

Échec de la recherche d'événements unifiés FMC avec les noms d'objets réseau dans Firepower 7.7

Problème

Lorsque vous utilisez Cisco Secure Firewall Management Center (FMC) version 7.7.10.1, les objets réseau et les groupes d'objets ne peuvent pas être utilisés comme critères de recherche dans la page Événements unifiés. Lorsque vous tentez de rechercher des événements à l'aide de noms d'objets ou de groupes spécifiques sous Source IP dans Unified Event search, le FMC ne renvoie aucun résultat ou affiche un message d'erreur :

The query contains an invalid constraint on the provided field: "Source IP" with value "\${000_ALL-USER_

Les objets sont visibles et utilisables sous Gestion des objets, et les recherches par adresse IP brute fonctionnent comme prévu. Ce comportement affecte les objets réseau existants et nouvellement créés, ce qui rend difficile la recherche d'événements à l'aide de noms d'objet ou de noms de groupe dans l'interface Événements unifiés.

Environnement

- Cisco Secure Firewall Management Center pour VMware (FMCv)
- Version du logiciel: 7.7.10.1
- Technologie : Cisco Secure Firewall Firepower - 7.7
- Sous-technologie : Pare-feu sécurisé Cisco - Surveillance / Événements / Journalisation - 7.7
- Déploiement: Configuration FMC autonome
- FMC contient plus de 1 000 objets réseau

- L'environnement inclut l'historique de migration de FMC sur site vers cdFMC et de retour vers sur site

Résolution

Ce problème est causé par un défaut logiciel connu et ne peut pas être entièrement résolu par des modifications de configuration sur la version logicielle actuelle. Il est recommandé de mettre en oeuvre cette approche de résolution.

Solution de contournement immédiate

Utilisez les champs d'adresse IP dans les recherches d'événements unifiés au lieu des noms d'objets ou des groupes comme solution de contournement provisoire. Lors de la recherche d'événements liés aux objets ou groupes affectés :

1. Accédez à Analysis > Unified Events.
2. Dans les critères de recherche, utilisez les adresses IP réelles au lieu des noms d'objet.
3. Saisissez l'adresse IP ou la plage d'adresses IP dans les champs Source IP ou Destination IP.
4. Exécutez la recherche pour récupérer les événements souhaités.

Solution à long terme

Le correctif permanent nécessite une mise à niveau vers une future version du logiciel FMC qui inclut la résolution de l'ID de bogue Cisco CSCws52418. Procédez comme suit :

1. Abonnez-vous aux notifications CSCws52418 défectueuses pour recevoir des alertes lorsque des versions FMC fixes deviennent disponibles.
2. Surveillez l'état du bogue pour les mises à jour de la disponibilité du correctif, provisoirement prévues pour mai 2026.
3. Planifiez une fenêtre de maintenance pour mettre à niveau FMC et les périphériques gérés vers une version qui inclut le correctif pour CSCws52418 une fois qu'il est publié.

Prévention et recommandations

Jusqu'à la fin de la mise à niveau logicielle :

- Utilisez des critères de recherche basés sur IP dans Unified Events (IP source/de destination) lors de l'analyse d'événements liés à des objets ou groupes affectés.
- Lors de la création de nouveaux workflows opérationnels, évitez de vous fier uniquement aux recherches de noms d'objet dans Unified Events pour les processus opérationnels ou d'audit de cette version.
- Documentez les noms des objets affectés et leurs adresses IP correspondantes pour référence lors du dépannage.

Motif

Le comportement est provoqué par l'ID de bogue Cisco CSCws52418, où la gestion interne des recherches d'objets pour les recherches d'événements est limitée par une limite interne d'environ 1000 entrées d'objets. Les objets en dehors de cette limite ne sont pas correctement indexés ou renvoyés dans les recherches d'événements unifiés par nom, ce qui entraîne des résultats manquants ou des erreurs de "contrainte non valide". La reconstruction de la base de données d'événements monetdb ne résout pas ce comportement, car il s'agit d'une limitation logicielle codée plutôt que d'un problème de corruption de la base de données.

Autres informations utiles

- ID de bogue Cisco CSCws52418 - Certains objets ne peuvent pas être sélectionnés dans les filtres de recherche d'événements
- ID de bogue Cisco CSCwt05296 - Impossible d'utiliser l'objet IPv4-Private-All-RFC1918 nouvellement créé ou défini par le système comme filtre dans les événements
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.