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

Publié: 2024-11-04

Le système ExtraHop détecte automatiquement les appareils qui envoient et reçoivent du trafic via le 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 au cours d'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. Dans le menu supérieur, cliquez sur **Actifs** puis cliquez sur **Groupes d'appareils** graphique.
3. Dans le coin supérieur droit, cliquez sur **Créer un groupe d'appareils**.
4. Dans le **Nom du groupe**dans ce 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 sur **Dynamique**.
   La section Critères de filtre 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 filtrage spécifiés.
Faites correspondre n'importe lequel	Filtre les appareils qui correspondent à l'un des critères de filtrage spécifiés.
Aucun match	Filtre les appareils qui ne correspondent à aucun des critères de filtrage 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 temps de découverte.

10. Dans le **De (à l'heure d'Unix)** champ, effectuez l'une des étapes suivantes :
    - Laissez ce champ vide pour spécifier la première fois que votre système a reçu du trafic.
    - Entrez une date fixe dans Format horaire Unix Epoch ou saisissez une valeur dans format temporel relatif.
11. Dans le **Jusqu'à (à l'heure d'Unix)** champ, effectuez les étapes suivantes :
    - Laissez ce champ vide pour spécifier le cadeau.

      Important: Si le champ De est vide, vous ne pouvez pas laisser le champ Jusqu'à vide et vous devez entrer un format d'heure fixe ou relatif.
    - Entrez une date fixe dans Format horaire Unix Epoch ou saisissez une valeur dans format temporel relatif.

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 dproximatif d'équipements comme source
- Filtrer les connexions des cartes dactivités par groupe

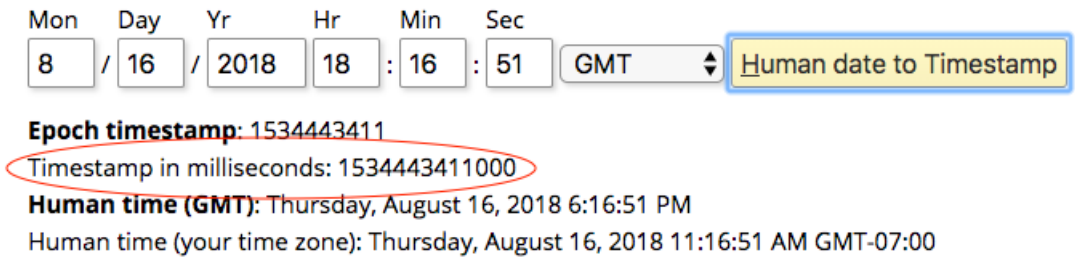
Formats temporels de découverte

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 déquipements. 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.



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

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

Exemple de saisie d'heure relative valide

-12h

Exemples de saisie d'heure relative non valide

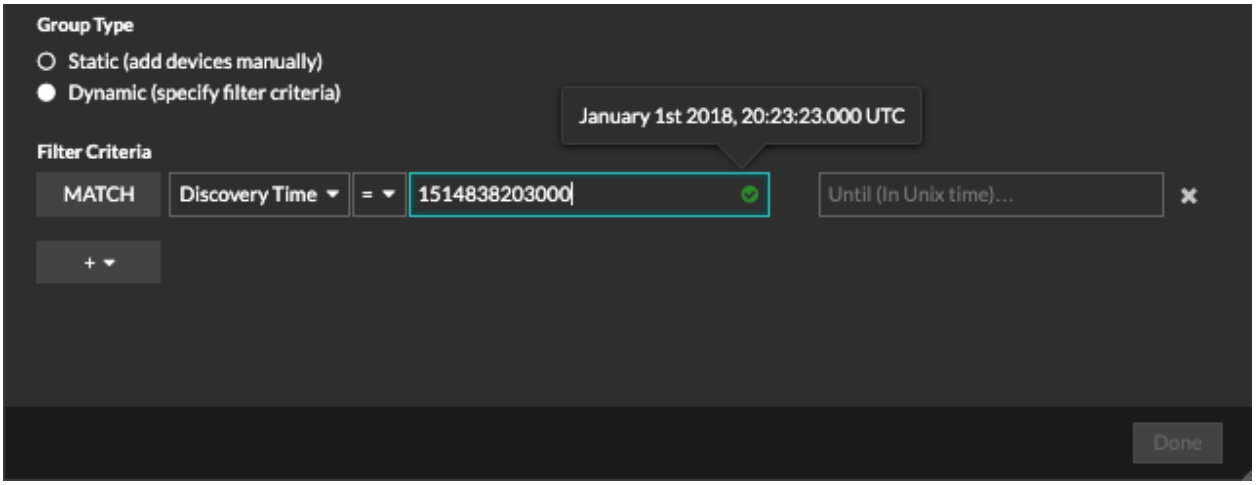
12h

-12H

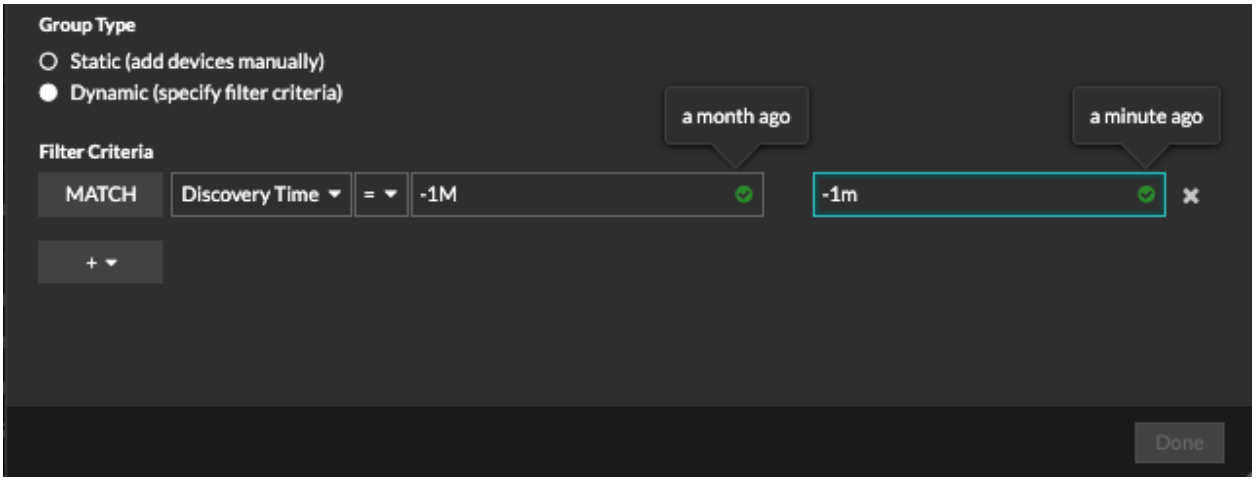
Exemples de critères relatifs au temps de découverte

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

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



D'il y a un mois à il y a une minute


Group Type
Static (add devices manually)
Dynamic (specify filter criteria)
a month ago
a minute ago
Filter Criteria
MATCH
Discovery Time
=
-1M
-1m
+
Done