Identificeren en analyseren van FTD-failover-gebeurtenissen op FMC

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

failover-gebeurtenissen op FMC

- Stap 1. Configuratie van het gezondheidsbeleid
- Stap 2. Beleidstoewijzing
- Stap 3. Waarschuwingen voor failover-gebeurtenissen
- Stap 4. Historische failover-gebeurtenissen
- Stap 5. Dashboard met hoge beschikbaarheid
- Stap 6. Threat Defense CLI

Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u failover-gebeurtenissen kunt identificeren en analyseren voor Secure Firewall Threat Defence op Secure Firewall Management Center GUI.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- High Availability (HA) Setup voor Cisco Secure Firewall Threat Defence (FTD)
- Basisbruikbaarheid van Cisco Firewall Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FMC v7.2.5
- Cisco Firepower 9300 Series v7.2.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Achtergrondinformatie

Het VCC is niet alleen het beheercentrum voor FirePOWER-apparaten, naast beheer- en configuratieopties, het biedt ook een grafische interface die logbestanden en gebeurtenissen in real en past helpt analyseren.

Wanneer het spreken over failover, heeft de interface nieuwe verbeteringen die helpen om failover gebeurtenissen te analyseren om de mislukkingen te begrijpen.

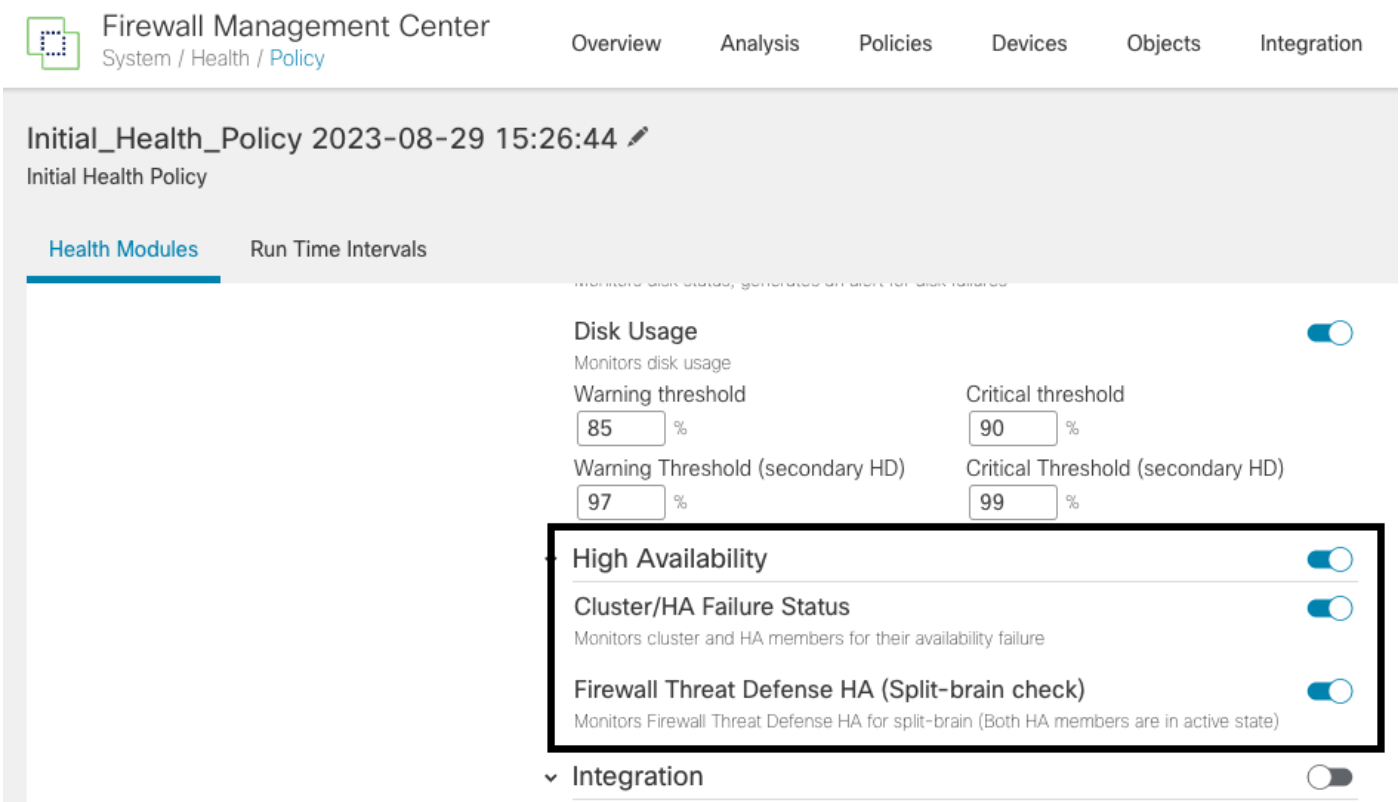
failover-gebeurtenissen op FMC

Stap 1. Configuratie van het gezondheidsbeleid

De module Cluster/HA Failure Status is standaard ingeschakeld op het Health Policy, maar daarnaast kunt u de optie Split-brain check inschakelen.

Om de opties voor HA in het gezondheidsbeleid mogelijk te maken, gaat u naar System > Health > Policy > Firewall Threat Defense Health Policy > High Avilability.

Dit beeld beschrijft de HA-configuratie van het gezondheidsbeleid:



Gezondheidsinstellingen voor hoge beschikbaarheid

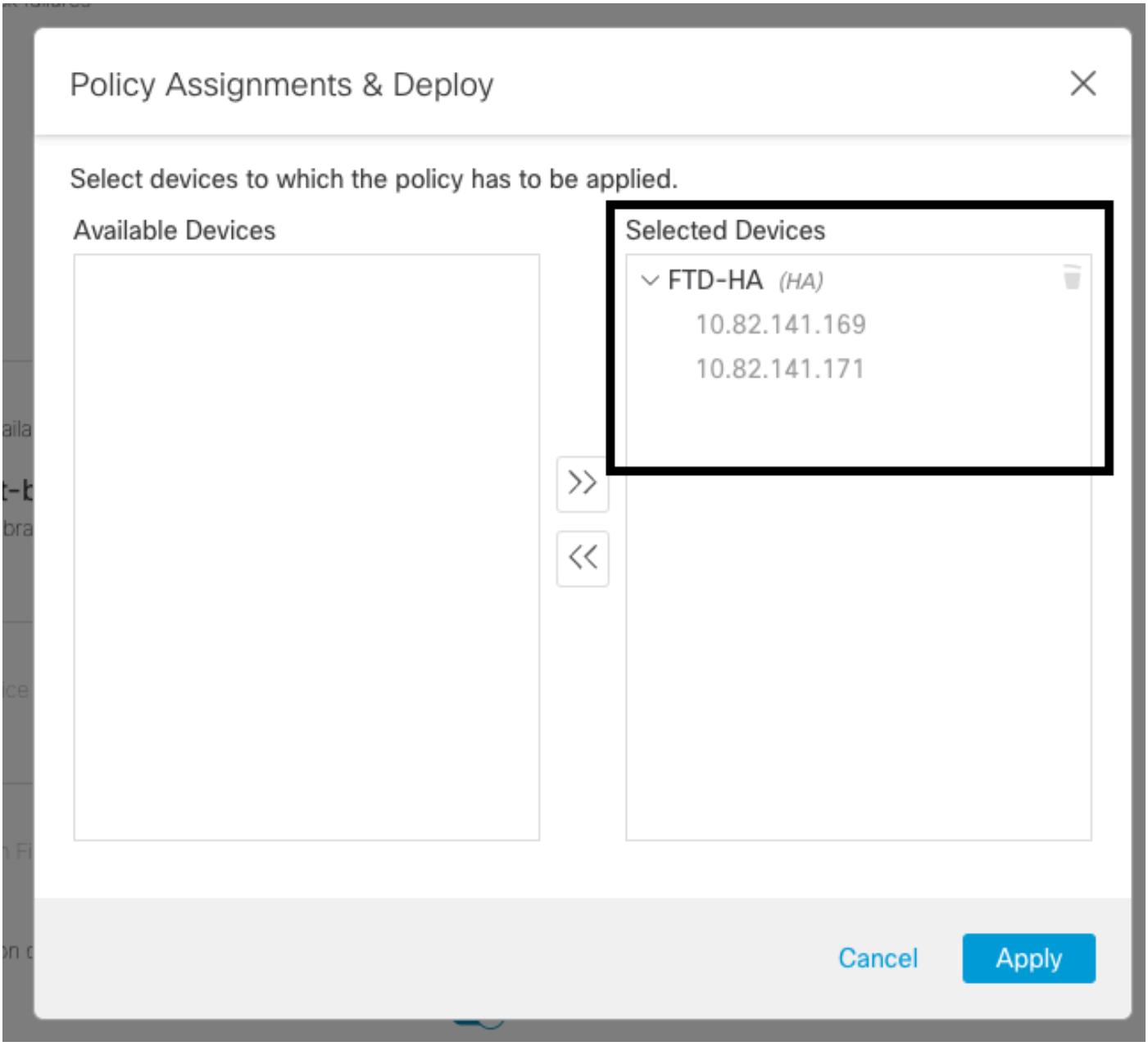
Stap 2. Beleidstoewijzing

Zorg ervoor dat het gezondheidsbeleid is toegewezen aan de HA-paren die u vanaf het VCC wilt

bewaken.

Ga om het beleid toe te wijzen naar System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

Deze afbeelding laat zien hoe het gezondheidsbeleid aan het HA-paar kan worden toegewezen:



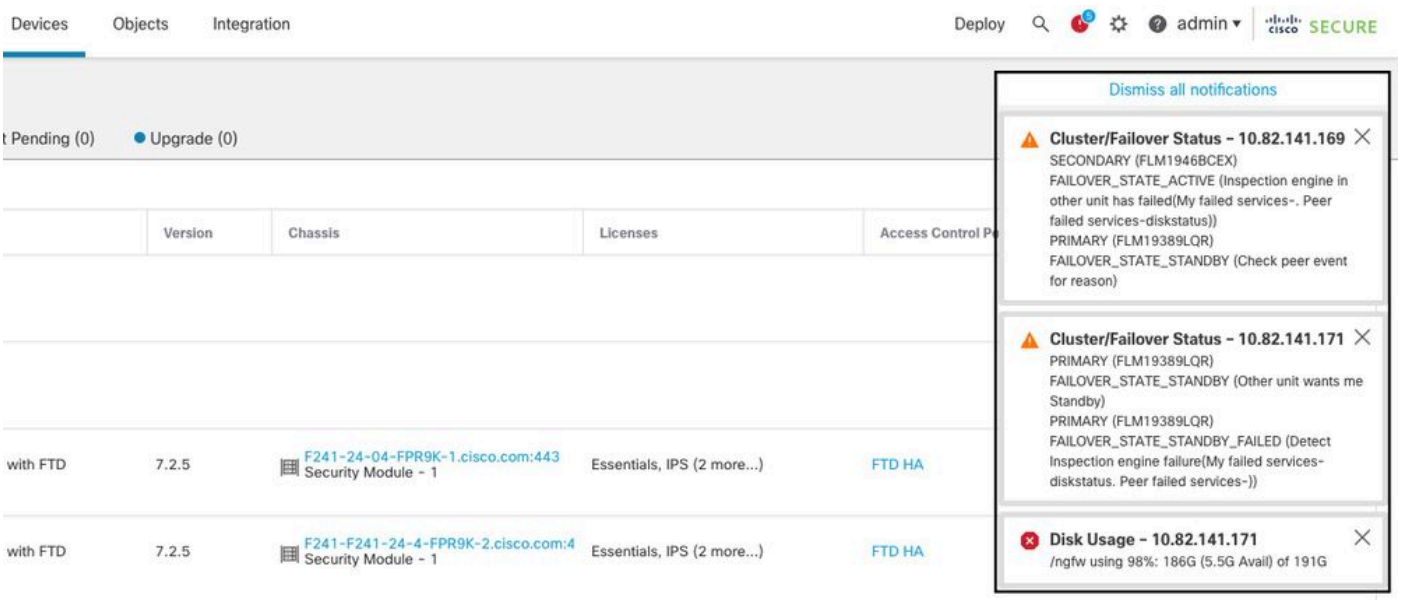
Toewijzing HA

Zodra het beleid is toegewezen en opgeslagen, past het VCC het automatisch toe op het FTD.

Stap 3. Waarschuwingen voor failover-gebeurtenissen

Afhankelijk van de configuratie van de HA, zodra een failover-gebeurtenis wordt geactiveerd, worden de pop-upwaarschuwingen die de failover-fout beschrijven weergegeven.

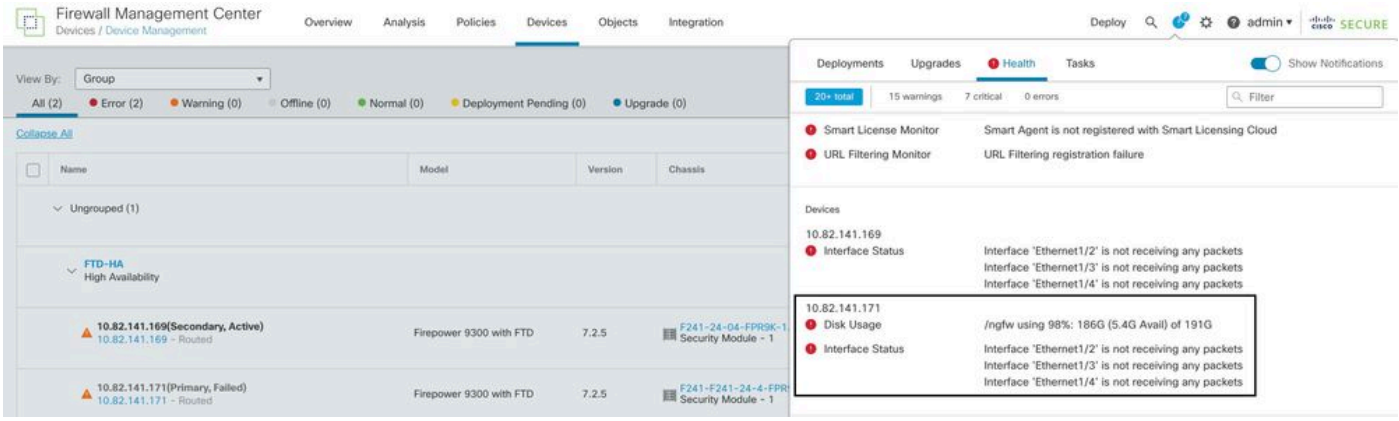
Dit beeld toont de gegenereerde failover-waarschuwingen:



Waarschuwingen voor failover

U kunt ook navigeren naar Notifications > Health om de failover-gezondheidswaarschuwingen te visualiseren.

Dit beeld toont de failover waarschuwingen onder meldingen:

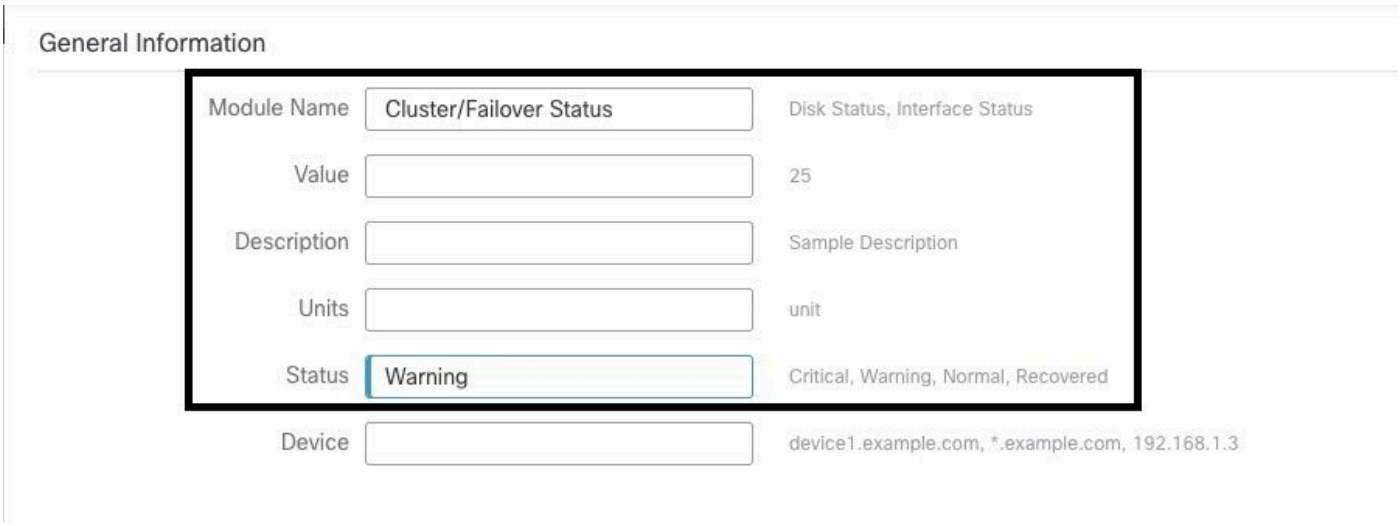


HA-meldingen

Stap 4. Historische failover-gebeurtenissen

Het VCC biedt een manier om de failover-gebeurtenissen in het verleden te visualiseren. Om de gebeurtenissen te filteren, navigeer naar System > Health > Events > Edit Search en specificeer de modulenaam als Cluster/failover-status. Bovendien kan het filter worden toegepast op basis van de status.

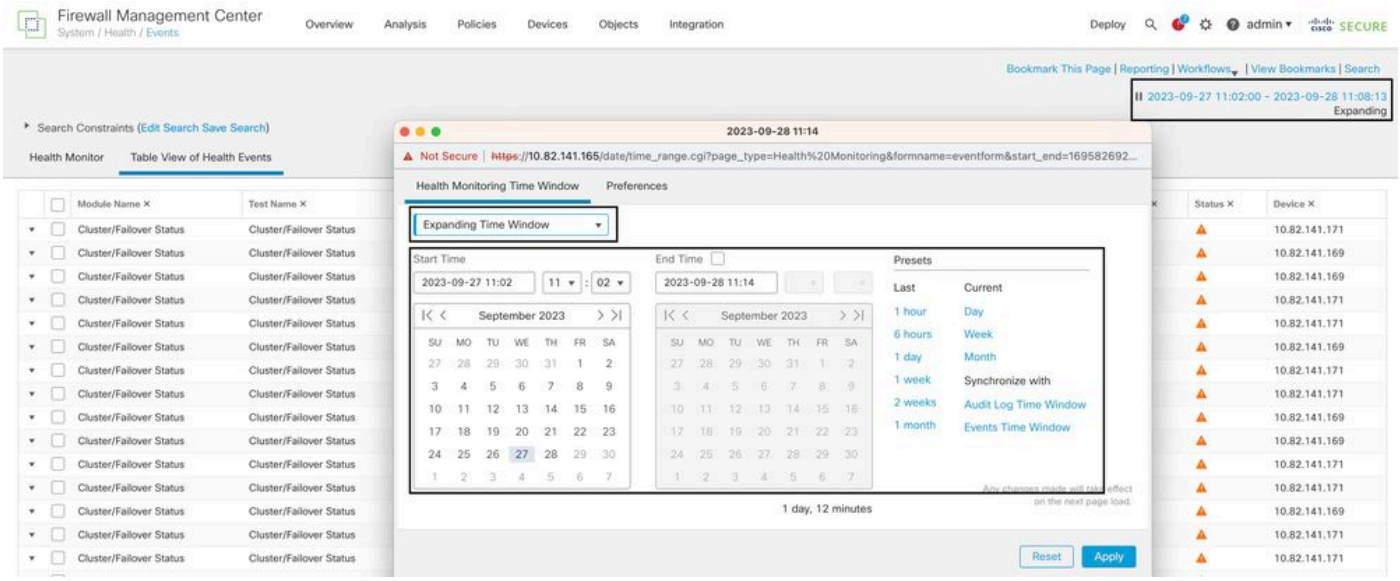
Dit beeld toont hoe failover-gebeurtenissen te filteren:



Berichten over failover-filters

U kunt de tijdinstellingen aanpassen om de gebeurtenissen voor een bepaalde datum en tijd weer te geven. Als u de tijdinstellingen wilt wijzigen, navigeert u naar System > Health > Events > Time.

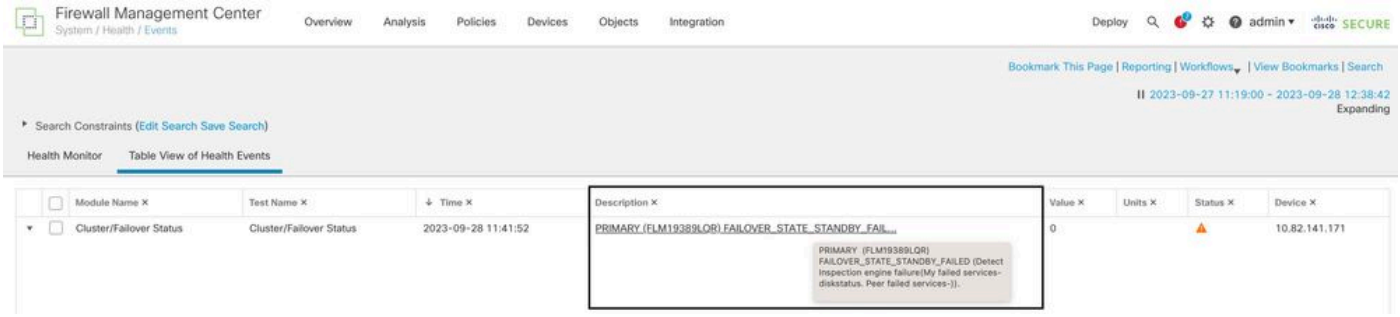
Deze afbeelding toont hoe u de tijdinstellingen kunt bewerken:



Tijdfilter

Zodra de gebeurtenissen zijn geïdentificeerd, om de reden voor de gebeurtenis te bevestigen, richt de cursor onder Beschrijving.

Dit beeld toont hoe de reden voor failover kan worden gezien.



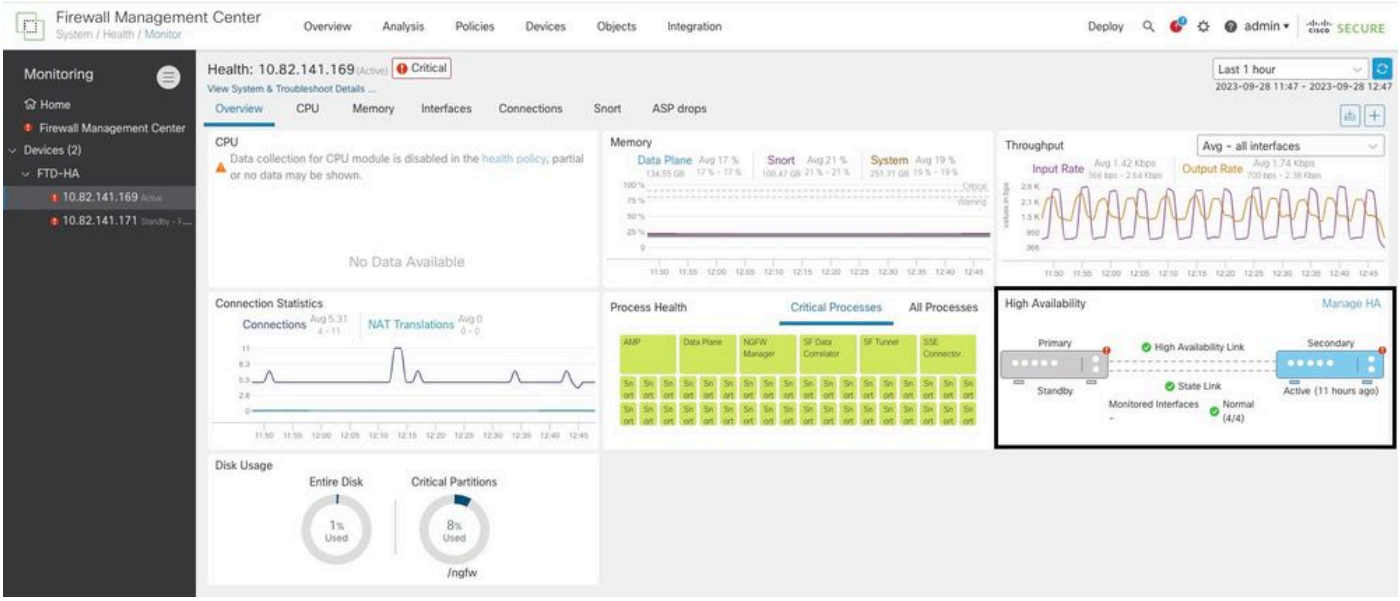
failover-gegevens

Stap 5. Dashboard met hoge beschikbaarheid

Een andere manier om de failover te bewaken is te vinden onder System > Health Montitor > Select Active or Standby Unit.

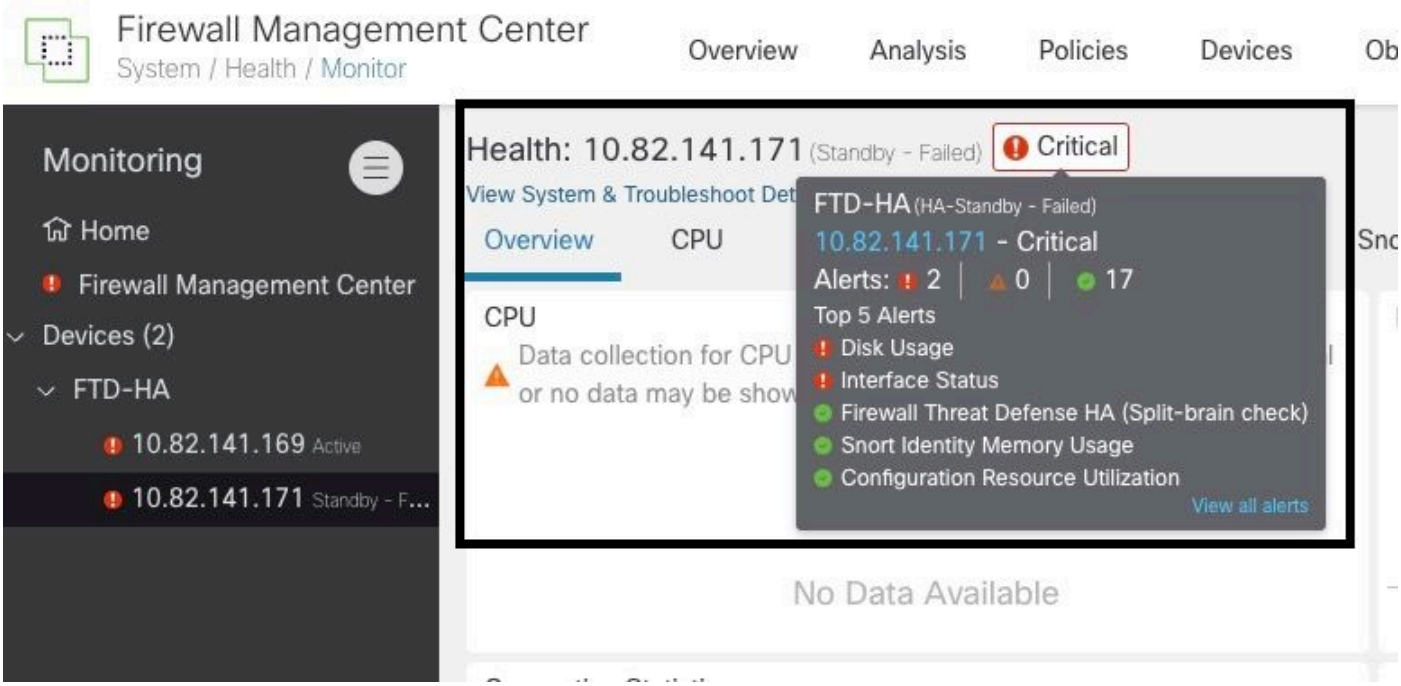
De HA-monitor biedt informatie over de status van de HA en State Link, bewaakte interfaces, ROL en de status van de waarschuwingen op elke eenheid.

Deze afbeelding toont de HA-monitor:



Afbeeldingen over gezondheid

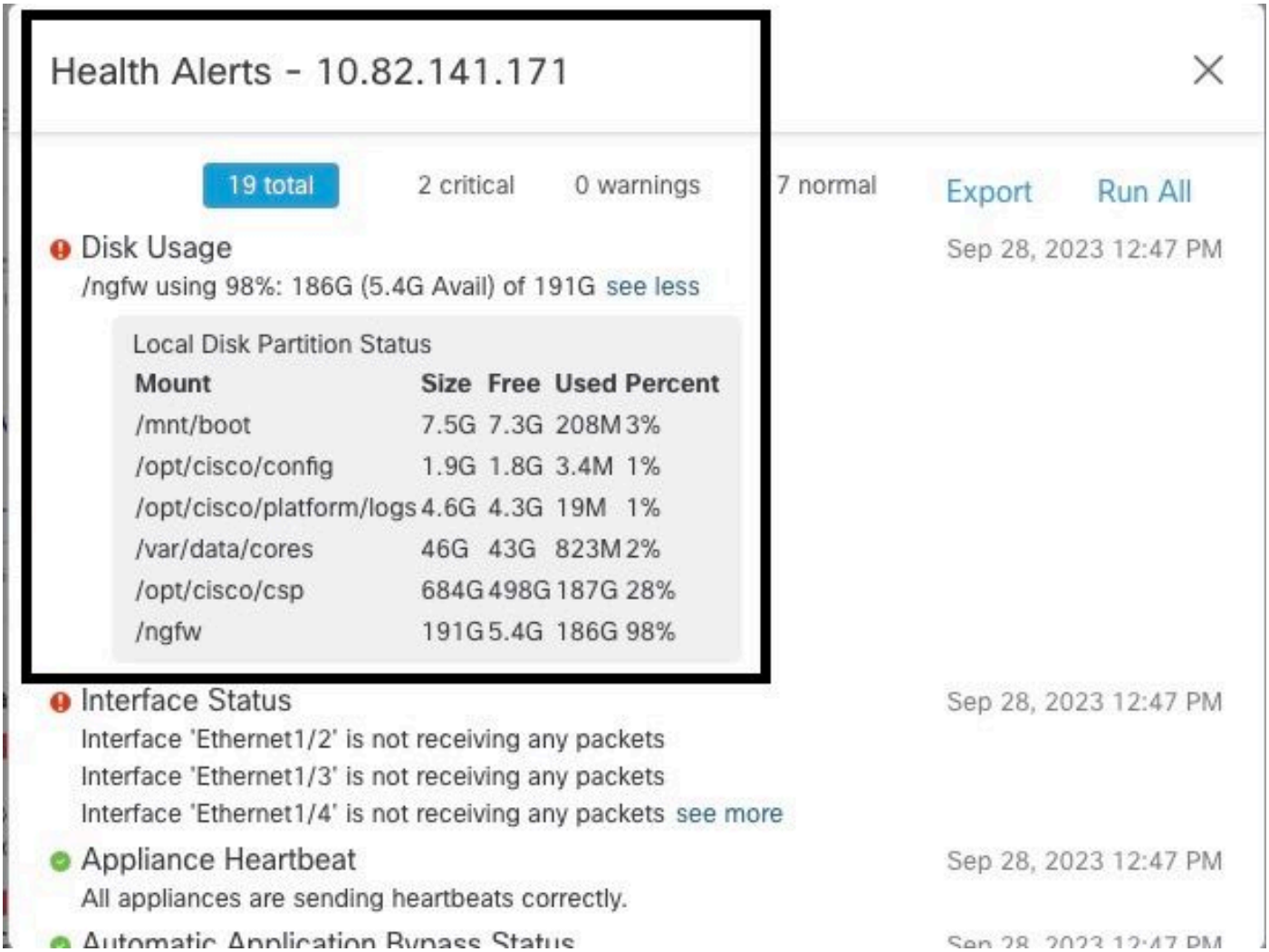
Blader naar om de waarschuwingen te visualiseren. System > Health Montitor > Select Active or Standby Unit > Select the Alerts.



Waarschuwing

Kies voor meer informatie over de waarschuwingen View all alerts > see more.

Dit beeld toont de diskstatus die de failover heeft veroorzaakt:

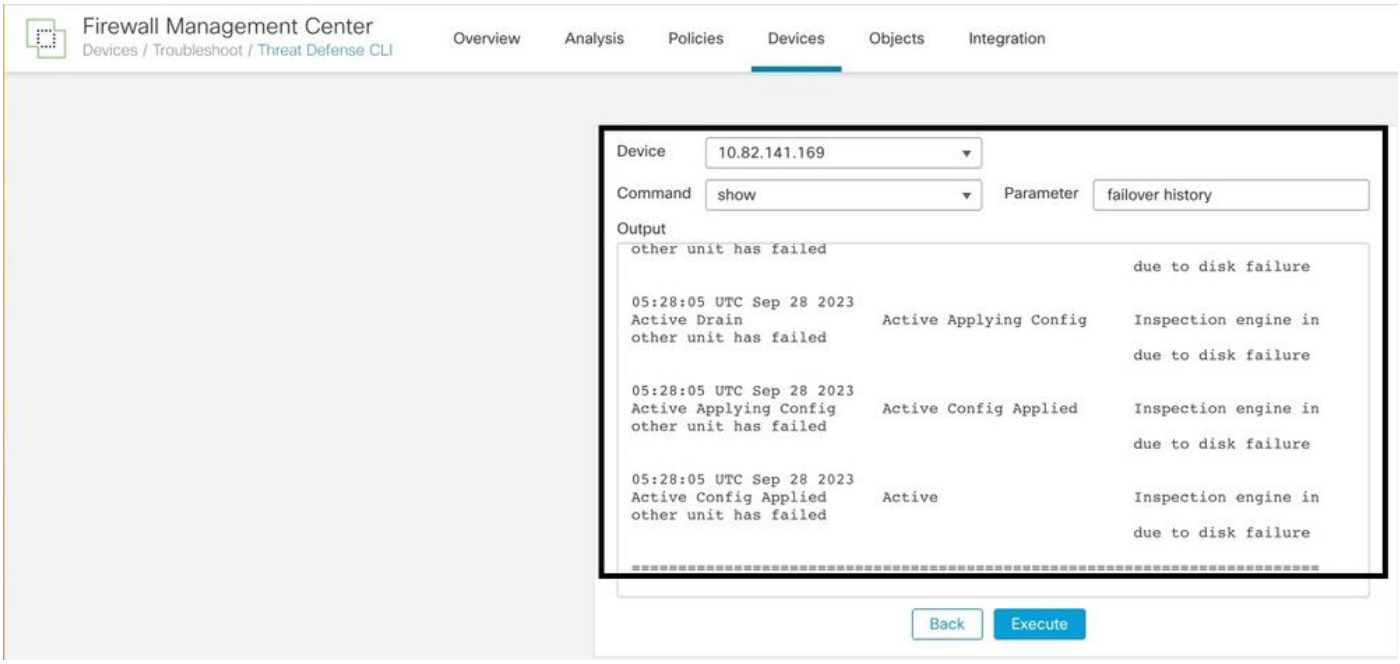


waarschuwingsdetails

Stap 6. Threat Defense CLI

Ten slotte kunt u voor het verzamelen van aanvullende informatie over VCC navigeren naar Devices > Troubleshoot > Threat Defense CLI. Configureer de parameters zoals Apparaat en de opdracht die moet worden uitgevoerd en klik Execute.

Deze afbeelding toont een voorbeeld van de opdracht show failover history die kunnen worden uitgevoerd op het VCC waar u de storing van failover kunt vaststellen.



failover-geschiedenis

Gerelateerde informatie

- Hoge beschikbaarheid voor FTD
- Hoge beschikbaarheid van FTD op Firepower-applicaties configureren
- Technische ondersteuning en documentatie – Cisco Systems

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.