Requête pour les enregistrements stockés

Publié: 2024-08-09

Vous pouvez interroger les enregistrements stockés dans l'espace de stockage des enregistrements à l'aide d'une recherche standard ou à l' aide de l'assistant de recherche AI.

- En savoir plus sur l'interrogation d'enregistrements à l'aide d'une recherche standard.
- En savoir plus sur la recherche d'enregistrements avec AI Search Assistant.
- Pour savoir comment rechercher un enregistrement spécifique, consultez notre procédure pas à pas pour Découvrir les ressources Web manquantes.
- Vous pouvez également automatiser cette tâche via l' API REST.

Prochaines étapes

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.

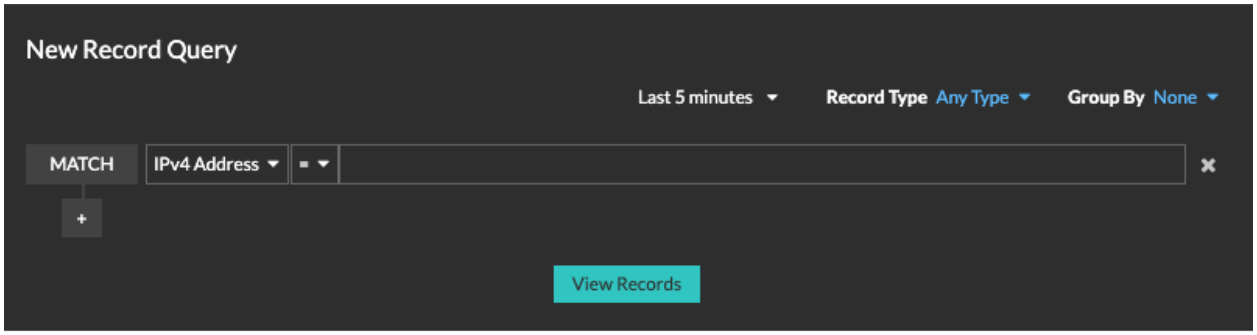
Interroger des enregistrements avec une recherche standard

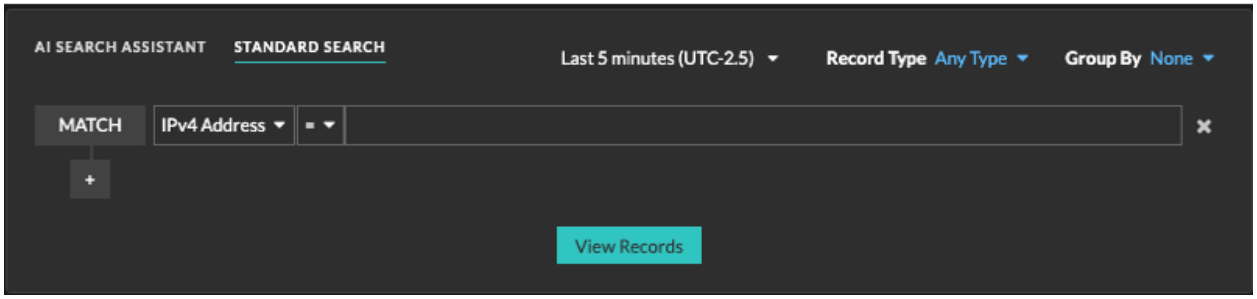
La page Enregistrements vous permet de créer un filtre complexe pour rechercher des enregistrements.

Voici quelques informations importantes à propos des requêtes d'enregistrement avec la recherche standard :

- Vous pouvez spécifier plusieurs critères à l'aide des opérateurs OR (Match Any), AND (Match All) et NOT.
- Vous pouvez regrouper les filtres et les imbriquer à quatre niveaux au sein de chaque groupe.
- Vous pouvez modifier un groupe de filtres après l'avoir créé pour

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Disques**.
   Si l'assistant de recherche AI n'est pas activé, la section Requête d'un nouvel enregistrement s' affiche.
   Si AI Search Assistant est activé, cliquez sur **Recherche standard**.



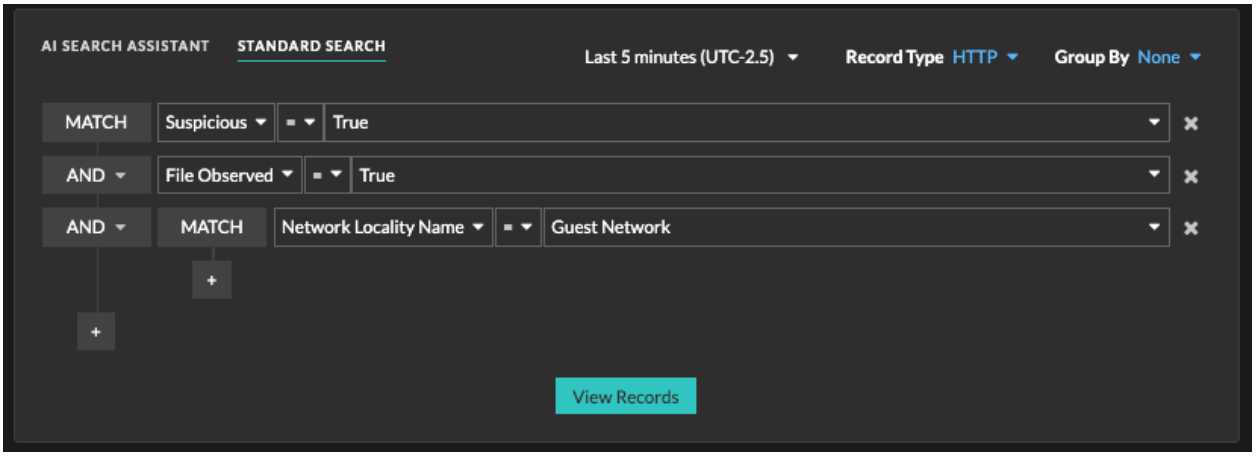


3. Sélectionnez l'intervalle de temps que vous souhaitez rechercher.

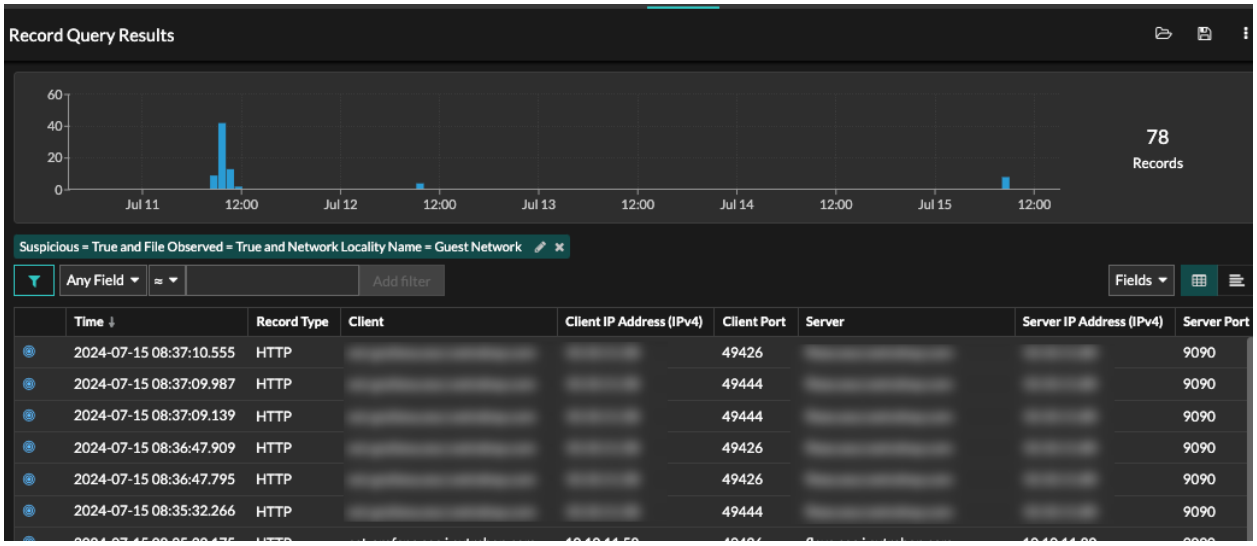
   L'intervalle de temps que vous sélectionnez modifie l'heure définie dans sélecteur de temps global.
4. À partir du **Type d'enregistrement** menu déroulant, sélectionnez un ou plusieurs types d'enregistrements que votre système ExtraHop est configuré pour collecter et stocker.
5. À partir du **Regrouper par** menu déroulant, sélectionnez une option pour spécifier la manière dont vous souhaitez regrouper les résultats. Les options affichées sont associées aux types d'enregistrement que vous avez sélectionnés.

   Par exemple, si vous regroupez les enregistrements HTTP par client, le tableau des résultats affiche les clients trouvés dans les transactions d'enregistrement, classés selon le nombre de fois que ce client a été trouvé.
6. Dans le menu déroulant des critères de filtre (la valeur par défaut est Adresse IPv4), sélectionnez les premiers critères auxquels vous souhaitez que le filtre corresponde. Les options affichées sont associées aux types d'enregistrement que vous avez sélectionnés.
7. Optionnel : Cliquez sur l'icône plus et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

   Un nouveau groupe de filtres ajoute des critères au résultat du filtre d'origine. Par exemple, si vous recherchez des transactions HTTP suspectes et contenant des fichiers, vous pouvez ajouter un groupe de filtres pour limiter les résultats aux enregistrements associés à une localité réseau spécifiée.



8. Cliquez **Afficher les enregistrements**.
   Les résultats des enregistrements sont affichés sur la page principale des enregistrements.



Prochaines étapes

- Tu peux afficher et explorer les résultats des requêtes d'enregistrement.
- Tu peux affinez votre filtre de requête d'enregistrement.
- Vous pouvez cliquer sur l'icône Enregistrer en haut à droite de la page pour enregistrer votre filtre pour une prochaine fois.
- Vous pouvez cliquer sur l'icône d'un paquet à côté d'un enregistrement pour démarrer un requête de paquet qui est filtré par cet enregistrement ou cliquez sur le lien de requête en bas du tableau pour lancer une requête par paquet pour tous les enregistrements affichés.

Interrogez des enregistrements avec AI Search Assistant

L'assistant de recherche AI vous permet de rechercher des enregistrements contenant des questions rédigées dans un langage naturel courant afin de créer rapidement des requêtes complexes par rapport à la création d'une requête de recherche standard avec les mêmes critères.

Par exemple, si vous recherchez « Y a-t-il eu des transactions HTTP suspectes avec des fichiers au cours des 7 derniers jours ? » , la requête suivante de l'assistant de recherche AI s'affiche :

```
Time Interval = Last 2 days and Record Type = [HTTP]
Suspicious = True and File Observed = True
```

Voici quelques éléments à prendre en compte lors de la recherche d'appareils avec AI Search Assistant :

- Les invites sont associées aux mêmes critères de filtre d'enregistrement que ceux que vous spécifiez lors de la création d'une recherche standard.
- Les invites peuvent inclure des plages temporelles absolues et relatives, telles que « Afficher le trafic avec Potential SQLi au cours des 7 derniers jours ». L'année en cours est appliquée si une année n' est pas incluse pour une date.
- Les instructions doivent être aussi claires et concises que possible et nous vous recommandons d'essayer d' écrire quelques variantes pour optimiser vos résultats.
- Le système ExtraHop peut ne pas être en mesure de traiter une requête contenant des demandes d'informations d'enregistrement qui ne sont pas incluses dans les filtres disponibles.
- Le système ExtraHop peut conserver les instructions des utilisateurs à des fins d'amélioration du produit ; nous vous recommandons de ne pas inclure de données exclusives ou confidentielles dans vos invites.
- Vous pouvez modifier les critères du filtre de requête pour affiner les résultats de recherche.

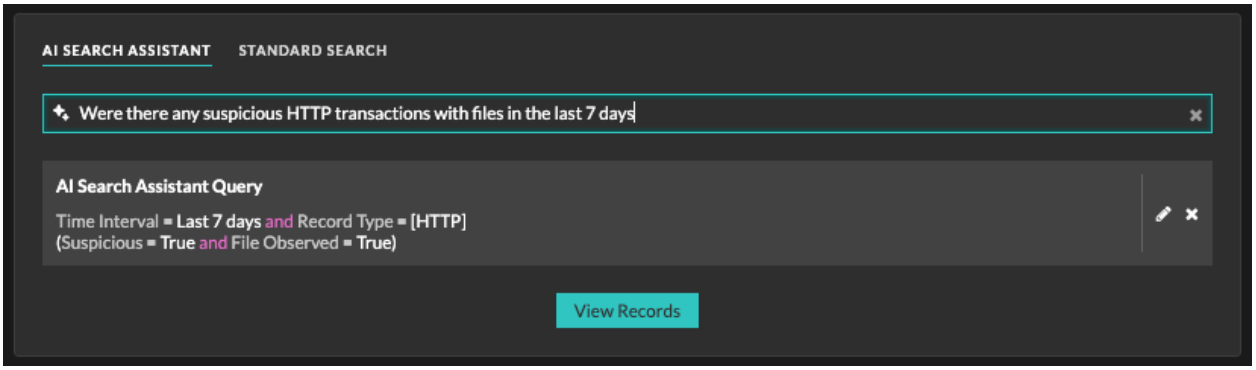
Avant de commencer

- Votre système ExtraHop doit être connecté à ExtraHop Cloud Services.
- L'assistant de recherche AI doit être activé par votre administrateur ExtraHop.

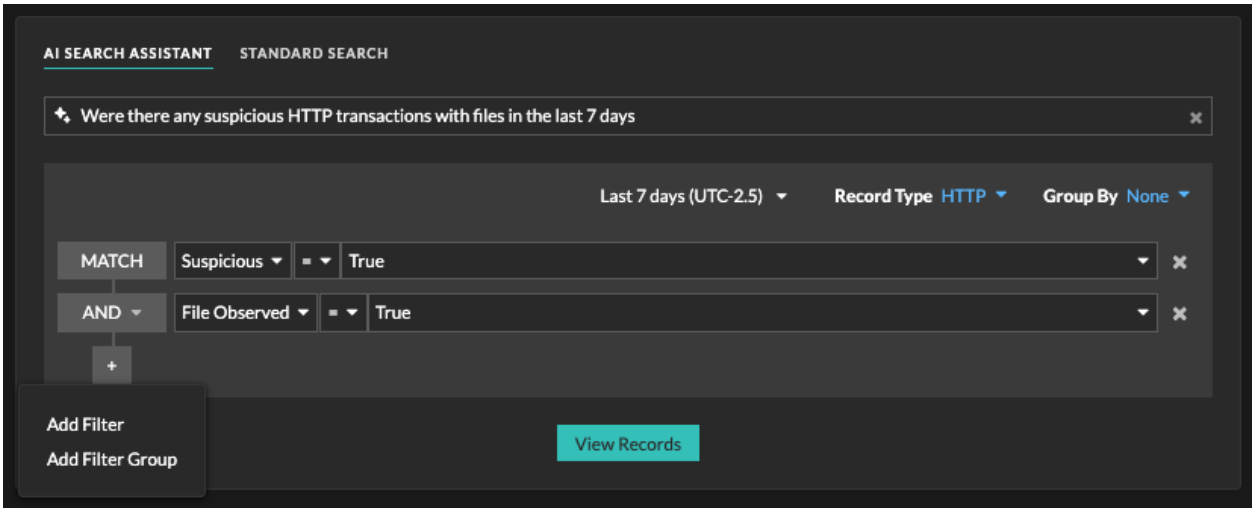
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Disques**.
3. Écrivez une invite dans le champ AI Search Assistant et appuyez sur ENTER.

   Conseil Cliquez sur le champ d'invite de recherche pour sélectionner une requête récente ou une recherche suggérée.

   Le filtre de requête AI Search Assistant s'affiche.



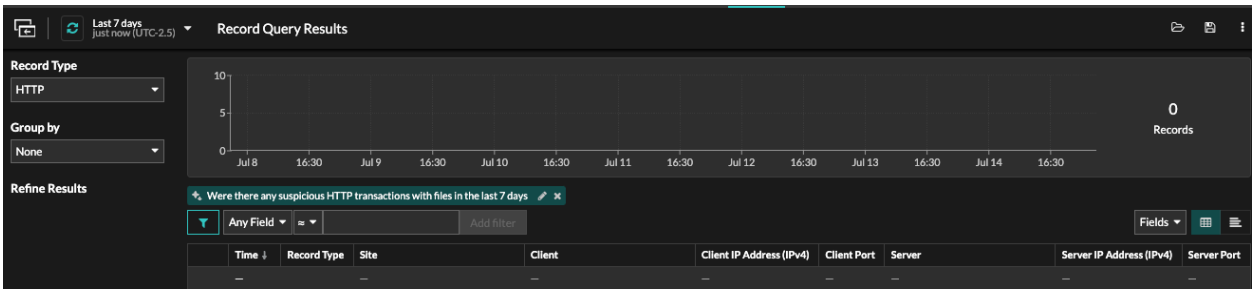
4. Optionnel : Dans la section Requête de l'assistant de recherche AI, cliquez sur l'icône de modification pour affiner les critères de votre filtre de requête.



   a) Dans la rangée supérieure, modifiez l'intervalle de temps, **Type d'enregistrement** ou **Grouper par** options.
   b) Cliquez sur l'icône plus et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

      Un nouveau groupe de filtres ajoute des critères au résultat du filtre d'origine. Par exemple, si vous recherchez des enregistrements HTTP suspects et contenant des fichiers, vous pouvez ajouter un groupe de filtres pour limiter les résultats aux enregistrements associés à une localité réseau spécifiée.
   c) Cliquez **Terminé**.
5. Cliquez **Afficher les enregistrements**.

Les résultats des enregistrements sont affichés sur la page principale des enregistrements. Le nom d'affichage du filtre AI Search Assistant est l'invite que vous avez saisie et s'affiche au-dessus des trois champs.



Prochaines étapes

- Tu peux afficher et explorer les résultats des requêtes d'enregistrement.
- Tu peux affinez votre filtre de requête d'enregistrement.
- Vous pouvez cliquer sur l'icône Enregistrer en haut à droite de la page pour enregistrer votre filtre pour une prochaine fois.
- Vous pouvez cliquer sur l'icône d'un paquet à côté d'un enregistrement pour démarrer requête de paquet qui est filtré par cet enregistrement ou cliquez sur le lien de requête en bas du tableau pour lancer une requête par paquet pour tous les enregistrements affichés.