes DNS**.
13. Cliquez sur le titre du graphique et sélectionnez **Renommer**. Type `Pourcentage d'erreur` dans le champ de titre personnalisé.



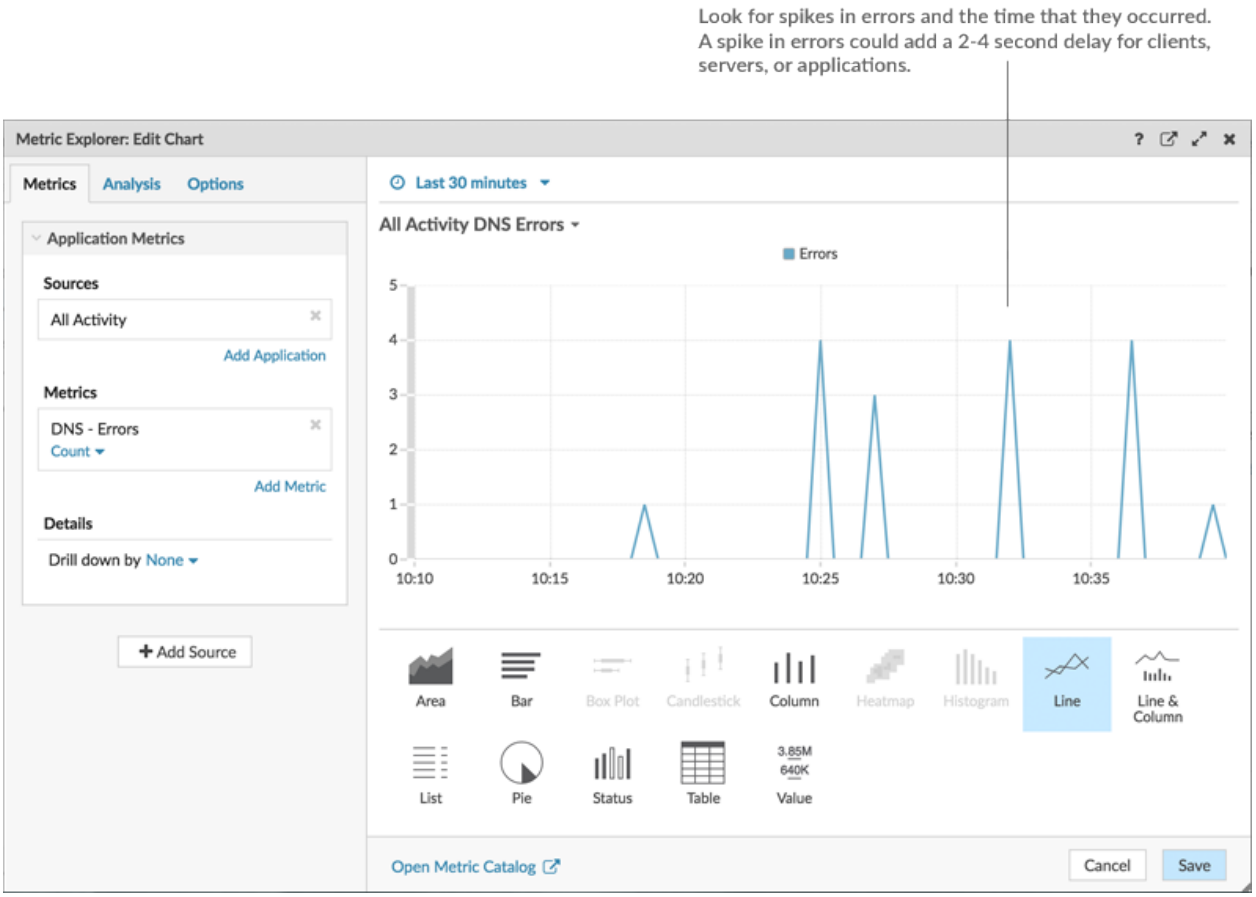
14. Cliquez **Enregistrer**.

Prochaines étapes
Vous pouvez désormais calculer le ratio entre les erreurs DNS et les transactions DNS.

Quand les erreurs DNS se sont-elles produites ?

Maintenant que vous avez déterminé l'étendue des erreurs DNS, examinons à quel moment les erreurs se sont produites et comment elles ont évolué au fil du temps.

1. Cliquez et faites glisser un nouveau widget graphique depuis le bas de la page vers un espace vide de la région.
2. Cliquez sur le graphique.
3. Cliquez **Ajouter une source**, sélectionnez **Toutes les activités**, puis sélectionnez **Erreurs DNS**.
4. Au bas de la page, cliquez sur **Ligne** graphique.



5. Cliquez **Enregistrer**.

Prochaines étapes
Vous disposez désormais de trois graphiques qui vous aident à visualiser l'état des transactions DNS effectuées sur votre réseau. Ensuite, ajoutons des graphiques qui vous aideront à identifier la cause des erreurs DNS et à voir leur effet sur l'ensemble de votre réseau.

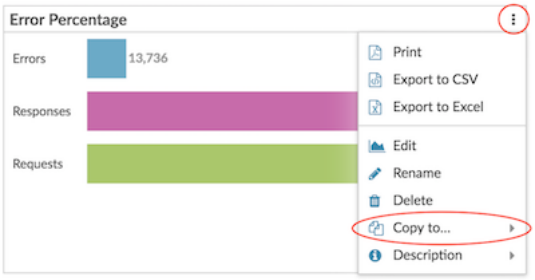
Quelles requêtes d'hôte sont à l'origine des erreurs DNS ?

Une requête d'hôte est envoyée par un client pour récupérer l'adresse IP d'un nom d'hôte (par exemple, pour « extrahop.com ») auprès d'un serveur DNS. Si le serveur DNS répond à la requête par une erreur, il est possible que le serveur soit mal configuré pour le domaine associé au nom d' hôte.

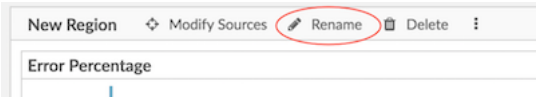
Vous pouvez explorer la métrique des erreurs DNS dans un graphique pour afficher jusqu'à 20 des principales requêtes de nom d'hôte ayant contribué au nombre total d'erreurs DNS sur votre réseau.

Avant d'ajouter un nouveau graphique des requêtes d'hôte à votre tableau de bord, ajoutons d'abord une autre région au tableau de bord afin de mieux organiser les graphiques actuels en groupes logiques.

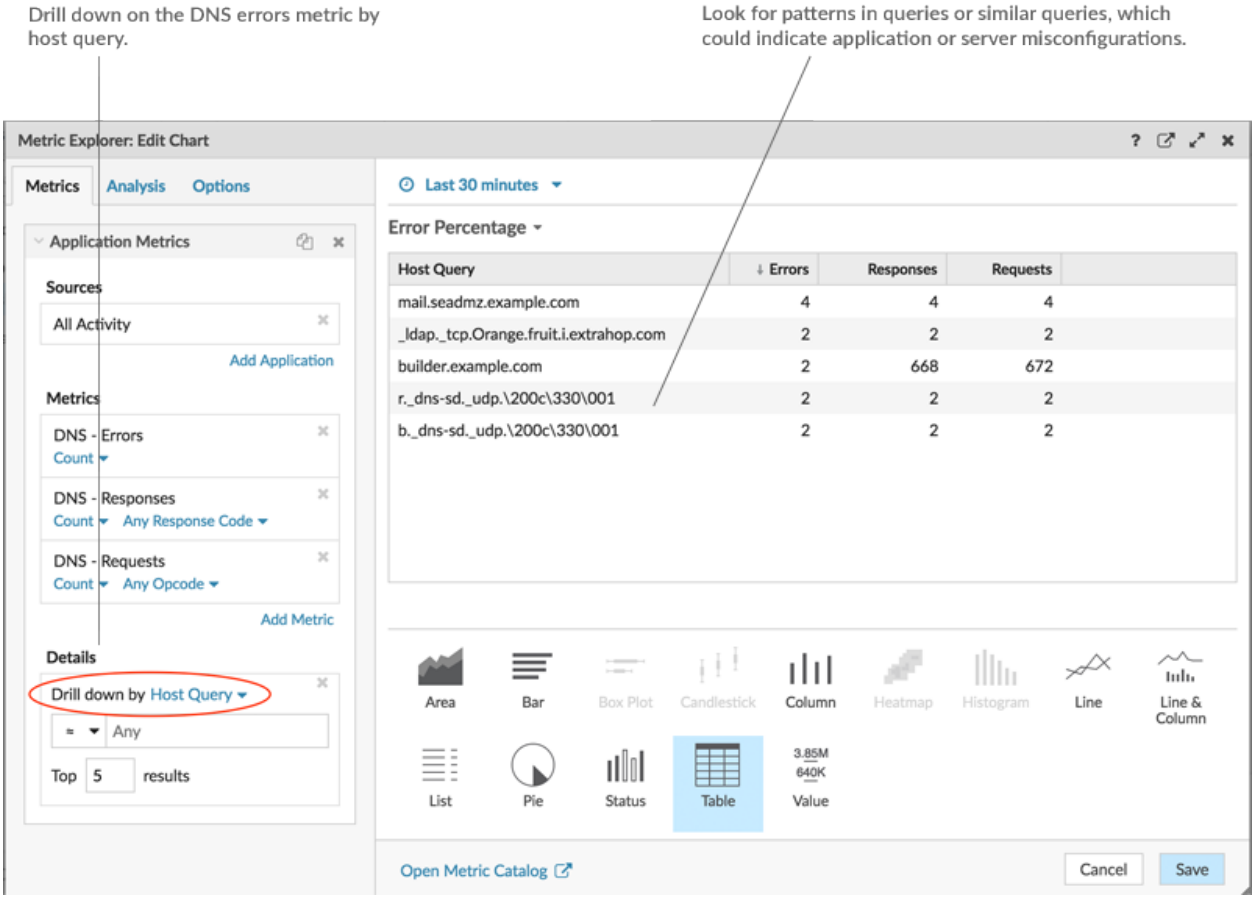
1. Sur le graphique « Pourcentage d'erreur », cliquez sur le menu des commandes ⋮ dans le coin supérieur droit.



2. Passez la souris sur **Copier vers...** et sélectionnez le nom de votre tableau de bord dans le menu. Cette étape crée une copie du graphique dans une nouvelle région. Les derniers tableaux de bord créés sont répertoriés en bas du menu.
3. Dans la nouvelle région, cliquez sur **Renommer**. Type `Détails des erreurs DNS` et cliquez **Enregistrer**.



4. Cliquez sur le graphique.
5. Cliquez sur le titre du graphique et tapez **Erreurs DNS par requête d'hôte**.
6. Au bas de la page, cliquez sur **Tableau**.
7. Dans la section Détails, cliquez sur **Extraire vers le bas par <None>** et sélectionnez **Requête sur l'hôte**.



Conseil Pour afficher davantage de requêtes, saisissez un plus grand nombre dans le champ Meilleurs résultats. Vous pouvez afficher jusqu'à 20 éléments détaillés dans un graphique de tableau de bord .

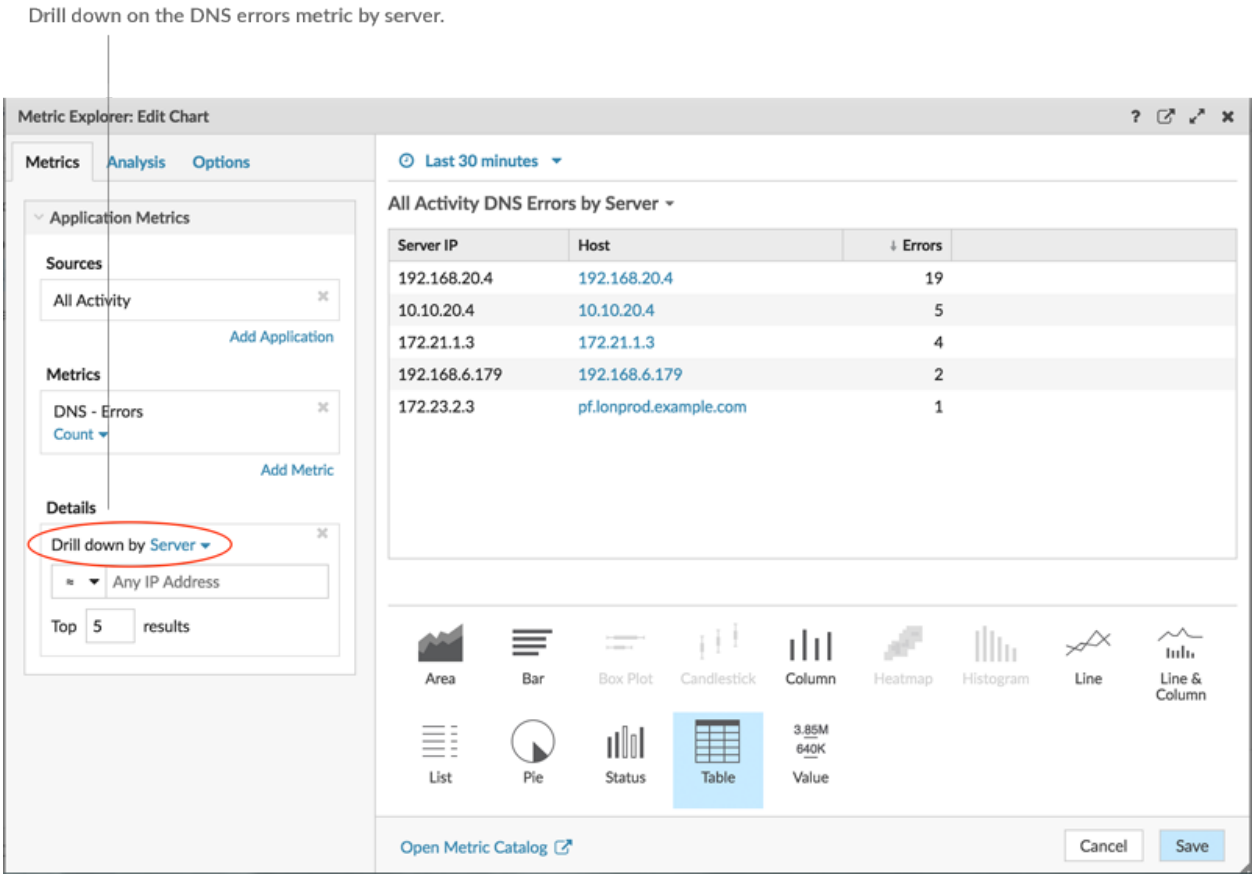
8. Cliquez **Enregistrer**.

Prochaines étapes
Après avoir identifié les requêtes qui ne résolvent pas ou qui sont à l'origine d'erreurs, vous pouvez commencer à résoudre les problèmes de configuration du serveur DNS dans votre environnement réseau.

Quels serveurs DNS renvoient des erreurs ?

Le fait de connaître les serveurs qui renvoient des erreurs DNS et le nombre d'erreurs envoyées par chaque serveur peut vous aider à résoudre les problèmes liés au DNS.

1. Cliquez et faites glisser le coin de la région pour faire de la place pour deux autres graphiques.
2. Cliquez sur un widget graphique et faites-le glisser depuis le bas de la page.
3. Cliquez sur le graphique.
4. Cliquez sur Ajouter une source, sélectionnez Toutes les activités, puis sélectionnez Erreurs DNS.
5. Au bas de la page, cliquez sur **Tableau**.
6. Dans la section Détails, cliquez sur **Profilez vers le bas par <None>** et sélectionnez **serveur**.



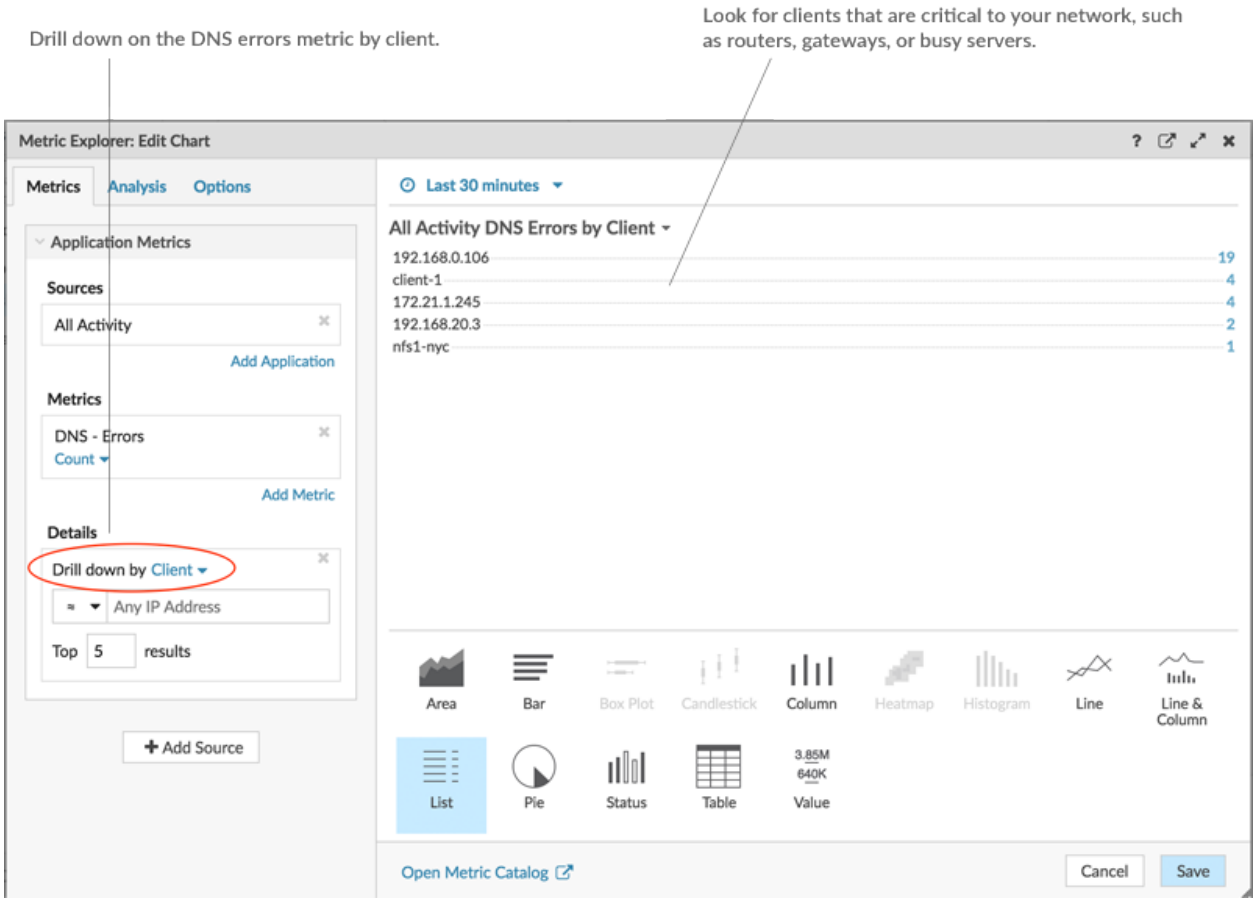
7. Cliquez **Enregistrer**.

Prochaines étapes
Vous pouvez désormais déterminer quels serveurs ont envoyé le plus d'erreurs DNS, potentiellement en raison de mauvaises configurations du serveur.

Les erreurs DNS affectent-elles les performances de mes autres serveurs ?

Vous pouvez déterminer quelles applications, bases de données et autres serveurs sont affectés négativement par les erreurs DNS. Créons un graphique qui indique le nombre d'erreurs DNS commises par les clients ayant reçu le plus grand nombre d'erreurs.

1. Au bas de la page, glissez et déposez un widget graphique dans une zone vide.
2. Cliquez sur le graphique.
3. Cliquez **Ajouter une source**, sélectionnez **Toutes les activités**, puis sélectionnez **Erreurs DNS**.
4. Au bas de la page, cliquez sur **Liste** graphique.
5. Dans la section Détails, cliquez sur **Extraire vers le bas par <None>** et sélectionnez **Cliente**.



Note: Vous pouvez ajouter un sparkline à votre graphique en listes pour voir comment le nombre de mesures pour chaque client a évolué au fil du temps. Cliquez sur l'onglet Options et sélectionnez **Inclure Sparkline**.

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

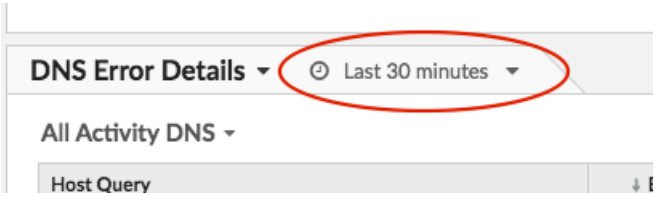
Prochaines étapes

Votre tableau de bord est terminé ! Vous pouvez désormais surveiller les erreurs DNS à des fins de résolution des problèmes. Les sections suivantes proposent des conseils supplémentaires pour analyser les problèmes liés au DNS à partir de votre tableau de bord.

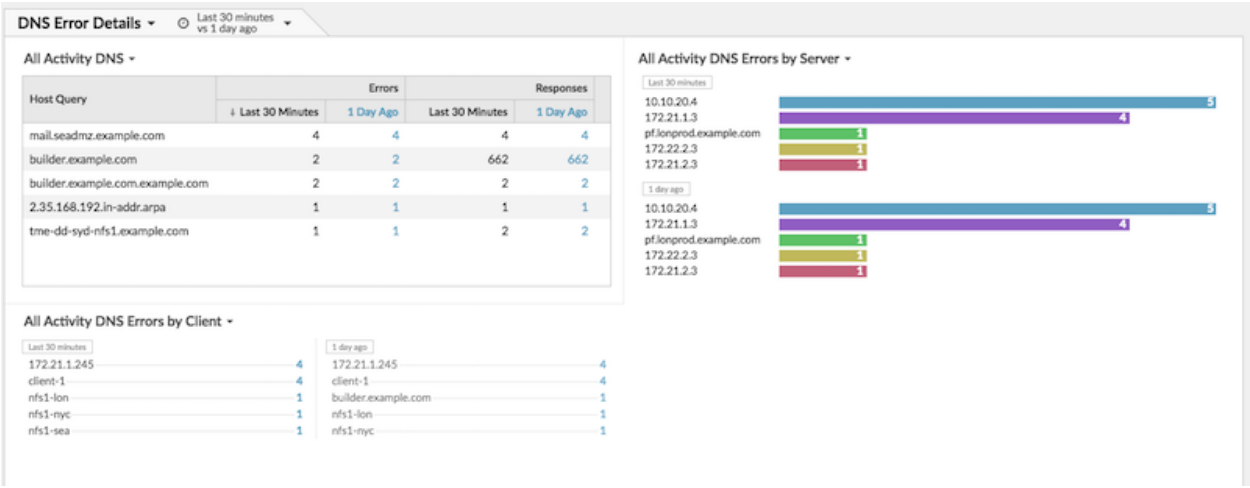
Comparez différents intervalles de temps

En appliquant une comparaison delta des intervalles de temps à vos graphiques, vous pouvez voir l'évolution des données entre deux intervalles de temps côte à côte.

1. Cliquez sur le titre de la région, « Détails des erreurs DNS », puis sélectionnez **Utiliser le sélecteur de temps par région**.
2. À côté de l'en-tête de région Détails des erreurs DNS, cliquez sur **30 dernières minutes**.



3. Au bas de la fenêtre d'intervalle de temps, cliquez sur **Comparez**. Vous pouvez désormais sélectionner deux intervalles pour effectuer une comparaison delta des mesures de chaque période. Pour cet exemple, comparons les statistiques d'hier à celles des 30 dernières minutes.
4. Cliquez **Enregistrer**. Vous pouvez désormais voir une comparaison des indicateurs dans tous les graphiques de la région, comme le montre la figure ci-dessous.



Note: Vous pouvez effectuer une comparaison delta pour l'ensemble du tableau de bord en modifiant l'intervalle de temps global. L'intervalle de temps global est situé dans le coin supérieur gauche de la page du tableau de bord.

5. Pour supprimer la comparaison des deltas, cliquez sur **Dernières 30 minutes vs il y a 1 jour** dans l'en-tête de la région, cliquez sur **Supprimer Delta**, puis cliquez sur **Enregistrer**.

Mesures DNS supplémentaires à surveiller

Les erreurs DNS sont une source d'informations sur l'état du trafic DNS sur votre réseau. Le tableau suivant contient des statistiques supplémentaires que vous pouvez ajouter à votre tableau de bord pour répondre aux questions suivantes :

Question	métrique DNS	Descriptif
Les serveurs DNS abandonnent-ils les requêtes ?	Expiration des requêtes DNS	Les requêtes DNS qui ne reçoivent pas de réponse de la part d'un serveur DNS constituent des goulots d' étranglement potentiels. Les délais d'attente

Question	métrique DNS	Descriptif
		des serveurs peuvent entraîner des ralentissements et des interruptions pour les serveurs, les clients et les applications.
Existe-t-il des failles de sécurité liées au DNS ?	Demandes DNS, hiérarchisez par requête hôte et filtrez pour « WPAD » ou « ISATAP ».	Découverte automatique du proxy Web (WPAD) et Protocole d'adressage automatique des tunnels intra-site (ISATAP) sont des exemples de requêtes d' hôte liées à des risques de sécurité connus.
Le réseau affecte-t-il les transactions DNS ?	Durée aller-retour du DNS	Le temps de trajet aller-retour (RTT) est calculé en observant le temps nécessaire aux paquets pour traverser le réseau entre les appareils. Un RTT élevé peut indiquer une latence du réseau.