FMC-hostlimietlicentiefout oplossen: " u hebt nog 0 van xxxxxx FireSIGHT-hostlicenties over"

Inhoud

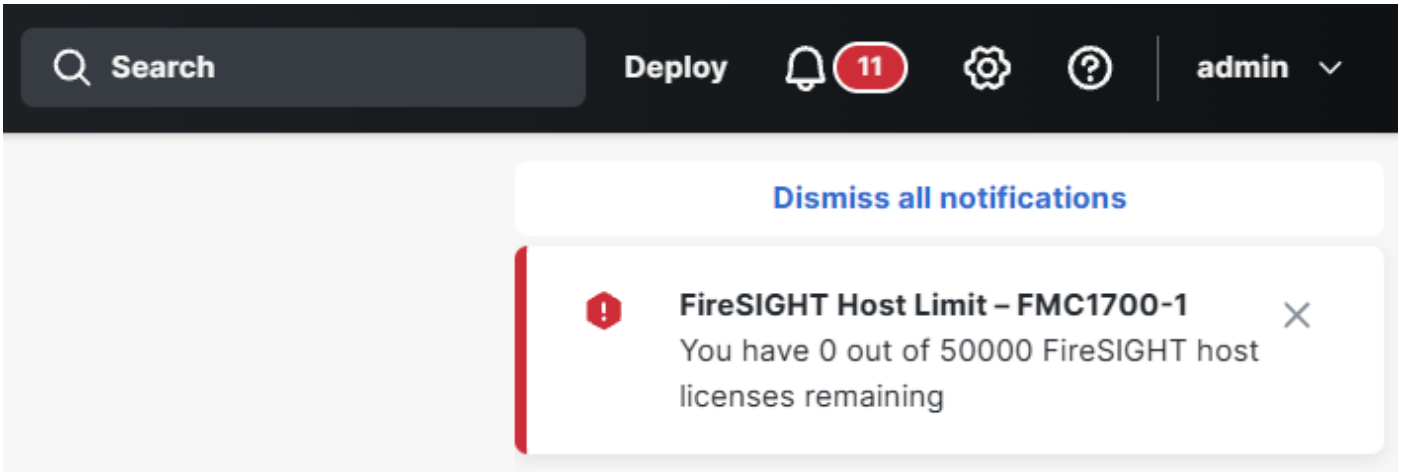
uitgifte

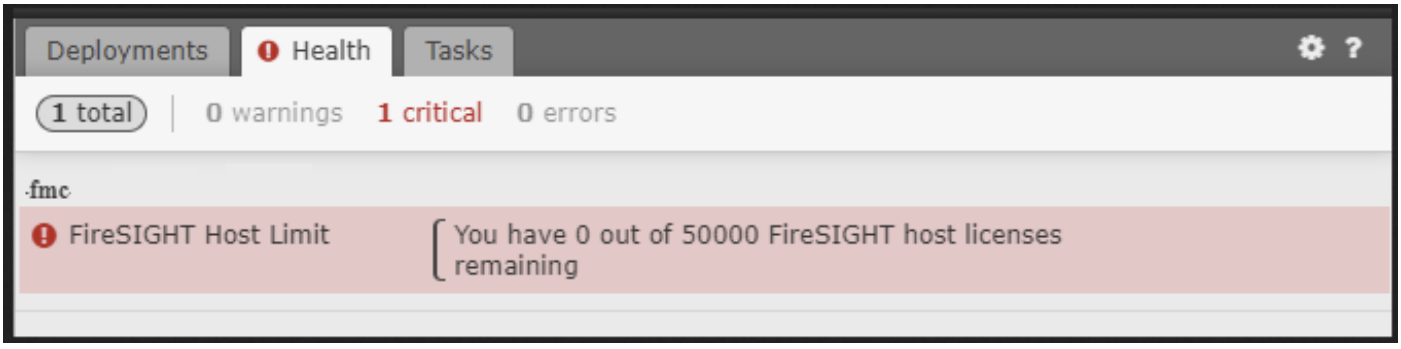
Een Firewall Management Center (FMC) geeft een gezondheidswaarschuwing weer die aangeeft dat de limiet voor de hostlicentie is bereikt. De specifieke foutmelding toont:

FireSIGHT-hostlimiet – [FMC-hostnaam]

Er blijven 0 van de xxxxxx FireSIGHT-hostlicenties over

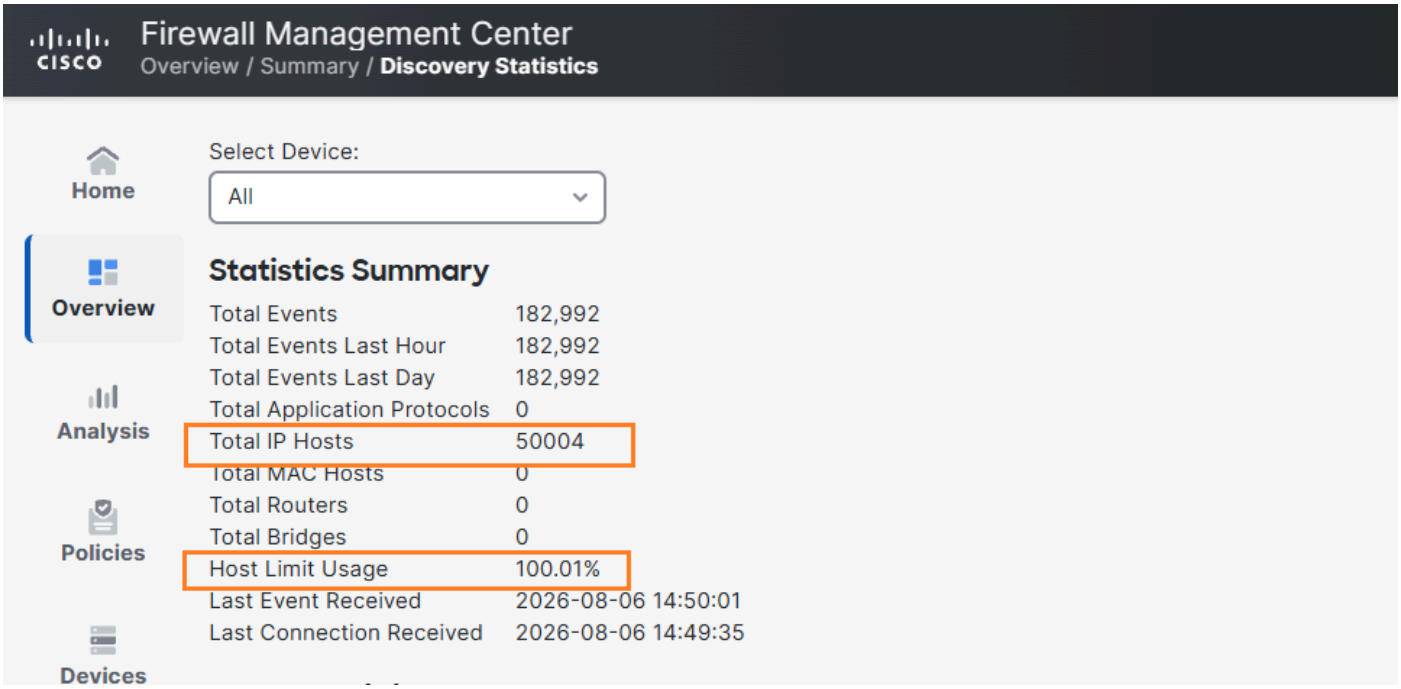
Voorbeelden:





Opmerking: het totale aantal hostlicenties is afhankelijk van het FMC-platform.

Bovendien toont de pagina Overzicht > Overzicht > Ontdekkingsstatistieken 100% gebruik:



milieu

- VCC 7.7.10. Ook andere softwareversies kunnen worden beïnvloed.
- Netwerkdetectie geconfigureerd met hosttracering ingeschakeld.

resolutie

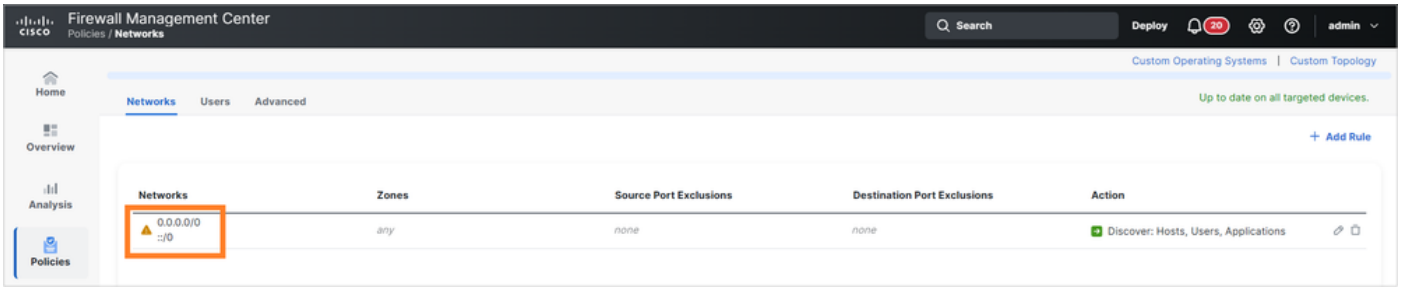
De FMC-hostlimietwaarschuwing veroorzaakt geen storingen in het firewallverkeer. Toegangscontrole en inspectie blijven normaal functioneren. De primaire impact is op de zichtbaarheid van de gastheer en het volgen van de context in het VCC.

Deze melding wordt weergegeven wanneer het VCC zijn maximale capaciteit voor het volgen van hosts in de netwerkkaart en de hostdatabase heeft bereikt.

Bereik voor netwerkdetectie controleren:

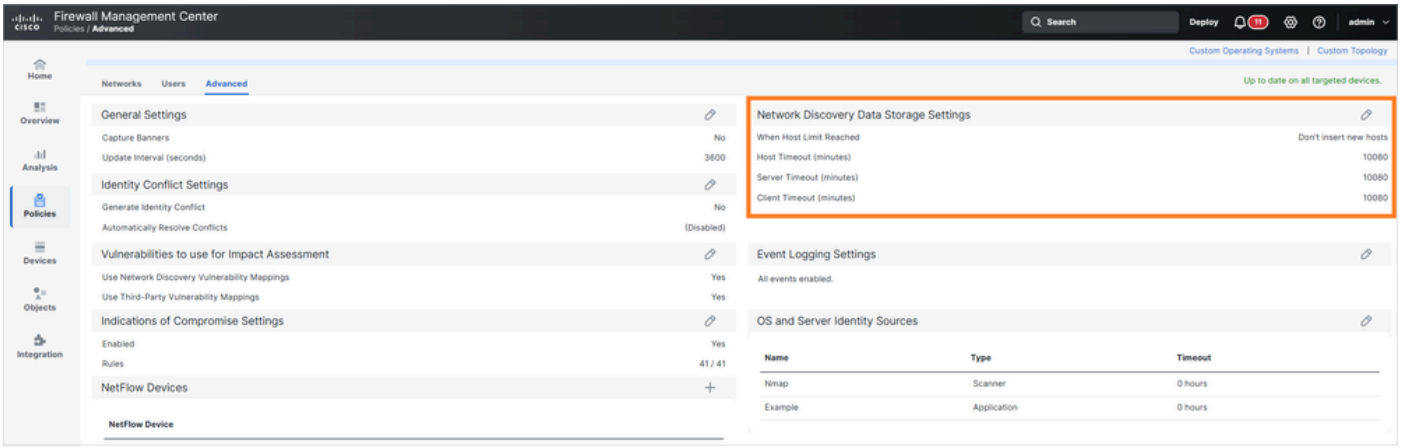
Zorg ervoor dat de detectie beperkt is tot de vereiste interne netwerken. Vermijd het ontdekken van onnodige openbare, NAT-, gast-, load-balancer- of transiënte adresbereiken, tenzij dit nodig is voor de zichtbaarheid van de beveiliging.

In dit geval moet u de configuratie voor netwerkdetectie wijzigen en alleen de interne netwerken opgeven die u wilt controleren. Anders kunnen externe (internet)hosts uw database vullen:



Huidige configuratieanalyse

Controleer de huidige hostlimiet door de instellingen voor netwerkdetectie te bekijken in Beleid > Netwerkdetectie > Geavanceerd > Instellingen voor gegevensopslag voor netwerkdetectie:



De configuratie toont meestal:

- Wanneer hostlimiet is bereikt: geen nieuwe hosts invoegen

- Host Time-out: 10080 minuten / 7 dagen
- Time-out server: 10080 minuten / 7 dagen
- Time-out voor client: 10080 minuten / 7 dagen

Met de huidige instelling "Geen nieuwe hosts invoegen" en de hostdatabase vol, voegt FMC pas nieuw ontdekte hosts toe wanneer het aantal hosts onder de limiet daalt, waardoor de zichtbaarheid van de host onvolledig is.

Optionele configuratiewijziging

U kunt het gedrag van de hostlimiet wijzigen om continue tracking van actieve hosts mogelijk te maken:

Stap 1: Navigeer naar Beleid > Netwerkdetectie.

Stap 2: Klik op het tabblad Geavanceerd.

Stap 3: Klik onder de instellingen voor netwerkdetectie en gegevensopslag op Bewerken.

Stap 4: Wijzig wanneer hostlimiet is bereikt van "Geen nieuwe hosts invoegen" naar Drop-hosts.

Stap 5: Sla de wijzigingen op.

Stap 6: Implementeer de configuratie om de wijzigingen toe te passen.

Verwachte impact en gedrag

Met de instelling "Drop hosts" ingeschakeld:

- Er wordt geen storing in het firewallverkeer verwacht.

- Toegangscontrole en inspectie gaan normaal door.
- FMC verwijdert de langst inactieve host uit de netwerkkaart wanneer nieuw ontdekte hosts worden toegevoegd.
- Het continue bijhouden van de huidige actieve hosts wordt gehandhaafd.
- Historische hostcontext voor gedropte hosts kan niet meer zichtbaar zijn totdat die hosts weer actief zijn.

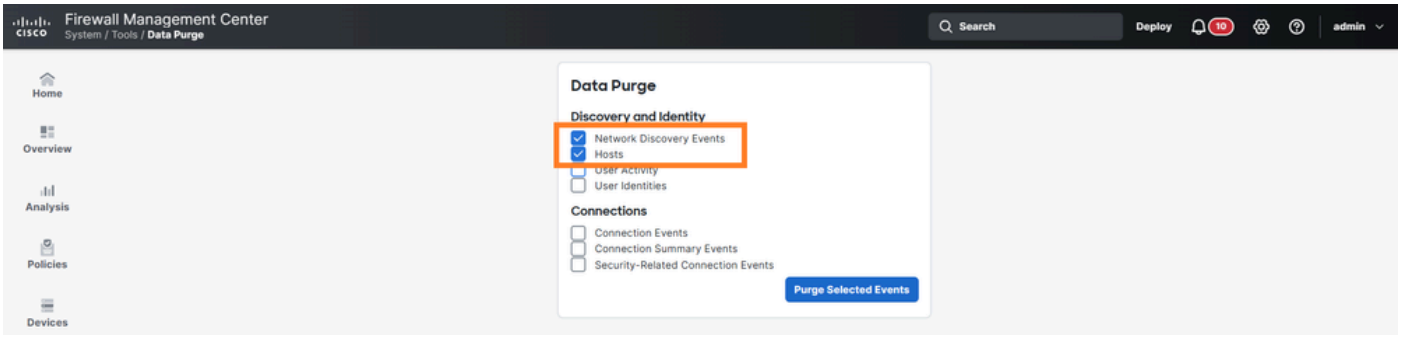
Time-outbeoordeling host:

De standaard time-outwaarden van 10080 minuten (7 dagen) zijn doorgaans geschikt. Overweeg alleen aanpassingen aan te brengen als inactieve hosts te lang worden bewaard.

Handmatige hostreiniging (indien nodig):

Als het aantal hosts onmiddellijk moet worden verlaagd, kunnen verouderde hosts worden verwijderd uit Analyse > Hosts > Tabelweergave van hosts. Merk op dat dit slechts een opruimactie is - als de detectieruimte te breed blijft, herontdekt FMC dezelfde hosts.

U kunt ook alle hosts uit de opsporingsdatabase opschonen vanuit Systeem > Extra > Gegevensopschoning:



Oorzaak

De FireSIGHT-hostlicentielimiet wordt bereikt wanneer het FMC het maximale aantal hosts in zijn netwerkkaart en hostdatabase heeft ontdekt en bijhoudt. Gemeenschappelijke bijdragende factoren zijn onder meer:

- Het bereik voor netwerkdetectie is te breed geconfigureerd, inclusief onnodige externe of openbare adresbereiken.
- Ontdekking van NAT-, load-balancer- of transient-adressen die hostlicenties verbruiken.
- Instellingen voor time-out van host die inactieve hosts gedurende langere perioden behouden.
- De natuurlijke netwerkgroei bereikt de FMC-hostcapaciteitslimiet.

Gerelateerde inhoud

- Apparaatconfiguratiehandleiding van Cisco Secure Firewall Management Center - Beleid voor netwerkdetectie
- 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.