Disques

Publié: 2024-09-26

Les enregistrements sont des informations structurées sur les flux de transactions, de messages et de réseaux qui sont générées et envoyées depuis le système ExtraHop vers un espace de stockage des enregistrements. Une fois vos enregistrements collectés et stockés, vous pouvez les rechercher dans le système ExtraHop.

Les enregistrements sont collectés à deux niveaux de protocole : L3 et L7. Les enregistrements L3 (ou flux) indiquent les transactions de couche réseau entre deux appareils via le protocole IP. Les enregistrements L7 présentent des transactions basées sur des messages (comme ActiveMQ, DNS et DHCP), transactionnelles (telles que HTTP, SMB et NFS) et basées sur des sessions (telles que TLS et ICA).

Par exemple, si vous avez rencontré cinquante erreurs HTTP 503, les transactions HTTP associées contiendraient des informations sur l'URL, le serveur Web, le client qui a envoyé la demande, etc. Ces informations peuvent vous aider à identifier le problème sous-jacent.

Vidéos Consultez la formation associée : Disques

Avant de commencer

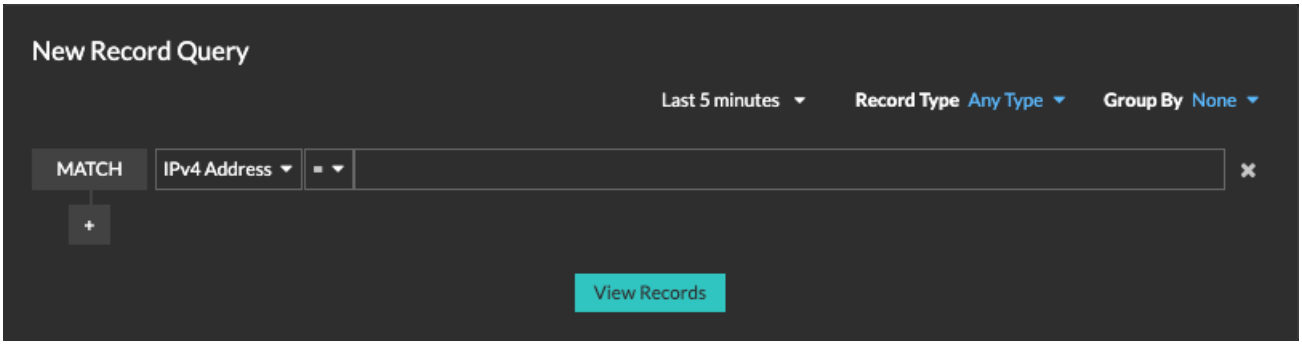
- Vous devez disposer d'un espace de stockage des enregistrements configuré, tel qu'un espace de stockage des enregistrements ExtraHop, Splunk, Google BigQuery, ou Balance à journaux CrowdStrike Falçon.
- Vous ne pouvez configurer qu'un seul espace de stockage des enregistrements pour le système ExtraHop.
- Votre système ExtraHop doit être configuré pour collecter et stocker enregistrements de flux ou records L7.

Naviguer dans les enregistrements

La page principale des enregistrements propose plusieurs méthodes pour rechercher des enregistrements stockés. Cliquez **Disques** depuis le menu supérieur pour commencer.

Recherche standard

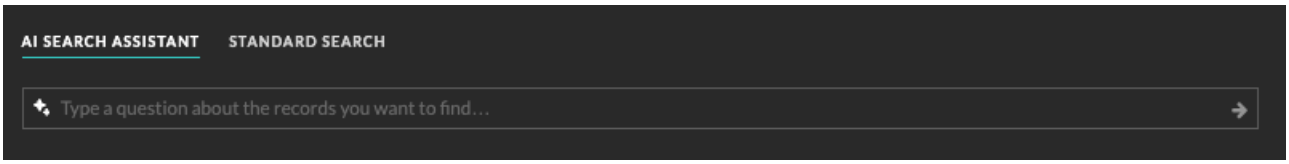
Recherchez des enregistrements à l'aide d'une recherche standard pour créer un filtre complexe en combinant les opérateurs « ET » et « OU » avec des options de filtre supplémentaires telles que le type d'enregistrement et l'intervalle de temps. En savoir plus sur l'interrogation d'enregistrements à l'aide d'une recherche standard.



Assistant de recherche IA

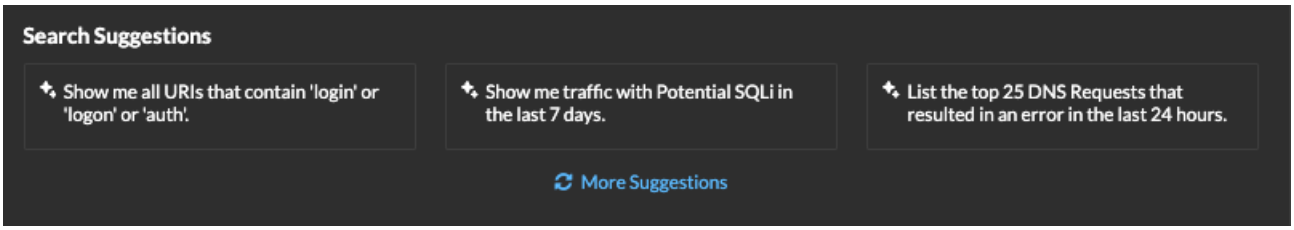
AI Search Assistant vous aide à rechercher des enregistrements contenant des questions rédigées dans un langage naturel et courant afin de créer rapidement des requêtes complexes par rapport à

la création d'une requête de recherche standard avec les mêmes critères. L'assistant de recherche AI doit être activé par votre administrateur ExtraHop.En savoir plus sur la recherche d'enregistrements avec AI Search Assistant.



Suggestion de recherche

Le système ExtraHop propose plusieurs recherches suggérées avec des filtres prédéfinis qui vous aident à effectuer plus efficacement des recherches d'enregistrements courantes. Cliquez sur une recherche suggérée pour appliquer la requête et afficher immédiatement les enregistrements ou cliquez sur **Plus de suggestions** pour plus d'options.



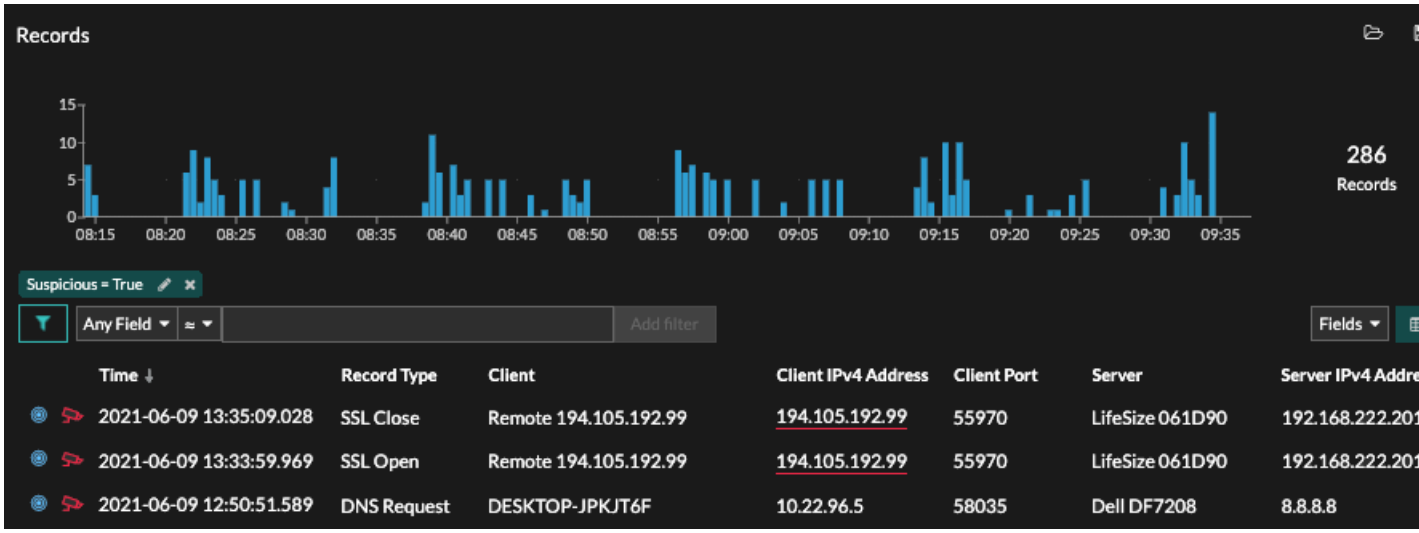
Requêtes enregistrées

Vous pouvez également sélectionner une requête précédemment enregistrée dans la liste de la page Enregistrements et afficher immédiatement les enregistrements, ou vous pouvez cliquer sur l'icône du dossier dans le coin supérieur droit de la page pour afficher toutes les requêtes enregistrées.

Note: Pour créer une requête d'enregistrement pour une métrique personnalisée, vous devez d'abord définir la relation entre les enregistrements en lier la métrique personnalisée à un type d'enregistrement.

Affichage des résultats d'une requête d'enregistrement

Une fois que vous avez soumis la requête, les résultats apparaissent sur la page principale des enregistrements.



Note: Une requête peut renvoyer des millions d'enregistrements en fonction de l' intervalle de temps et des critères de filtre. Si une requête dépasse le nombre maximum de résultats de requête, un nombre tronqué d'enregistrements apparaît (espace de stockage des enregistrements ExtraHop uniquement). Par exemple, les requêtes provenant du filtre Any Field par défaut génèrent souvent un très grand nombre de résultats et peuvent avoir un impact sur les performances.

Voici quelques méthodes pour explorer les résultats des requêtes d'enregistrement :

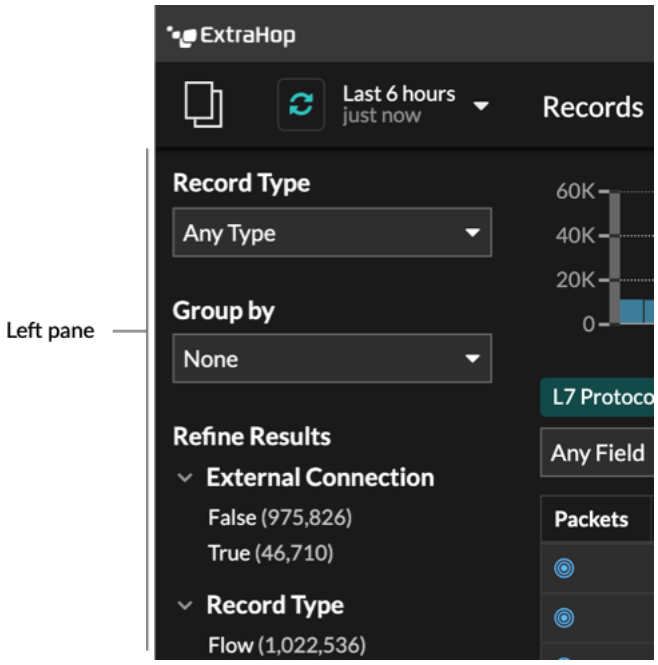
- Dans le graphique des enregistrements, passez la souris sur un intervalle de temps pour afficher le nombre d' enregistrements, ou cliquez et faites glisser le pointeur sur le graphique pour limiter les résultats de la requête d'enregistrement à un intervalle de temps spécifique.
- Cliquez sur un nom d'hôte ou une adresse IP pour afficher les détails de l'équipement ou du point de terminaison externe.
- Les enregistrements contenant des adresses IP, des noms d'hôte et des URI suspects apparaissent avec une icône de caméra rouge. Cliquez sur l'icône de la caméra pour voir renseignements sur les menaces pour l' enregistrement.
- Cliquez sur l'icône d'un paquet pour démarrer requête de paquet qui est filtré par cet enregistrement.
- Les résultats des enregistrements apparaissent dans un tableau par défaut. Cliquez sur la vue tabulaire ou la vue détaillée icônes pour basculer l'affichage.
- Une requête s'arrête automatiquement si le nombre d'octets d'enregistrement scannés ou renvoyés est extrêmement important. En cas de pause, la requête affiche les enregistrements les plus récents. Cliquez **Poursuivre la requête** pour reprendre la recherche.
- Cliquez sur **Champs** liste déroulante pour ajouter des informations d'enregistrement supplémentaires à la vue des enregistrements.
- Dans la vue sous forme de tableau, cliquez et faites glisser les en-têtes de colonne pour organiser les informations d'enregistrement.
- Postulez simple ou filtres avancés pour détecter les problèmes potentiels, tels que des délais de traitement trop longs ou des tailles de réponse inhabituelles.

Affinez votre filtre de requête d'enregistrement

Vous pouvez affiner votre filtre de recherche d'enregistrements de plusieurs manières pour trouver les enregistrements exacts que vous recherchez. Les sections ci-dessous décrivent chaque méthode et présentent des exemples avec lesquels vous pouvez commencer pour vous familiariser.

Filtrer les résultats de l'enregistrement depuis le volet de gauche

Une fois que tous les enregistrements disponibles pour l'intervalle de temps que vous avez sélectionné apparaissent sur la page Enregistrements, vous pouvez filtrer depuis le volet de gauche pour affiner vos résultats.



Le **Type d'enregistrement** le menu déroulant affiche une liste de tous les types d' enregistrements que votre système ExtraHop est configuré pour collecter et stocker. Un type d'enregistrement détermine quelles données sont collectées et stockées dans l'espace de stockage des enregistrements.

Note: Comme vous devez créer un déclencheur pour collecter des enregistrements, vous avez besoin d'un moyen d' identifier le type de données que vous allez collecter. Il existe des types d'enregistrement intégrés qui collectent tous les champs connus disponibles pour un protocole. Vous pouvez commencer avec un type d' enregistrement intégré (tel que HTTP) et créer un déclencheur pour ne collecter que les champs du protocole qui vous intéressent (tels que l'URI et le code dstatus). Les utilisateurs avancés peuvent également créer un type d'enregistrement personnalisé s'ils ont besoin de collecter des informations propriétaires qui ne sont pas disponibles via un type d'enregistrement intégré.

Le **Regrouper par** La liste déroulante vous donne une liste de champs permettant de filtrer davantage le type d'enregistrement.

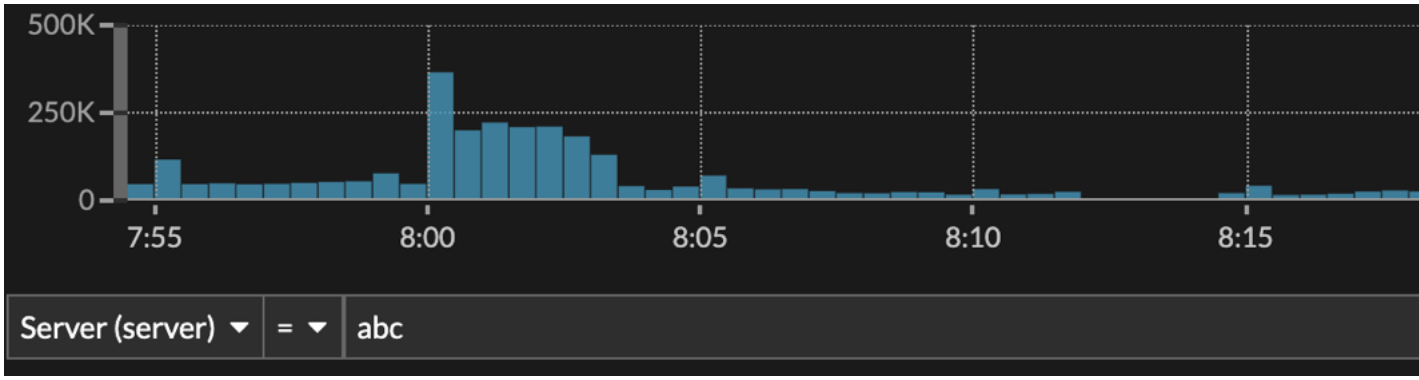
Le **Affiner les résultats** La section affiche une liste des filtres d'enregistrement courants pour le type d'enregistrement sélectionné avec le nombre d'enregistrements correspondant au filtre entre parenthèses.

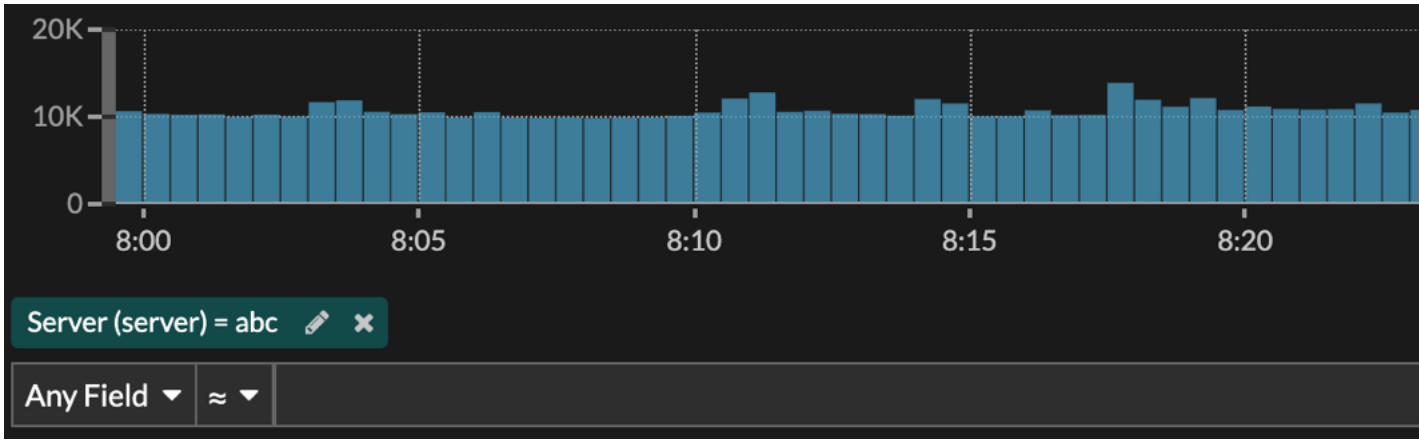
Filtrer les résultats de l'enregistrement via le trifield

Cliquez sur l'icône en forme de crayon pour modifier un filtre existant ou cliquez sur le bouton Ajouter un filtre avancé pour ajouter un nouveau filtre.

Dans le **Nom d'affichage du filtre** champ, vous pouvez spécifier un nom descriptif pour identifier l'objectif général de la requête.

Sélectionnez une option de critère dans le menu déroulant (l'option par défaut est Adresse IPv4), sélectionnez un opérateur (tel que le signe égal (=)), puis saisissez la valeur de recherche . Cliquez **Ajouter un filtre**, et le filtre est ajouté au-dessus de la barre de filtre.





Vos résultats n'affichent que les enregistrements correspondant au filtre.

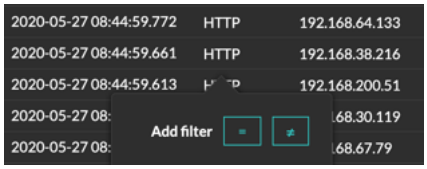
Les opérateurs suivants peuvent être sélectionnés en fonction du nom du champ sélectionné :

Opérateur	Descriptif
=	Égaux
≠	N'est pas égal
≈	Inclut Si les enregistrements sont stockés sur un espace de stockage des enregistrements ExtraHop, l'opérateur includes fait correspondre les mots entiers délimités par des espaces et des signes de ponctuation. Par exemple, une recherche sur « www.extra » correspondrait à « www.extra.com » mais pas à « www.extrahop.com ». Pour toutes les autres librairies, l'opérateur includes fait correspondre les sous-chaînes, y compris les espaces et la ponctuation. Par exemple, une recherche pour « www.extra » correspondrait à « www.extrahop.com », mais une recherche pour « www extra » ne correspondrait pas à « www.extrahop.com ».

Opérateur	Descriptif
	Les caractères Regex et les caractères génériques ne sont pas pris en charge.
≈/	Exclut Si les enregistrements sont stockés sur un espace de stockage des enregistrements ExtraHop, l'opérateur d'exclusion fait correspondre les mots entiers délimités par des espaces et des signes de ponctuation. Par exemple, une recherche sur « extra » exclurait « www.extra.com » mais pas « www.extrahop.com ». Pour toutes les autres librairies, l'opérateur d'exclusion fait correspondre les sous-chaînes, y compris les espaces et la ponctuation. Par exemple, une recherche sur « www.extra » exclurait « www.extrahop.com », mais une recherche sur « www extra » n'exclurait pas « www.extrahop.com ». Les caractères Regex et les caractères génériques ne sont pas pris en charge.
<	Moins de
≤	Inférieur ou égal à
>	Plus grand que
≥	Supérieur ou égal à
commence par	Commence par
existe	Existe
ne sort pas	N'existe pas

Filtrer directement à partir des résultats de l'enregistrement

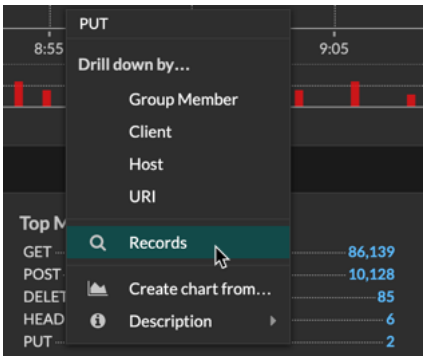
Vous pouvez sélectionner n'importe quelle entrée de champ affichée en mode tableau ou en affichage détaillé dans les résultats de votre enregistrement, puis cliquer sur l'opérateur contextuel pour ajouter le filtre. Les filtres sont affichés sous le résumé du graphique (à l'exception du champ de type d'enregistrement, qui est modifié dans le volet de gauche).



Recherche d'enregistrements dans le système ExtraHop

- Tapez un terme de recherche dans le champ de recherche global en haut de l'écran et cliquez sur Rechercher des enregistrements pour lancer une recherche sur tous les enregistrements stockés.

- Sur la page de présentation de l'équipement, cliquez sur **Enregistrements** pour démarrer une requête filtrée par cet équipement.
- Sur la page de présentation d'un groupe déquipements, cliquez sur **Afficher les enregistrements** pour démarrer une requête filtrée en fonction de ce groupe déquipements.
- À partir d'une carte de détection, cliquez sur Afficher les enregistrements pour lancer une requête filtrée avec les transactions associées à la détection.
- Cliquez sur l'icône Records à partir d'un widget graphique, comme illustré dans la figure suivante.



- Cliquez sur l'icône Records à côté d'une métrique détaillée après avoir exploré une métrique de niveau supérieur. Par exemple, après avoir étudié les réponses HTTP par serveur, cliquez sur l'icône Enregistrements pour créer une requête pour les enregistrements contenant une adresse IP de serveur spécifique.