

# Créer un groupe de périphériques en fonction de l'heure de découverte

Publié: 2023-09-19

Le système ExtraHop découvre automatiquement les périphériques qui envoient et reçoivent du trafic sur le réseau. Outre les groupes intégrés qui découvrent les périphériques ajoutés au cours des 24 dernières heures et des 7 derniers jours, vous pouvez créer un groupe de périphériques dynamique personnalisé qui ajoute automatiquement les périphériques découverts au cours d'un intervalle de temps spécifique.

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

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

Option	Description
Match All (Tout)	Filtre uniquement les dispositifs qui correspondent à tous les critères de filtrage spécifiés.
Correspondre à n'importe quel	Filtre les dispositifs qui correspondent à l'un des critères de filtrage spécifiés.
Correspondre à aucun	Filtre les dispositifs qui ne correspondent à aucun des critères de filtrage spécifiés.

8. Dans la liste déroulante des catégories, cliquez sur **Temps de découverte**.


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

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

10. Dans le champ **From (In Unix time)**, effectuez l'une des opérations suivantes :

- Laissez ce champ vide pour indiquer la première fois que votre système a reçu du trafic.
- Saisissez une date fixe dans le [format Unix Epoch time](#) ou saisissez une valeur dans le [format relative time](#).

11. Dans le champ **Jusqu'à (en heure Unix)**, effectuez l'une des étapes suivantes :

-  **Important:** Si le champ From est vide, vous ne pouvez pas laisser le champ Until vide et vous devez entrer un format de temps fixe ou relatif

- Entrez une date fixe dans le [format Unix Epoch](#) ou saisissez une valeur dans le [format d'heure relative](#)

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

12. Cliquez sur **Enregistrer**.

#### Prochaines étapes

- [Créer un graphique dans votre tableau de bord](#) et sélectionnez votre nouveau groupe de dispositifs comme source.
- [Filtrer les connexions de la carte d'activité par groupe](#)

## Formats de l'heure de découverte

Lors de la création d'un groupe de dispositifs personnalisé pour les dispositifs découverts au cours d'un intervalle de temps spécifique, les critères de temps de découverte doivent être soit en heure Unix, soit dans une plage de temps relative.

### Heure d'époque Unix

Les dates spécifiques doivent être converties en heure Unix Epoch. Cette conversion permet d'atténuer les divergences entre les fuseaux horaires et les heures des différents serveurs.

Vous pouvez convertir votre date en horodatage à l'aide d'un outil en ligne, tel que <https://www.epochconverter.com/>. Après avoir créé l'horodatage Unix Epoch, copiez et collez l'horodatage dans les champs FROM et UNTIL de vos critères de groupe de dispositifs. L'horodatage doit inclure les millisecondes. Par exemple, pour spécifier le 16 août 2018, 6:16:51 PM, entrez 1534443411000, comme indiqué dans la figure suivante.

Mon	Day	Yr	Hr	Min	Sec			
8	/	16	/	2018	18	:	16 : 51	
							GMT	Human date to Timestamp

**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'une entrée valide de l'heure Unix Epoch

1534238700000

### Exemple d'une entrée de temps Unix Epoch non valide

1534238700000ms

### Plage de temps relative

Pour spécifier un point dans le temps par rapport à un autre point dans le temps, 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 `-1w` pour spécifier il y a une semaine. Vous ne pouvez pas spécifier une période future. Les plages de temps relatives doivent commencer par une valeur négative.

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

Unité de temps	Suffixe de l'unité
Année	y
Mois	M
Semaine	w

Unité de temps	Suffixe de l'unité
Jour	d
Heure	h
Minute	m
seconde	s
Milliseconde	ms

### Exemple d'une entrée valide de temps relatif

-12h

### Exemples de saisie de l'heure relative non valide

12h

-12H

### Exemples de critères pour la période de recherche

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

#### Du 1er 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