Zoeken in FMC Unified Events mislukt met namen van netwerkobjecten in Firepower 7.7

uitgeven

Wanneer u Cisco Secure Firewall Management Center (FMC) versie 7.7.10.1 gebruikt, kunnen netwerkobjecten en objectgroepen niet worden gebruikt als zoekcriteria op de pagina Unified Events. Wanneer u probeert te zoeken naar gebeurtenissen met behulp van specifieke object- of groepsnamen onder Bron-IP in Unified Event-zoekopdracht, retourneert de FMC geen resultaten of geeft een foutbericht weer:

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

De objecten zijn zichtbaar en bruikbaar onder Objectbeheer en zoekopdrachten op basis van onbewerkte IP-adressen werken zoals verwacht. Dit gedrag is van invloed op zowel bestaande als nieuw gemaakte netwerkobjecten, waardoor het moeilijk is om te zoeken naar gebeurtenissen met behulp van objectnamen of groepsnamen in de interface Unified Events.

milieu

- Cisco Secure Firewall Management Center voor VMware (FMCv)
- Softwareversie: 7.7.10.1
- Technologie: Cisco Secure Firewall Firepower - 7.7
- Subtechnologie: Cisco Secure Firewall - Monitoring / Eventing / Logging - 7.7
- Implementatie: zelfstandige FMC-configuratie
- FMC bevat meer dan 1000 netwerkobjecten
- Omgeving omvat migratiegeschiedenis van on-premises FMC naar cdFMC en terug naar on-premises

resolutie

Dit probleem wordt veroorzaakt door een bekend softwaredefect en kan niet volledig worden opgelost door configuratiewijzigingen in de huidige softwareversie. Het verdient aanbeveling deze resolutieaanpak toe te passen.

Onmiddellijke tijdelijke oplossing

Gebruik IP-adresvelden in zoekopdrachten in Unified Event in plaats van objectnamen of groepen als tijdelijke tijdelijke tijdelijke oplossing. Bij het onderzoeken van gebeurtenissen met betrekking tot getroffen objecten of groepen:

1. Navigeer naar Analyse > Unified Events.
2. Gebruik in de zoekcriteria de werkelijke IP-adressen in plaats van objectnamen.
3. Voer het specifieke IP-adres of IP-bereik in de velden Bron-IP of Bestemming-IP in.
4. Voer de zoekopdracht uit om de gewenste gebeurtenissen op te halen.

Oplossing op lange termijn

De permanente oplossing vereist een upgrade naar een toekomstige FMC-softwarerelease met de resolutie voor Cisco Bug ID CSCws52418. Neem deze stappen:

1. Abonneer u op defecten CSCws52418-meldingen om waarschuwingen te ontvangen wanneer vaste FMC-versies beschikbaar komen.
2. Controleer de bugstatus voor updates over de beschikbaarheid van de fix, voorlopig gepland voor mei 2026.
3. Plan een onderhoudsvenster om FMC en beheerde apparaten te upgraden naar een release die de oplossing voor CSCws52418 bevat zodra deze is gepubliceerd.

Preventie en aanbevelingen

Totdat de software-upgrade is voltooid:

- Gebruik op IP gebaseerde zoekcriteria in Unified Events (bron/bestemming-IP) bij het

onderzoeken van gebeurtenissen met betrekking tot getroffen objecten of groepen.

- Bij het maken van nieuwe operationele workflows moet u ervoor zorgen dat u niet alleen vertrouwt op zoekopdrachten naar objectnamen in Unified Events voor operationele of auditprocessen voor deze versie.
- Documentnamen van objecten en de bijbehorende IP-adressen ter referentie tijdens het oplossen van problemen.

Oorzaak

Het gedrag wordt veroorzaakt door Cisco Bug ID CSCws52418, waarbij de interne afhandeling van object lookups voor event searches wordt beperkt door een interne limiet van ongeveer 1000 object entries. Objecten buiten deze limiet worden niet correct geïndexeerd of geretourneerd in zoekopdrachten naar Unified Event op naam, wat resulteert in ontbrekende resultaten of fouten met ongeldige beperkingen. De herbouw van de database met gebeurtenissen van monetdb lost dit gedrag niet op, omdat het een gecodeerd softwarebeperking is in plaats van een probleem met databasecorruptie.

Verwante inhoud

- Cisco Bug ID CSCws52418 - Sommige objecten zijn niet beschikbaar voor selectie in zoekfilters voor gebeurtenissen
- Cisco Bug ID CSCwt05296 - Kan nieuw gemaakt of door het systeem gedefinieerd object IPv4-Private-All-RFC1918 niet gebruiken als filter in gebeurtenissen
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.