

Création d'un groupe déquipements

Publié: 2023-11-14


Vous pouvez créer des groupes d'équipements dynamiques et statiques. Les groupes dynamiques ajoutent automatiquement au groupe tous les appareils répondant aux critères spécifiés, tandis que les groupes statiques vous obligent à ajouter manuellement chaque équipement.

Création d'un groupe d'équipements dynamiques

Vous pouvez créer des groupes d'équipements dynamiques avec des filtres complexes, qui vous permettent de définir plusieurs critères et de créer des groupes de critères imbriqués.



Conseil Vous pouvez créer rapidement un groupe d'appareils dynamique à partir d'une liste filtrée d'appareils sur la page Appareils. Cliquez **Créer un groupe dynamique** depuis le coin supérieur droit.

Vous pouvez également créer un groupe d'équipements dynamique à partir d'un groupe de périphériques intégré. Sur la page Appareils, cliquez sur un rôle ou un protocole, mettez à jour les critères de filtre, puis cliquez sur Enregistrer  dans le coin supérieur droit.

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** dans le volet de gauche.
3. Cliquez **Créer un groupe d'appareils**.
4. Dans le **Nom du groupe** champ, saisissez un nom descriptif pour identifier le groupe
5. Optionnel : À partir du **Rédacteurs** liste déroulante, sélectionnez les utilisateurs dotés de droits d'écriture limités qui peuvent modifier ce groupe déquipements. Ce privilège global doit être activé dans les paramètres d'administration.
 - La liste affiche uniquement un nombre limité d'utilisateurs en écriture possédant des comptes actifs.
 - Seul un utilisateur disposant d'une autorisation de modification pour un groupe déquipements peut ajouter d'autres utilisateurs d'écriture limités.
6. Optionnel : Dans le **Descriptif** champ, ajoutez des informations sur ce groupe déquipements.
7. Dans le Type de groupe section, cliquez **Dynamique**.
8. Dans le Critères de filtrage section, cliquez **Tout faire correspondre** puis sélectionnez l'un des opérateurs de correspondance suivants dans la liste déroulante :

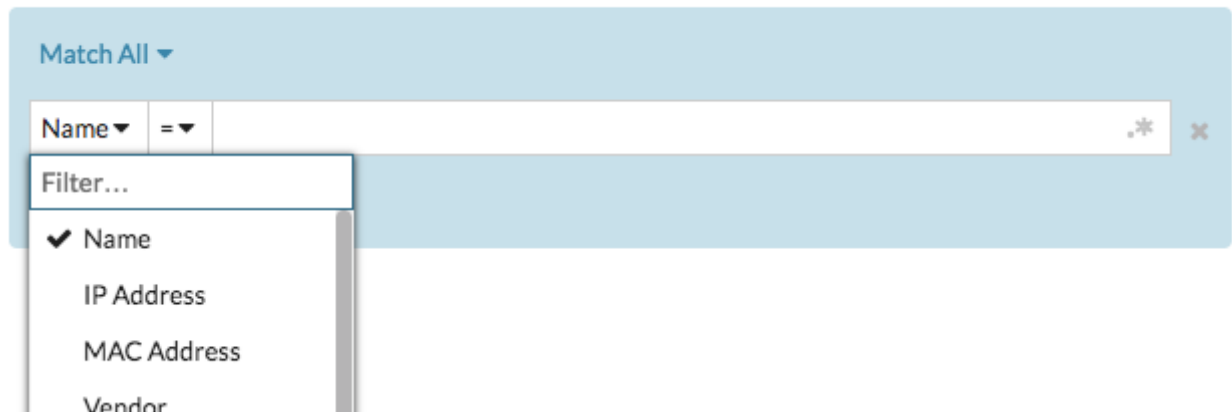
FILTER CRITERIA



Option	Description
Tout faire correspondre	Filtre uniquement les appareils qui répondent à tous les critères spécifiés.
Faites correspondre n'importe lequel	Filtre les appareils qui répondent à l'un des critères spécifiés.
Aucune correspondance	Filtre les appareils qui ne répondent à aucun des critères spécifiés.

9. Cliquez **Nom** et sélectionnez l'une des catégories suivantes dans la liste déroulante :

FILTER CRITERIA



Option	Description
Nom	Filtre les appareils en fonction du nom de l'équipement découvert. Par exemple, le nom d'un équipement découvert peut inclure l'adresse IP ou le nom d'hôte.
Adresse MAC	Filtre les appareils en fonction de l'adresse MAC de l'équipement.
Adresse IP	Filtre les appareils par adresse IP au format de bloc IPv4, IPv6 ou CIDR.
Site	Filtre les appareils associés à un site connecté. Console uniquement.
Heure de découverte	Filtre les appareils détectés automatiquement par le système ExtraHop dans l'intervalle de temps spécifié. Pour plus d'informations, voir Création d'un groupe d'équipements en fonction de l'heure de découverte .
Niveau d'analyse	Filtre les appareils par niveau d'analyse, ce qui détermine les données et les mesures collectées pour un appareil. Vous ne pouvez pas créer de groupe d'équipements dynamique pour les appareils filtrés par niveau d'analyse.
Modèle	Filtre les appareils par marque et nom de modèle. Les conseils suivants peuvent vous aider à trouver le modèle d'équipement que vous souhaitez : <ul style="list-style-type: none"> • Sélectionnez l'opérateur de correspondance exact (=) pour afficher une liste déroulante des modèles et ensembles de modèles existants. • Sélectionnez l'opérateur de correspondance exact (=), puis sélectionnez Modèles personnalisés pour filtrer tous les appareils affectés à un ensemble de modèles personnalisé.

Option	Description
Activité	<p>Filtre les appareils en fonction de l'activité du protocole associée à l'équipement. Par exemple, si vous sélectionnez Serveur HTTP, vous renvoyez les appareils avec des métriques de serveur HTTP et tout autre équipement dont le rôle d'équipement est défini sur Serveur HTTP.</p> <p>Filtre également les appareils qui ont accepté ou initié une connexion externe, ce qui peut vous aider à déterminer si les appareils sont impliqués dans des activités suspectes.</p>
Compte cloud	Filtre les appareils en fonction du compte de service cloud associé à l'équipement.
ID d'instance Cloud	Filtre les appareils en fonction de l'ID d'instance cloud associé à l'équipement.
Type d'instance cloud	Filtre les appareils en fonction du type d'instance cloud associé à l'équipement.
Valeur élevée	Filtre les appareils considérés comme ayant une valeur élevée parce qu'ils fournissent des services d'authentification, prennent en charge des services essentiels sur votre réseau ou sont spécifiés par l'utilisateur comme ayant une valeur élevée.
Actuellement actif	Filtre les appareils en fonction de l'activité observée sur un équipement au cours des 30 dernières minutes.
Type de localité du réseau	Filtre les appareils en fonction de toutes les localisations du réseau interne ou externe.
Nom de la localité du réseau	Filtre les appareils par nom de localité du réseau.
Rôle	Filtre les appareils en fonction du rôle d'équipement attribué, tel que passerelle, pare-feu, équilibreur de charge et serveur DNS.
Logiciel	Filtre les appareils en fonction du logiciel du système d'exploitation détecté sur l'équipement.
Sous-réseau	Filtre les appareils en fonction du sous-réseau associé à l'équipement.
Balise	Filtre les appareils en fonction de balises d'équipement définies par l'utilisateur.
Fournisseur	Filtre les appareils en fonction du nom du fournisseur de l'équipement, tel que déterminé par la recherche de l'identifiant unique de l'organisation (OUI).
Cloud privé virtuel	Filtre les appareils en fonction du VPC associé à l'équipement.
VLAN	Filtre les appareils en fonction de la balise VLAN de l'équipement. Les informations VLAN sont extraites des balises VLAN, si le processus de

Option	Description
	mise en miroir du trafic les conserve sur le port miroir. Disponible uniquement si <code>devices_accross_vlans</code> le réglage est défini sur <code>False</code> dans le fichier de configuration en cours d'exécution.
Nom CDP	Filtre les appareils en fonction du nom CDP attribué à l'équipement.
Nom de l'instance Cloud	Filtre les appareils en fonction du nom d'instance cloud attribué à l'équipement.
Nom personnalisé	Filtre les appareils en fonction du nom personnalisé attribué à l'équipement.
Nom DHCP	Filtre les appareils en fonction du nom DHCP attribué à l'équipement.
Nom DNS	Filtre les appareils en fonction de tout nom DNS attribué à l'équipement.
Nom NetBIOS	Filtre les appareils en fonction du nom NetBIOS attribué à l'équipement.

10. Sélectionnez l'un des opérateurs suivants dans la liste déroulante ; les opérateurs disponibles sont basés sur la catégorie sélectionnée :



Option	Description
=	Filtre les appareils qui correspondent exactement au champ de recherche de la catégorie sélectionnée.
↓	Filtre les appareils qui ne correspondent pas exactement au champ de recherche.
≈	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.
≈/	Filtre les appareils qui excluent la valeur du champ de recherche pour la catégorie sélectionnée.
commence par	Filtre les appareils qui commencent par la valeur du champ de recherche pour la catégorie sélectionnée.
existe	Filtre les appareils dont la valeur correspond à la catégorie sélectionnée.

Option	Description
n'existe pas	Filtre les appareils qui n'ont pas de valeur pour la catégorie sélectionnée.
correspondre	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.

11. Dans le champ de recherche, tapez la chaîne à mettre en correspondance ou sélectionnez une valeur dans la liste déroulante. Le type d'entrée est déterminé par la catégorie sélectionnée.
Par exemple, si vous souhaitez rechercher des appareils en fonction du nom, tapez la chaîne à rechercher dans le champ de recherche. Si vous souhaitez rechercher des appareils en fonction de leur rôle, sélectionnez-les dans la liste déroulante des rôles.

FILTER CRITERIA

The screenshot shows the 'FILTER CRITERIA' section with a 'Match All' dropdown. Below it, a search field is set to 'Name' with a search operator '≈' and the text 'accounting-'. A regex icon is visible on the right side of the search field. Below the search field are two buttons: 'Add Filter' and 'Add Filter Group'.

FILTER CRITERIA

The screenshot shows the 'FILTER CRITERIA' section with a 'Match All' dropdown. Below it, a search field is set to 'Role' with a search operator '=' and the text 'Select an item...'. A dropdown menu is open below the search field, showing options: 'Filter...', 'Database', 'DHCP Server', and 'DNS Server'. Below the search field is an 'Add Filter' button.

Conseil Selon la catégorie sélectionnée, vous pouvez cliquer sur l'icône Regex dans le champ de texte pour activer la correspondance par expression régulière.

FILTER CRITERIA

The screenshot shows the 'FILTER CRITERIA' section with a 'Match All' dropdown. Below it, a search field is set to 'Name' with a search operator '='. A tooltip with the text 'Type regular expression' is pointing to the regex icon on the right side of the search field. Below the search field are two buttons: 'Add Filter' and 'Add Filter Group'.

12. Optionnel : Cliquez **Ajouter un filtre** pour ajouter d'autres critères de filtre.
13. Optionnel : Cliquez **Ajouter un groupe de filtres** pour ajouter des critères de filtre aux résultats du filtre d'origine.
Par exemple, si vous filtrez les noms d'appareils commençant par « acct », vous pouvez ajouter un nouveau groupe de critères qui filtrent un certain rôle ou une étiquette au sein du groupe d'appareils commençant par « acct ».

14. Cliquez **Enregistrer**.

Vous pouvez modifier les critères en cliquant sur le groupe que vous souhaitez modifier sur la page Groupes de périphériques, puis en cliquant sur **Propriétés**.

Création d'un groupe d'équipements statique

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs** puis cliquez sur **Groupes d'appareils**.
3. Cliquez **Créer un groupe d'appareils**.
4. Dans le **Nom du groupe** dans ce champ, saisissez le nom du nouveau groupe.
5. Optionnel : À partir du **Rédacteurs** liste déroulante, sélectionnez les utilisateurs dotés de droits d'écriture limités qui peuvent modifier ce groupe d'équipements. Ce privilège global doit être activé dans les paramètres d'administration.
 - La liste affiche uniquement un nombre limité d'utilisateurs en écriture possédant des comptes actifs.
 - Seul un utilisateur disposant d'une autorisation de modification pour un groupe d'équipements peut ajouter d'autres utilisateurs d'écriture limités.
6. Optionnel : Dans le **Descriptif** champ, ajoutez des informations sur ce groupe d'équipements.
7. Dans le Type de groupe section, sélectionnez **Statique**.
8. Cliquez **Enregistrer**.
Votre groupe d'équipements est maintenant créé.
9. Ajoutez des appareils à votre groupe.
 - a) Cliquez **Appareils** dans le volet de gauche.
 - b) **Trouvez un équipement** puis cochez la case à côté des appareils que vous souhaitez ajouter à votre groupe.
 - c) En haut du tableau des équipements, cliquez sur **Attribuer au groupe**.
 - d) Sélectionnez un groupe d'équipements dans le Groupe liste déroulante.
 - e) Cliquez **Ajouter au groupe**.

Prochaines étapes

Supprimer des appareils d'un groupe en cochant la case à côté du nom de l'équipement et en cliquant sur **Supprimer du groupe** dans le coin supérieur droit.