

Création d'un groupe d'équipements en fonction de l'heure de découverte

Publié: 2023-10-01

Le système ExtraHop détecte automatiquement les appareils qui envoient et reçoivent du trafic par câble. Outre les groupes intégrés qui détectent les appareils ajoutés au cours des dernières 24 heures et des 7 derniers jours, vous pouvez créer un groupe d'appareils dynamique personnalisé qui ajoute automatiquement les appareils découverts pendant un intervalle de temps spécifique.

Pour en savoir plus sur les différents formats d'heure, voir [Formats temporels de découverte](#).

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**, puis cliquez sur **Groupes d'appareils** dans le volet de gauche.
3. Dans le coin supérieur droit, cliquez sur **Créer un groupe d'appareils**.
4. Dans le **Nom du groupe** champ, saisissez le nom du groupe d'équipements.
5. Dans le **Description du groupe** champ, saisissez toute information pouvant servir de référence pour la plage de temps de découverte que vous spécifiez.
6. Dans le Type de groupe section, cliquez **Dynamique**.
La section Critères de filtrage apparaît.
7. Sélectionnez un opérateur de correspondance dans la liste déroulante :

Option	Description
Tout faire correspondre	Filtre uniquement les appareils qui répondent à tous les critères de filtre spécifiés.
Faites correspondre n'importe lequel	Filtre les appareils qui répondent à l'un des critères de filtre spécifiés.
Ne correspond à aucune	Filtre les appareils qui ne répondent à aucun des critères de filtre spécifiés.

8. Dans la liste déroulante des catégories, cliquez sur **L'heure de la découverte**.


9. Sélectionnez un opérateur de recherche dans la liste déroulante :

Option	Description
=	Filtre les appareils qui correspondent exactement à l' intervalle de temps de découverte.
↓	Filtre les appareils qui ne correspondent pas exactement à l' intervalle de découverte.

10. Dans le **De (à l'heure d'Unix)** dans ce champ, effectuez l'une des étapes suivantes :

- Laissez ce champ vide pour indiquer la première fois que votre système a reçu du trafic.
- Entrez une date fixe dans le [Format d'heure Unix Epoch](#) ou saisissez une valeur dans [format de l'heure relative](#).

11. Dans le **Jusqu'à (à l'heure d'Unix)** champ, en suivant les étapes suivantes :

- Laissez ce champ vide pour indiquer le cadeau.
-  **Important:** Si le champ From est vide, vous ne pouvez pas laisser le champ Until vide et vous devez saisir un format d'heure fixe ou relatif.
- Entrez une date fixe dans le [Format d'heure Unix Epoch](#) ou saisissez une valeur dans [format de l'heure relative](#).

 **Important:** Le format du champ Until doit correspondre au format du champ From.

12. Cliquez **Enregistrer**.

Prochaines étapes

- [Créez un graphique dans votre tableau de bord](#) et sélectionnez votre nouveau groupe d'équipements comme source
- [Filtrer les connexions à la carte d'activités par groupe](#)

Formats temporels de découverte

Lors de la création d'un groupe de périphériques personnalisé pour les appareils découverts pendant un intervalle de temps spécifique, les critères de découverte doivent être exprimés en temps Unix Epoch ou dans une plage de temps relative.

Unix Epoch Time

Les dates spécifiques doivent être converties en heure Unix Epoch. Cette conversion permet de réduire les écarts entre les fuseaux horaires et les différents horaires des serveurs.

Vous pouvez convertir votre date en horodateur à l'aide d'un outil en ligne, tel que <https://www.epochconverter.com/>. Après avoir créé l'horodateur Unix Epoch, copiez-le et collez-le dans les champs FROM et UNTIL correspondant aux critères de votre groupe d'équipements. L'horodateur doit inclure des millisecondes. Par exemple, pour spécifier le 16 août 2018 à 18 h 16 min 51 s, entrez 1534443411000, comme le montre la figure suivante.

Mon	Day	Yr	Hr	Min	Sec		
8	/	16	/	2018	18	:	16 : 51

GMT

Epoch timestamp: 1534443411

Timestamp in milliseconds: 1534443411000

Human time (GMT): Thursday, August 16, 2018 6:16:51 PM

Human time (your time zone): Thursday, August 16, 2018 11:16:51 AM GMT-07:00

Exemple d'entrée d'heure Unix Epoch valide

1534238700000

Exemple d'entrée d'heure Unix Epoch non valide

1534238700000ms

Plage de temps relative

Pour spécifier un point dans le temps par rapport à un autre point, par exemple il y a une semaine, vous devez ajouter un signe moins à une valeur, puis ajouter l'une des unités de temps suivantes : y, M, w, d, h, m, ms. Par exemple, tapez `-1 w` à préciser il y a une semaine. Vous ne pouvez pas spécifier un intervalle de temps futur. Les plages de temps relatives doivent commencer par une valeur négative.

Le tableau suivant indique les unités de temps prises en charge.

Unité de temps	Suffixe d'unité
Année	y
Mois	M
Semaine	w
Journée	d
Heure	h

Unité de temps	Suffixe d'unité
Minutes	m
Deuxième	s
Milliseconde	ms

Exemple de saisie d'heure relative valide

-12h

Exemples de saisie d'heure relative non valide

12h

-12H

Exemples de critères relatifs au temps de découverte

Voici des exemples de critères pour différentes plages de temps de découverte.

Du 1 janvier 2018 12:23:23:00 UTC à aujourd'hui

GROUP TYPE

- Static (add devices manually)
- Dynamic (specify filter criteria)

FILTER CRITERIA

January 1st 2018, 20:23:23.000 UTC

Match All ▾

Discovery Time ▾ = ▾ 1514838203000 ✔ Until (In Unix time)... ✕

Add Filter
Add Filter Group

D'il y a un mois à il y a une minute

GROUP TYPE

- Static (add devices manually)
- Dynamic (specify filter criteria)

FILTER CRITERIA

a month ago

a minute ago

Match All ▾

Discovery Time ▾ = ▾ -1M ✔ -1m ✔ ✕

Add Filter
Add Filter Group