Naviguer dans le système ExtraHop

Publié: 2024-07-02

Le système ExtraHop permet d'accéder aux données d'activité du réseau et aux détails de détection via une interface utilisateur dynamique et hautement personnalisable.

Ce guide fournit une vue d'ensemble de la navigation globale ainsi que des commandes, des champs et des options disponibles dans l'ensemble du système. Voir Présentation du système ExtraHop pour savoir comment le système ExtraHop collecte et analyse vos données.

Vidéos Consultez la formation associée : Parcours d'apprentissage complet des fondamentaux de l'interface utilisateur

Navigateurs pris en charge

Les navigateurs suivants sont compatibles avec tous les systèmes ExtraHop. Appliquez les fonctionnalités d'accessibilité et de compatibilité fournies par votre navigateur pour accéder au contenu par le biais d'outils technologiques d'assistance.

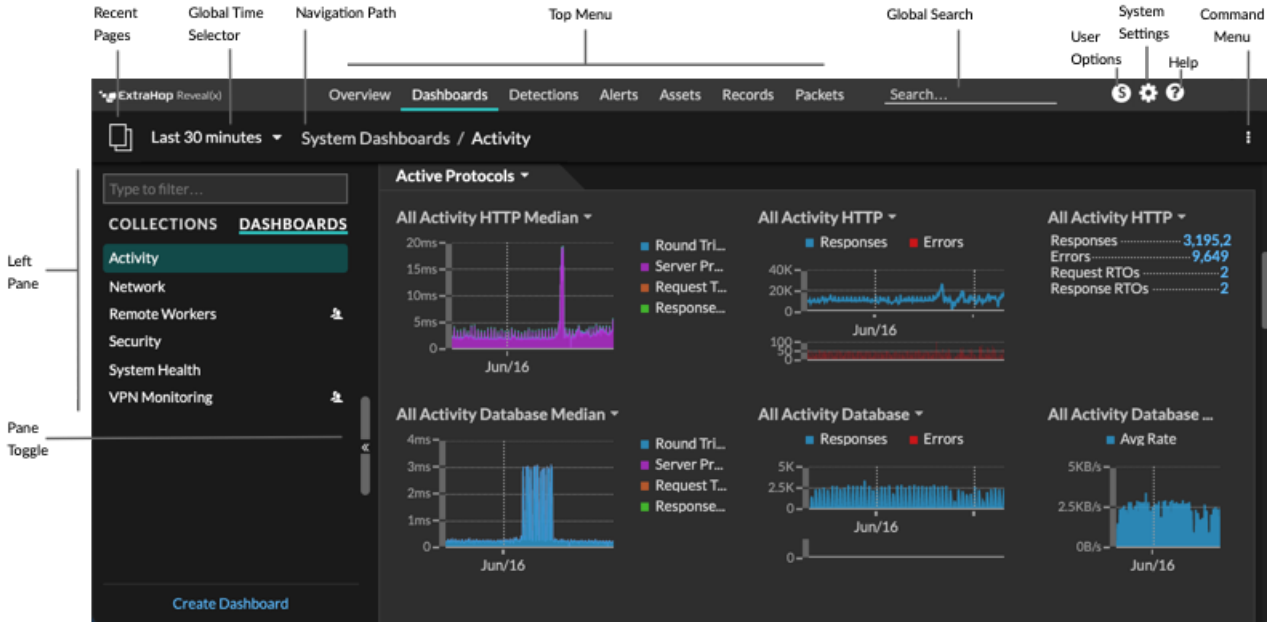
- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Important: Internet Explorer 11 n'est plus pris en charge. Nous vous recommandons d' installer la dernière version de tout navigateur compatible.

Disposition et menus

Les éléments de navigation globale sont situés en haut de la page et contiennent des liens vers les principales sections du système. Dans chaque section, le volet de gauche contient des liens vers des pages ou des données spécifiques.

La figure suivante montre à la fois les éléments de navigation globaux et du volet gauche.



Voici les définitions de chaque élément de navigation global :

Pages de présentation

Les pages de présentation vous permettent d'évaluer rapidement l'étendue des activités suspectes sur votre réseau, d'en savoir plus sur l'activité du protocole et les connexions des équipements, et d'étudier le trafic entrant et sortant sur votre réseau.

- Consultez le Aperçu de la sécurité pour obtenir des informations sur les détections de sécurité sur votre réseau.
- Consultez le Vue d'ensemble du réseau pour obtenir des informations sur les appareils actifs de votre réseau.
- Consultez le Vue d'ensemble du périmètre pour obtenir des informations sur le trafic entrant et sortant de votre réseau.

Tableaux de bord

Cliquez **Tableaux de bord** pour afficher, créer ou partager des tableaux de bord afin de surveiller tous les aspects de votre réseau ou de vos applications. Tableaux de bord du système vous offrent un aperçu instantané de l'activité et des menaces de sécurité potentielles sur votre réseau.

Alertes

Cliquez **Alertes** pour afficher les informations relatives à chaque alerte générée pendant l'intervalle de temps.

Détections

Si votre paquet ou flux sonde est connecté au service d'apprentissage automatique ExtraHop, la navigation de niveau supérieur affiche **Détections** menu. Cliquez **Détections** pour consulter les détections identifiées à partir de vos données Wire Data. Vous pouvez accéder aux détections enregistrées même si sonde est déconnecté du service d'apprentissage automatique.

Note: Les détections par apprentissage automatique nécessitent connexion aux services cloud ExtraHop.

Actifs

Cliquez **Actifs** pour trouver n'importe quelle application, réseau ou équipement découvert par le système ExtraHop. Vous pouvez consulter les mesures de protocole relatives à vos actifs, à vos utilisateurs actifs ou à l'activité réseau par protocole.

Disques

Si votre système ExtraHop est configuré avec espace de stockage des enregistrements, la navigation de niveau supérieur affiche le menu Enregistrements. Cliquez **Disques** pour rechercher tous les enregistrements stockés pour l' intervalle de temps actuel. Les enregistrements sont des informations structurées sur les transactions, les messages et les flux réseau.

Paquets

Si votre système ExtraHop est configuré avec stockage des paquets, la navigation de niveau supérieur affiche le menu Paquets. Cliquez **Paquets** pour rechercher tous les paquets stockés pour l' intervalle de temps actuel.

champ de recherche global

Tapez le nom de n'importe quel équipement, nom d'hôte ou adresse IP, application ou réseau pour trouver une correspondance sur votre sonde ou console. Si vous avez un espace de stockage des enregistrements connecté, vous pouvez rechercher des enregistrements enregistrés. Si vous avez un système de stockage des paquets connecté, vous pouvez rechercher des paquets.

Icône d'aide

Consultez les informations d'aide relatives à la page que vous êtes en train de consulter. Pour accéder à la documentation ExtraHop la plus récente et la plus complète, visitez le Site de documentation ExtraHop.

Icône des paramètres système

Accédez aux options de configuration du système, telles que les déclencheurs, les alertes, les rapports planifiés et les appareils personnalisés, puis cliquez pour afficher le système ExtraHop et sa version. Cliquez **Avis relatifs au système** pour afficher la liste des fonctionnalités de la version la plus récente et de toutes notifications relatives au système telles que les licences expirant ou les mises à niveau du microprogramme disponibles.

Icône d'option utilisateur

Connectez-vous et déconnectez-vous de votre sonde ou console, modifiez votre mot de passe, sélectionnez le thème d'affichage, définir une langue, et accédez aux options de l'API.

Basculement du volet

Réduisez ou agrandissez le volet de gauche.

sélecteur de temps global

Modifier l'intervalle de temps pour afficher l'activité des applications et du réseau observée par le système ExtraHop pendant une période donnée. L'intervalle de temps global est appliqué à toutes les mesures du système et ne change pas lorsque vous naviguez sur différentes pages.

Pages récentes

Consultez la liste des dernières pages que vous avez visitées dans un menu déroulant et faites une sélection pour revenir à la page précédente. Les pages répétées sont dédupliquées et condensées pour économiser de l'espace.

Trajectoire de navigation

Affichez où vous vous trouvez dans le système et cliquez sur le nom d'une page dans le chemin pour revenir à cette page.

Menu déroulant des commandes

Cliquez pour accéder à des actions spécifiques pour la page que vous consultez. Par exemple, lorsque vous cliquez **Tableaux de bord** en haut de la page, le menu de commandes ⋮ propose des actions permettant de modifier les propriétés du tableau de bord ou de créer un nouveau tableau de bord.

Commencez à analyser les données

Commencez votre parcours d'analyse de données avec le système ExtraHop en suivant les flux de travail de base répertoriés ci-dessous. Au fur et à mesure que vous vous familiariserez avec le système ExtraHop,

vous pourrez effectuer des tâches plus avancées, telles que l'installation de bundles et la création de déclencheurs.

Voici quelques méthodes de base pour naviguer et utiliser le système ExtraHop pour analyser l' activité du réseau.

Surveillez les métriques et étudiez les données intéressantes

Les bons points de départ sont tableau de bord de l'activité réseau et tableau de bord des performances du réseau, qui vous présentent des résumés des indicateurs importants relatifs aux performances des applications sur votre réseau. Lorsque vous constatez un pic de trafic, des erreurs ou le temps de traitement du serveur, vous pouvez interagir avec les données du tableau de bord pour approfondissez et identifiez quels clients, serveurs, méthodes ou autres facteurs ont contribué à cette activité inhabituelle.

Vous pouvez ensuite poursuivre le suivi des performances ou le dépannage en création d'un tableau de bord personnalisé pour suivre un ensemble de mesures et d' appareils intéressants.

Consultez ce qui suit procédures pas à pas pour en savoir plus sur la surveillance des données dans les tableaux de bord :

- Surveillez les performances du site Web dans un tableau de bord
- Surveiller les erreurs DNS dans un tableau de bord
- Surveiller l'état de la base de données dans un tableau de bord

Recherchez un équipement spécifique et étudiez les métriques et les transactions associées

Si vous souhaitez étudier un serveur lent, vous pouvez recherchez le serveur dans le système ExtraHop par nom d'équipement ou adresse IP puis examinez l'activité du serveur sur une page de protocole. Y a-t-il eu une augmentation du nombre d'erreurs de réponse ou de demandes ? Le temps de traitement du serveur était-il trop long ou la latence du réseau a-t-elle affecté le taux de transfert de données ? Cliquez sur différents protocoles sur la page Appareils pour étudier d'autres données métriques collectées par le système ExtraHop. Exploration par adresses IP homologues pour voir à quels clients ou applications le serveur a communiqué.

Si votre système ExtraHop est connecté à un espace de stockage des enregistrements, vous pouvez examiner l'intégralité des transactions auxquelles le serveur a participé en création d'une requête d'enregistrement.

Consultez ce qui suit procédures pas à pas pour en savoir plus sur l'exploration des indicateurs et des enregistrements :

- Explorez les métriques du système ExtraHop pour étudier les défaillances du DNS
- Interrogez les enregistrements pour trouver les ressources Web manquantes

Obtenez de la visibilité sur les modifications apportées à votre réseau en recherchant l'activité du protocole

Vous pouvez obtenir une vue de haut en bas de votre réseau en consultant les groupes de protocoles intégrés. Un groupe de protocoles est un ensemble d'appareils automatiquement regroupés par le système ExtraHop en fonction du trafic de protocole observé sur le fil. Par exemple, vous pouvez trouver des serveurs nouveaux ou mis hors service qui communiquent activement via un protocole en création d'une carte d'activités.

Si vous trouvez un ensemble d'appareils que vous souhaitez continuer à surveiller, vous pouvez ajouter une étiquette d'équipement ou nom de l'équipement personnalisé pour que ces appareils soient plus faciles à trouver dans le système ExtraHop. Vous pouvez également créer un groupe d'équipements personnalisé ou un tableau de bord personnalisé pour surveiller l'activité d'un groupe déquipements.

Flux de travail avancés pour personnaliser votre système ExtraHop

Une fois familiarisé avec les flux de travail de base, vous pouvez personnaliser votre système ExtraHop en configurant des notifications d'alerte, en créant des métriques personnalisées ou en installant des offres groupées.

Configurer des alertes

Alertes suivez les mesures spécifiées pour vous informer des écarts de trafic susceptibles d'indiquer un problème avec un équipement réseau. Configuration d'une alerte de seuil pour vous avertir lorsqu'une métrique surveillée dépasse une valeur définie. Configuration d'une alerte de tendance pour vous avertir lorsqu'une métrique surveillée s'écarte des tendances normales observées par le système.

Créez un déclencheur pour créer des mesures et des applications personnalisées

déclencheurs sont des scripts personnalisés qui exécutent une action lors d'un événement prédéfini. Les déclencheurs nécessitent une planification pour s'assurer qu'ils n'ont pas d'impact négatif sur les performances du système.

Consultez ce qui suit procédures pas à pas pour en savoir plus sur l'exploration des métriques et des enregistrements :

- Créez un déclencheur pour collecter des métriques personnalisées pour les erreurs HTTP 404
- Créez un déclencheur pour surveiller les réponses aux requêtes NTP monlist