Création d'un groupe dquelconque d'équipements

Publié: 2024-10-26

Vous pouvez créer des groupes d'appareils qui collectent des statistiques pour tous les appareils spécifiés dans un groupe. Avec les groupes d'appareils, vous pouvez toujours consulter les statistiques de chaque appareil ou membre du groupe. Les groupes d'appareils peuvent également être définis en tant que source métrique.

Utilisateurs avec privilèges d'écriture limités peut créer et modifier des groupes d'équipements dynamiques et statiques.

- Création d'un groupe d'équipements dynamique pour ajouter automatiquement au groupe tous les appareils qui correspondent à des critères spécifiques.
- Création d'un groupe d'équipements statiques pour ajouter manuellement chaque équipement.

Voici quelques considérations relatives aux performances à prendre en compte lors de la création d'un groupe diciéquipements :

- Le traitement d'un grand nombre de groupes d'appareils comportant un grand nombre d'appareils prendra plus de temps.
- Les groupes statiques sont traités plus rapidement que les groupes dynamiques et sont recommandés pour un groupe défini d' appareils.
- Les groupes dynamiques avec des critères complexes peuvent avoir un coût de performance plus élevé.

Création d'un groupe dproximatif d'équipements

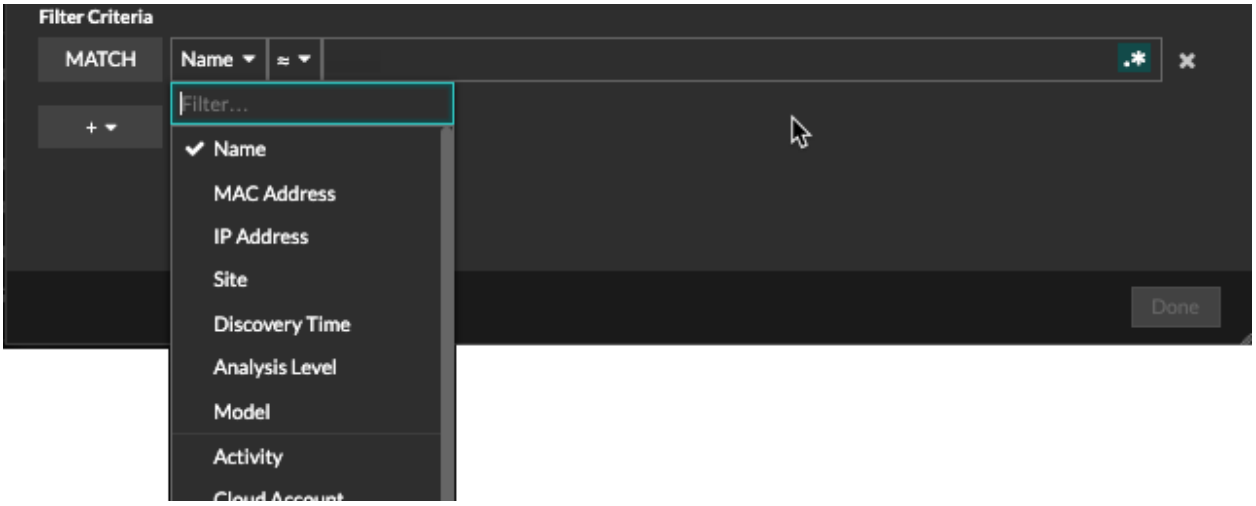
Vous pouvez créer des groupes d'équipements dynamiques avec des filtres complexes, qui vous permettent de spécifier plusieurs critères et de créer des groupes de critères imbriqués.

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

Vous pouvez également créer un groupe d'appareils dynamique à partir d'un groupe d'appareils intégré . Sur la page Ressources, cliquez sur un rôle ou un protocole, mettez à jour les critères de filtre, puis cliquez sur Enregistrer icône 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** graphique.
3. Cliquez **Créer un groupe d'appareils**.
4. Dans le **Nom du groupe** dans le champ, saisissez un nom descriptif pour identifier le groupe
5. Optionnel : À partir du **Rédacteurs** dans la liste déroulante, sélectionnez les utilisateurs disposant de privilèges d'écriture limités qui peuvent modifier ce groupe dcesséquipements. 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 à écriture limitée.
6. Optionnel : Dans le **Descriptif** dans ce champ, ajoutez des informations sur ce groupe dproximatif d'équipements.
7. Dans le Type de groupe section, cliquez sur **Dynamique**.

8. Dans le Critères de filtrage rubrique, **Nom** et sélectionnez l'une des catégories suivantes dans la liste déroulante :
9. Cliquez **Nom** et sélectionnez l'une des catégories suivantes dans la liste déroulante :

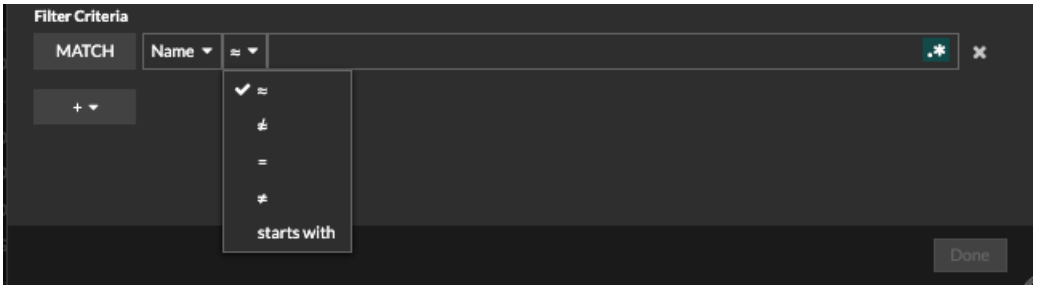


Option	Description
Nom	Filtre les appareils en fonction du nom de l'équipement découvert. Par exemple, le nom d'un équipement découvert peut inclure l'adresse IP ou le nom d'hôte.
Adresse MAC	Filtre les appareils en fonction de leur adresse MAC.
Adresse IP	Filtre les appareils par adresse IP au format de bloc IPv4, IPv6 ou CIDR.
Site	Filtre les appareils associés à un site connecté. Console uniquement.
L'heure de la découverte	Filtre les appareils découverts automatiquement par le système ExtraHop dans l'intervalle de temps spécifié. Pour plus d'informations, voir Création d'un groupe dproximatif d'équipements en fonction de l'heure de découverte.
Niveau d'analyse	Filtre les appareils par niveau d'analyse, ce qui détermine quelles données et mesures sont collectées pour un équipement. Vous ne pouvez pas créer de groupe déquipements dynamique pour les appareils filtrés par niveau d'analyse.
modèle	Filtre les appareils par marque, famille ou nom de modèle. La marque représente le fabricant de l'équipement. Une famille représente un groupe tel qu'une gamme de produits. Les conseils suivants peuvent vous aider à trouver le modèle d'équipement que vous souhaitez : • Vous pouvez faire votre choix parmi la liste des marques présentes sur votre système

Option	Description
	ExtraHop, puis cliquer sur le filtre pour affiner les résultats. • Vous pouvez afficher des info-bulles à côté des marques et des familles pour voir combien d'appareils et de modèles correspondants ont été trouvés. • Vous pouvez sélectionner une marque ou une famille pour trouver tous les appareils de ce groupe, quel que soit le modèle.
Activité	Filtre les appareils en fonction de l'activité de protocole associée à l'équipement. Par exemple, la sélection d'un serveur HTTP renvoie les appareils dont les métriques sont associées au serveur HTTP, ainsi que tout autre équipement dont le rôle d' équipement est défini sur Serveur HTTP. 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 une activité suspecte.
Compte Cloud	Filtre les appareils en fonction du compte de service cloud associé à l'appareil.
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.
Hachage de fichiers SHA-256	Filtre les appareils sur lesquels des fichiers hachés par l'algorithme de hachage SHA-256 ont été observés. Vous pouvez consulter un tableau des fichiers hachés sur le Page Fichiers.
Valeur élevée	Filtre les appareils considérés comme à valeur élevée parce qu'ils fournissent des services d'authentification, prennent en charge les services essentiels de votre réseau ou sont spécifiés par l'utilisateur comme étant à 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 localités 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 la passerelle, le pare-feu, l'équilibreur de charge et le serveur DNS.
Logiciel	Filtre les appareils en fonction du logiciel du système d'exploitation détecté sur l'équipement.

Option	Description
Type de logiciel	Filtre les appareils en fonction du type de logiciel observé sur l'équipement, tel qu'un simulateur d'attaque, un accès à distance ou un serveur de bases de données.
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 organisationnel (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 mise en miroir du trafic les conserve sur le port miroir. Disponible uniquement si le `devices_accross_vlans` le réglage est réglé sur `False` 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 selon n'importe quel nom DNS attribué à l'équipement.
Nom NetBIOS	Filtre les appareils en fonction du nom NetBIOS attribué à l'équipement.
Activité de détection	Filtre les appareils ayant une activité de détection où l'équipement était un participant. Active des critères supplémentaires tels que la catégorie, l'indice de risque et la technique MITRE. **Note:** Vous ne pouvez pas créer de groupe dveloppement contenant cette option de critère.

10. Sélectionnez l'un des opérateurs suivants dans la liste déroulante ; les opérateurs disponibles dépendent de la catégorie sélectionnée :

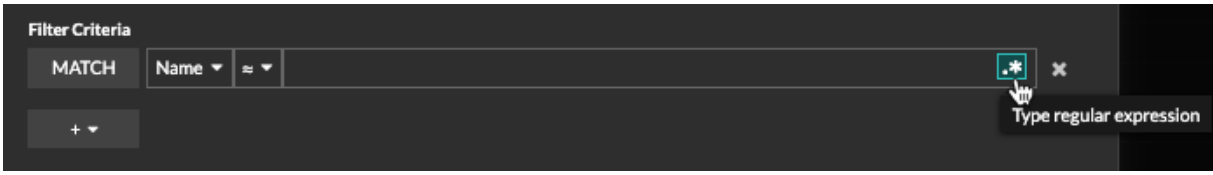


Option	Description
=	Filtre les appareils qui correspondent exactement au champ de recherche de la catégorie sélectionnée.
≠	Filtre les appareils qui ne correspondent pas exactement au champ de recherche.
≈	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.
≈/	Filtre les appareils qui excluent la valeur du champ de recherche pour la catégorie sélectionnée.
commence par	Filtre les appareils dont le nom commence par la valeur du champ de recherche de la catégorie sélectionnée.
existe	Filtre les appareils qui ont une valeur pour la catégorie sélectionnée.
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.
et	Filtre les appareils qui correspondent aux conditions spécifiées dans au moins deux champs de recherche.
ou	Filtre les appareils qui correspondent à au moins une condition spécifiée dans au moins deux champs de recherche.
pas	Filtre les appareils qui ne correspondent pas aux conditions spécifiées dans un champ de recherche.

11. Dans le champ de recherche, saisissez la chaîne à rechercher 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 de leur nom, saisissez la chaîne à laquelle vous souhaitez faire correspondre dans le champ de recherche. Si vous souhaitez rechercher des appareils en fonction du rôle, sélectionnez-le dans la liste déroulante des rôles.

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



12. Optionnel : Cliquez sur l'icône Ajouter un filtre + et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

    Par exemple, si vous filtrez les noms d'appareils commençant par « acct », vous pouvez ajouter un nouveau groupe de critères qui filtre un certain rôle ou une étiquette au sein du groupe d'appareils commençant par « acct ».
13. Cliquez **Enregistrer**.

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

Création d'un groupe dcessaires d'équipements

Conseil : Sur la page Appareils, vous pouvez cocher la case à côté d'un ou de plusieurs appareils et cliquer sur **Ajouter au groupe** pour créer rapidement un groupe d'appareils statique ou ajouter des appareils à un groupe existant.

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. 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** dans la liste déroulante, sélectionnez les utilisateurs disposant de privilèges d'écriture limités qui peuvent modifier ce groupe dcesséquipements. 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 dproximatifs d'équipements peut ajouter d'autres utilisateurs à écriture limitée.
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 dcesséquipements est maintenant créé.
9. Ajoutez un équipement spécifique à votre groupe.
   a) Cliquez sur le groupe dcesséquipements statiques de votre choix, puis cliquez sur **Appareils** depuis le volet de gauche.
   b) Cliquez sur le champ Rechercher un équipement... en haut du tableau des appareils, saisissez le nom de l'appareil souhaité, puis sélectionnez-le dans la liste.
   c) Cliquez **Ajouter au groupe**.
10. Ajoutez à votre groupe des appareils répondant à des critères spécifiques.
    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 **Ajouter au groupe**.
    d) Dans la boîte de dialogue Ajouter au groupe, sélectionnez **Ajouter à un groupe existant**.
    e) Sélectionnez un groupe diciels dans Groupe liste déroulante.

f) Cliquez **Ajouter au groupe**.

Prochaines étapes
Supprimez 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.