# Enregistrements

Publié: 2023-09-19

Les enregistrements sont des informations structurées sur les transactions, les messages et les flux réseau qui sont générés et envoyés par le système ExtraHop à un magasin d'enregistrements. Une fois les enregistrements collectés et stockés, vous pouvez les consulter dans tout le système ExtraHop.

Les enregistrements sont collectés à deux niveaux de protocole : L3 et L7. Les enregistrements L3 (ou flux) montrent les transactions de la couche réseau entre deux appareils via le protocole IP. Les enregistrements L7 montrent les transactions basées sur les messages (comme ActiveMQ, DNS et DHCP), transactionnelles (comme HTTP, CIFS et NFS) et basées sur les sessions (comme SSL et ICA).

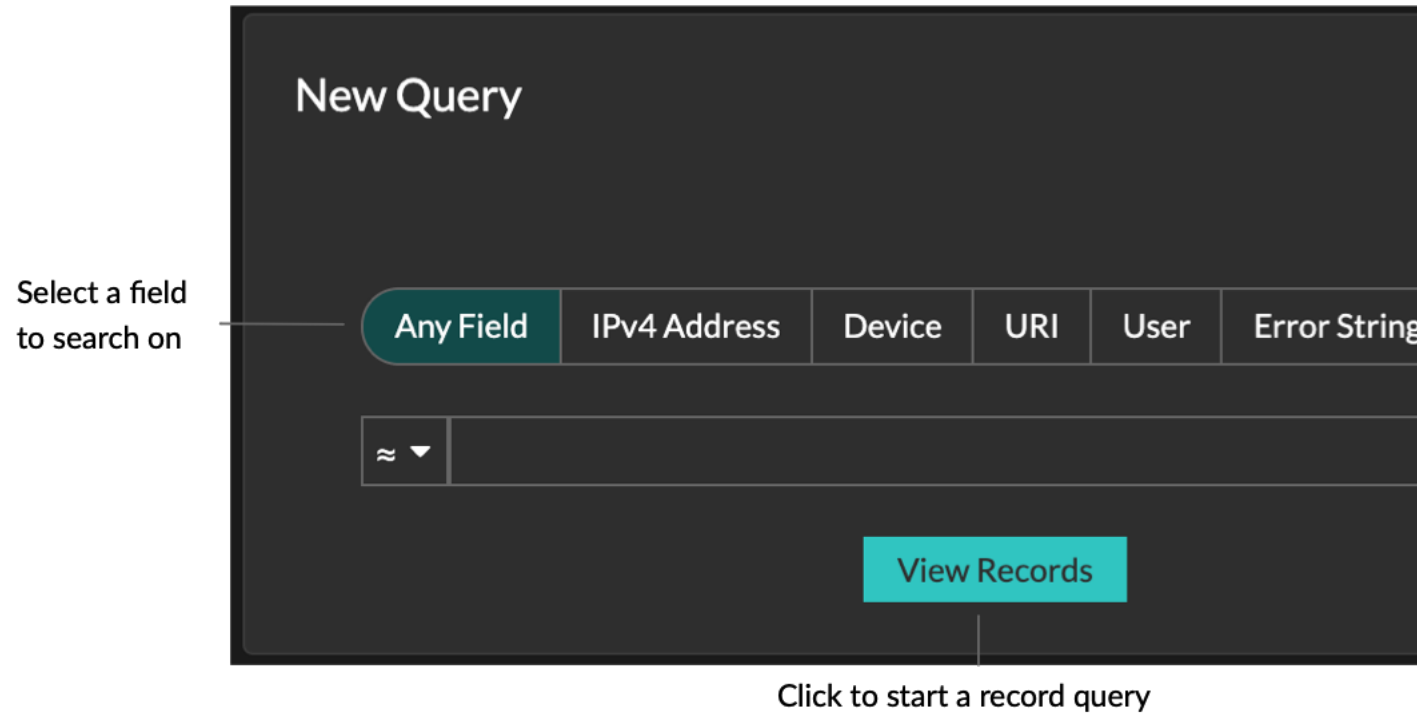
Par exemple, si vous avez cinquante erreurs HTTP 503, les transactions HTTP correspondantes contiendront des informations sur l'URL, le serveur web, le client qui a envoyé la requête, etc. Ces détails peuvent vous aider à identifier le problème sous-jacent.

**Avant de commencer**

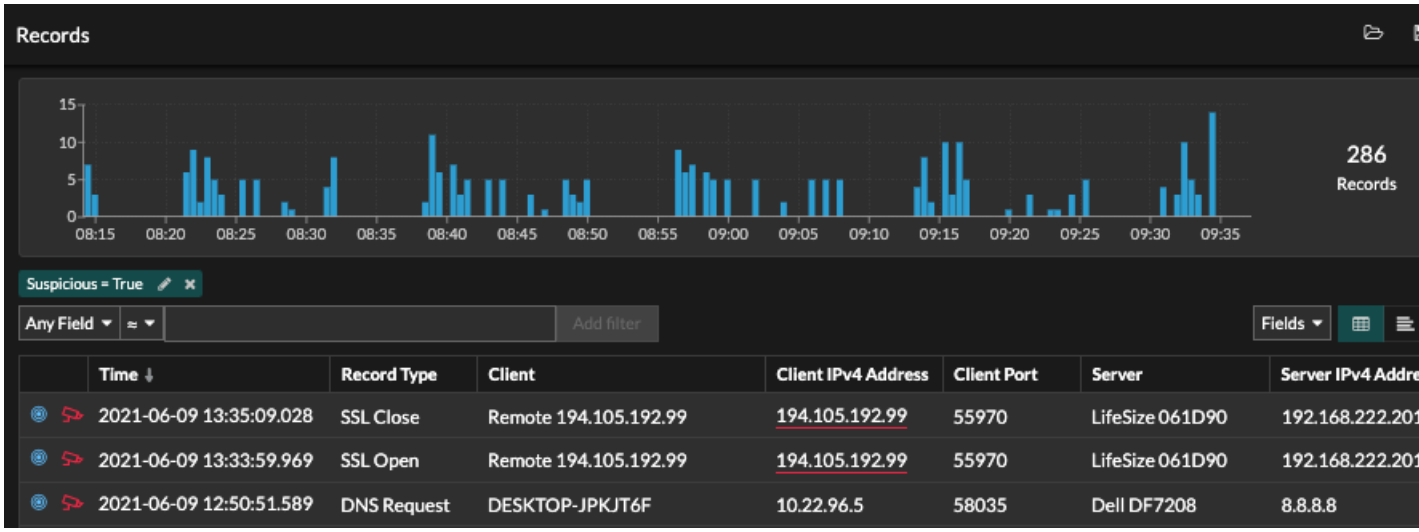
- Vous devez disposer d'un magasin d'enregistrements configuré, tel qu'un magasin d'enregistrements ExtraHop, Splunk ou Google BigQuery.
- Vous ne pouvez configurer qu'un seul magasin d'enregistrements pour le système ExtraHop.
- Votre système ExtraHop doit être configuré pour collecter et stocker des enregistrements de flux ou des enregistrements L7.

## Navigation dans les enregistrements

Cliquez sur **Enregistrements** dans le menu supérieur pour créer une nouvelle requête d'enregistrement. Sur la page Nouvelle requête, vous pouvez spécifier un filtre et un type d'enregistrement.




Les résultats s'affichent sur la page principale des enregistrements.




**Note:** Une requête peut aboutir à des millions d'enregistrements en fonction de l'intervalle de temps et des critères de filtrage. Si une requête dépasse le nombre maximum de résultats, un nombre tronqué d'enregistrements apparaît. (ExtraHop recordstore uniquement.)

Voici quelques façons d'explorer les résultats d'une requête d'enregistrement :

- Dans le tableau des enregistrements, survolez un intervalle de temps pour afficher le nombre d'enregistrements, ou cliquez-glissez sur le tableau pour réduire les résultats de la requête d'enregistrement à un intervalle de temps.

- Cliquez sur un nom d'hôte ou une adresse IP pour afficher les détails du périphérique 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 afficher les renseignements sur les menaces pour l'enregistrement.
- Cliquez sur une icône de paquet pour lancer une requête de paquet filtrée par cet enregistrement.
- Par défaut, les résultats de l'enregistrement apparaissent dans un tableau. Cliquez sur les icônes Table View ou Verbose View  pour basculer l'affichage de l'enregistrement.
- Une requête s'interrompt automatiquement si le nombre d'octets d'enregistrement analysés ou renvoyés est très élevé. En cas de pause, la requête affiche les enregistrements les plus récents. Cliquez sur **Continuer la requête** pour reprendre la recherche.
- Cliquez sur la liste déroulante **Champs** pour ajouter des informations supplémentaires à la vue des enregistrements.
- Dans la vue tableau, cliquez sur les en-têtes de colonne et faites-les glisser pour organiser les informations de l'enregistrement.
- Appliquez des filtres simplesou avancés pour trouver des problèmes potentiels, tels que des temps de traitement trop longs ou des tailles de réponse inhabituelles.

**Note:** Pour créer une requête d'enregistrement pour une mesure personnalisée, vous devez d'abord définir la relation d'enregistrement en liant la mesure personnalisée à un type d'enregistrement.

## Filtrez vos enregistrements à l'aide d'une simple requête

Vous pouvez filtrer les résultats de votre recherche d'enregistrements de plusieurs façons afin de trouver la transaction exacte que vous recherchez. Les sections ci-dessous décrivent chaque méthode et présentent des exemples avec lesquels vous pouvez commencer à vous familiariser.

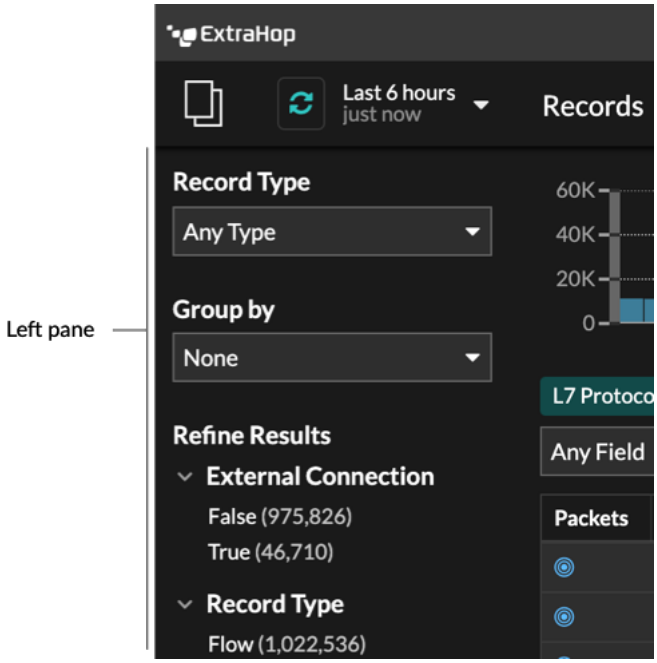
Si vous essayez de filtrer les enregistrements selon des critères simples (par exemple, si vous voulez toutes les transactions HTTP d'un seul serveur qui a généré des 404), vous pouvez créer une requête simple de l'une des manières suivantes :

- Ajouter un filtre ou affiner les résultats à partir du volet de gauche
- Ajouter un filtre à partir du tri-champ
- Ajouter un filtre directement à partir des résultats de l'enregistrement

Pour un filtrage complexe, voir Interroger les enregistrements avec un filtre avancé.

### Filtrer les résultats d'un enregistrement à partir du volet gauche

Lorsque vous cliquez sur **Enregistrements** dans le menu supérieur, tous les enregistrements disponibles pour l'intervalle de temps sélectionné s'affichent. Vous pouvez ensuite filtrer à partir du volet de gauche pour affiner vos résultats.




Le menu déroulant **Type d'enregistrement** 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 le magasin d'enregistrements.

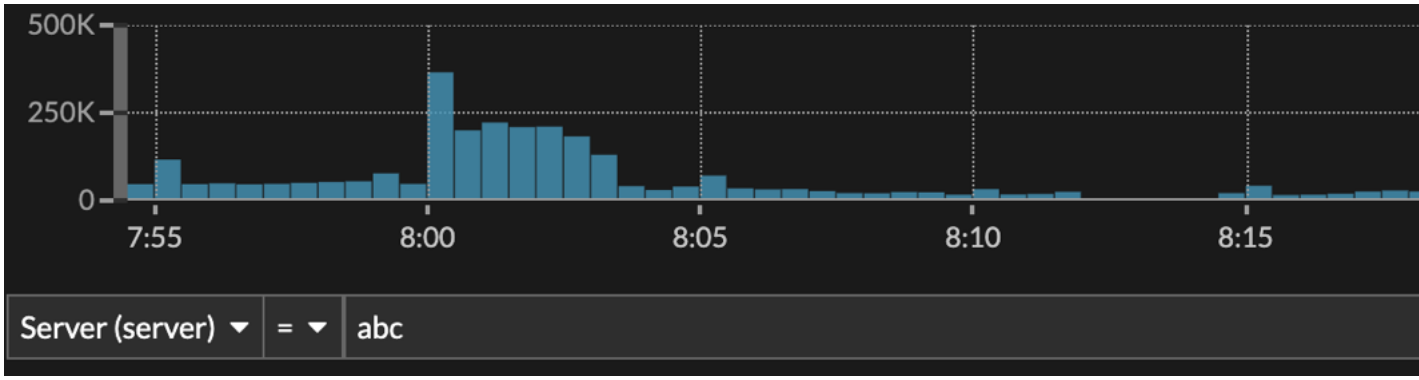
**Note:** Comme vous devez écrire un déclencheur pour collecter des enregistrements, vous devez pouvoir identifier le type de données que vous allez collecter. Il existe des types d'enregistrement intégrés, qui collectent tous les champs connus disponibles pour un protocole. Vous pouvez commencer par un type d'enregistrement intégré (tel que HTTP) et écrire un déclencheur pour collecter uniquement les champs de ce protocole qui vous intéressent (tels que l'URI et le code d'état). 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.

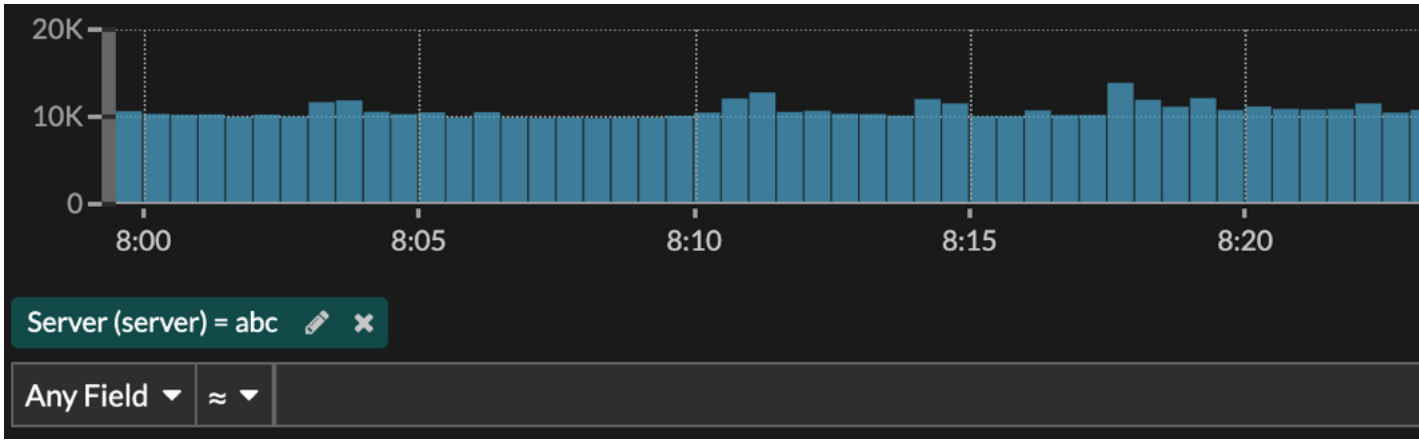
Le menu déroulant **Grouper par** vous donne une liste de champs par lesquels vous pouvez filtrer davantage le type d'enregistrement.

La section **Affiner les résultats** présente 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 d'un enregistrement à l'aide du tri-champ

Sélectionnez un champ dans la liste déroulante **N'importe quel champ** (tel que Serveur), sélectionnez un opérateur (tel que le signe égal (=)), puis tapez un nom d'hôte. Cliquez sur **Ajouter un** filtre et le filtre est ajouté au-dessus de la barre de filtre.




Vos résultats n'affichent que les enregistrements qui correspondent au filtre ; dans notre exemple, cela signifie que nous n'affichons que les résultats des transactions qui concernent le serveur nommé abc.

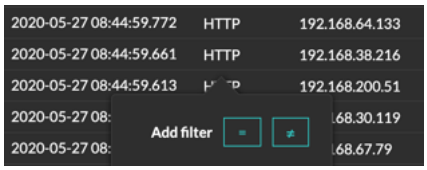
Les opérateurs suivants peuvent être sélectionnés en fonction du nom du champ sélectionné :

| Opérateur | Description |
|---|---|
| = | Égal à |
| ≠ | N'est pas égal à |
| ≈ | InclutSi les enregistrements sont stockés dans un magasin d'enregistrements ExtraHop, l'opérateur inclut les mots entiers délimités par des espaces et des signes de ponctuation . Par exemple, une recherche sur "www.extra" donnerait " www.extra.com" mais pas "www.extrahop.com". Pour tous les autres magasins d'enregistrements, l'opérateur includes correspond à des sous-chaînes de mots, y compris les espaces et la ponctuation . Par exemple, une recherche pour "www. |

| Opérateur | Description |
| --- | --- |
| | extra" correspondra à "www.extrahop.com", mais une recherche pour "www extra" ne correspondra pas à "www.extrahop.com".<br>Les<br>expressions rationnelles et les caractères génériques ne sont pas pris en charge<br>. |
| ≈/ | ExclusionsSi les<br>enregistrements sont stockés dans un magasin d'enregistrements ExtraHop, l'opérateur exclut les mots entiers délimités par des espaces et des signes de ponctuation. Par exemple, une recherche portant sur "extra" exclura "www.extra.com" mais pas "www.extrahop.com".<br>Pour tous les autres disquaires, l'opérateur exclut les sous-chaînes de mots, y compris les espaces et la ponctuation.<br>Par exemple, une recherche sur<br>"www.extra" exclura "www.extrahop.com", mais une recherche sur "www extra" n'exclura pas "www.extrahop.com".<br>Les expressions rationnelles et les caractères génériques ne sont pas pris en charge<br>. |
| < | Moins que |
| ≤ | Inférieur ou égal à |
| > | Supérieur à |
| ≥ | Supérieur ou égal à |
| commence par | Commence par |
| existe | Existe |
| n'existe pas | N'existe pas |

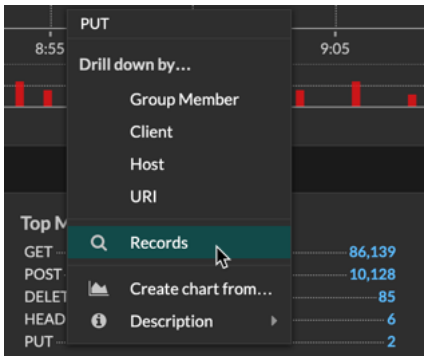
### Filtrer directement à partir des résultats de l'enregistrement

Vous pouvez sélectionner n'importe quelle entrée de champ affichée en vue tableau ou en vue verbeuse 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 (sauf pour le champ du type d'enregistrement, qui est modifié dans le volet gauche).



## Recherche d'enregistrements dans le système ExtraHop

- Saisissez un terme de recherche dans le champ de recherche global situé en haut de l'écran et cliquez sur Rechercher des enregistrements pour lancer une requête sur tous les enregistrements stockés.
- Dans la page de présentation d'un appareil, cliquez sur **Enregistrements** pour lancer une recherche filtrée par cet appareil.
- Dans la page de présentation d'un groupe de dispositifs, cliquez sur **Afficher les enregistrements** pour lancer une requête filtrée par ce groupe de dispositifs.
- Dans une fiche de détection, cliquez sur Afficher les enregistrements pour lancer une requête filtrée sur les transactions associées à la détection.
- Cliquez sur l'icône Enregistrements à partir d'un widget graphique, comme illustré dans la figure suivante.




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