Identificar e analisar eventos de failover de FTD no FMC

Contents

Introdução

Este documento descreve como identificar e analisar eventos de failover para Secure Firewall Threat Defense na GUI do Secure Firewall Management Center.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de alta disponibilidade (HA) para Cisco Secure Firewall Threat Defense (FTD)
- Utilização básica do Cisco Firewall Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

O FMC não é apenas o centro administrativo de dispositivos Firepower, além do gerenciamento e das opções de configuração, ele também fornece uma interface gráfica que ajuda a analisar logs e eventos em tempo real e passado.

Ao falar sobre failover, a interface tem novas melhorias que ajudam a analisar os eventos de failover para entender as falhas.

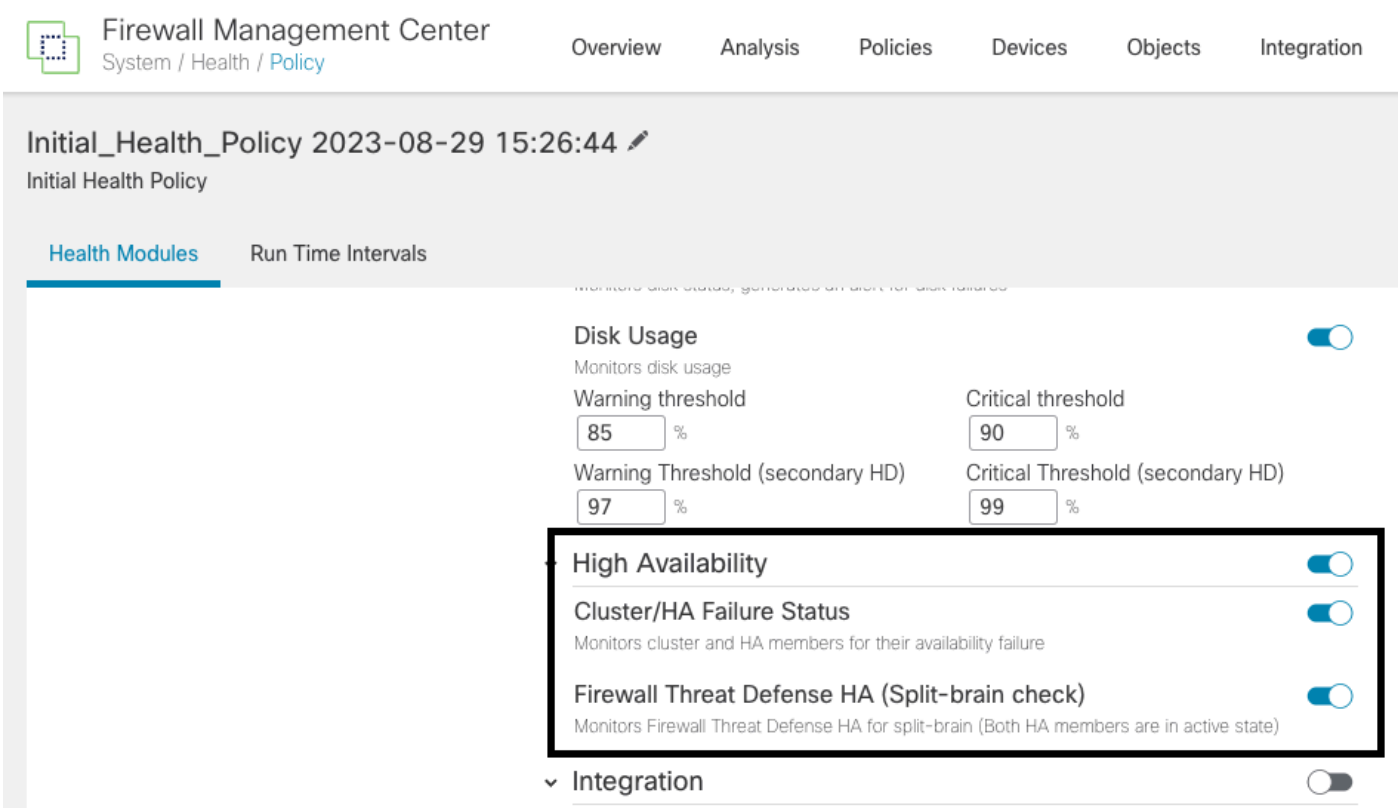
Eventos de failover no FMC

Etapa 1. Configuração de Política de Integridade

O módulo Cluster/HA Failure Status (Status de falha de HA/cluster) é ativado por padrão na Health Policy (Política de integridade), mas, além disso, você pode ativar a opção Split-brain check (Dividir cérebro).

Para habilitar as opções de HA na política de integridade, navegue até System > Health > Policy > Firewall Threat Defense Health Policy > High Avilability.

Esta imagem descreve a configuração de HA da Política de Integridade:



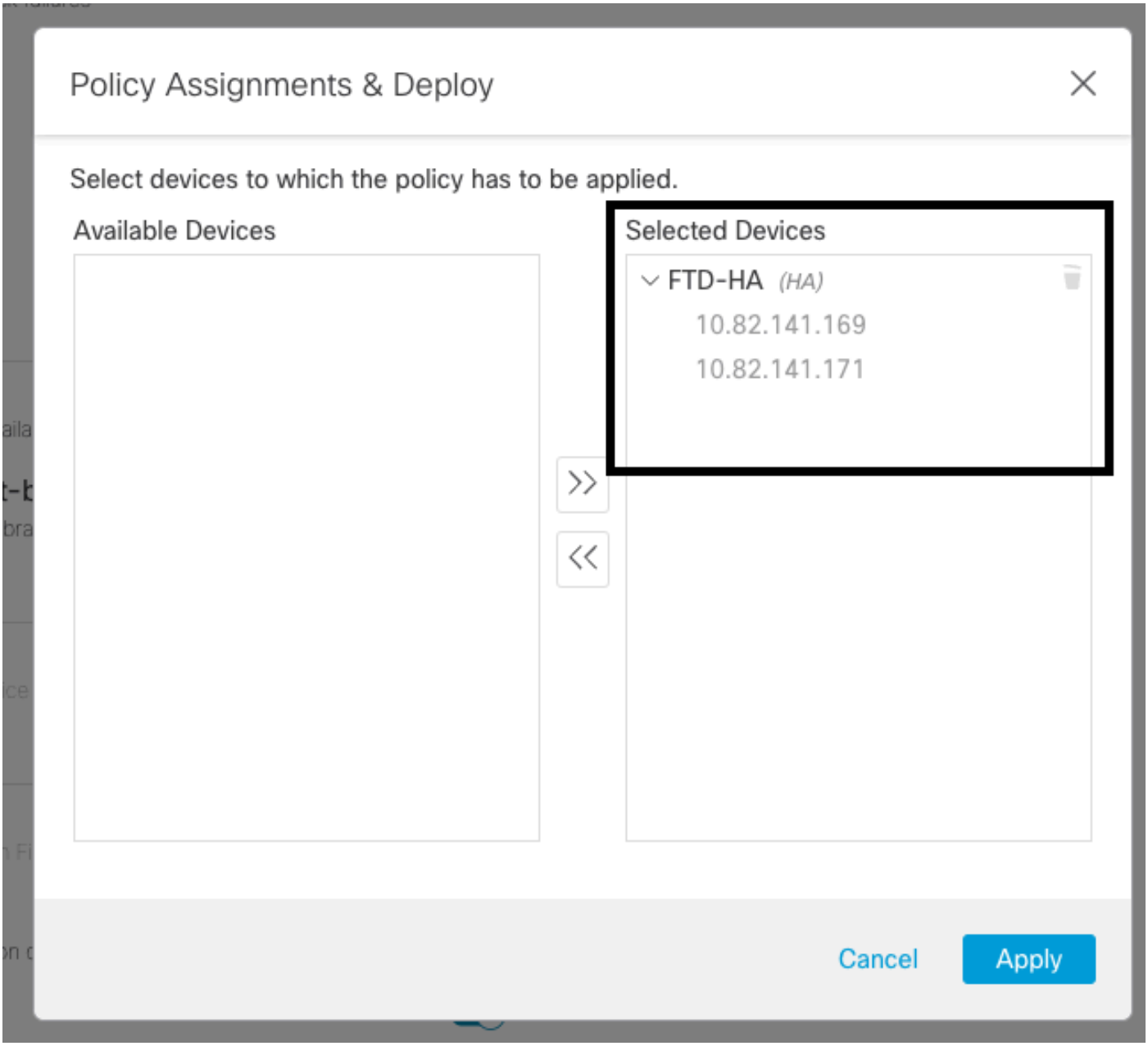
Configurações de Integridade de Alta Disponibilidade

Etapa 2. Atribuição de política

Certifique-se de que a Política de integridade esteja atribuída aos pares de alta disponibilidade que você deseja monitorar do FMC.

Para atribuir a regra, navegue até System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

Esta imagem mostra como atribuir a política de integridade ao par HA:



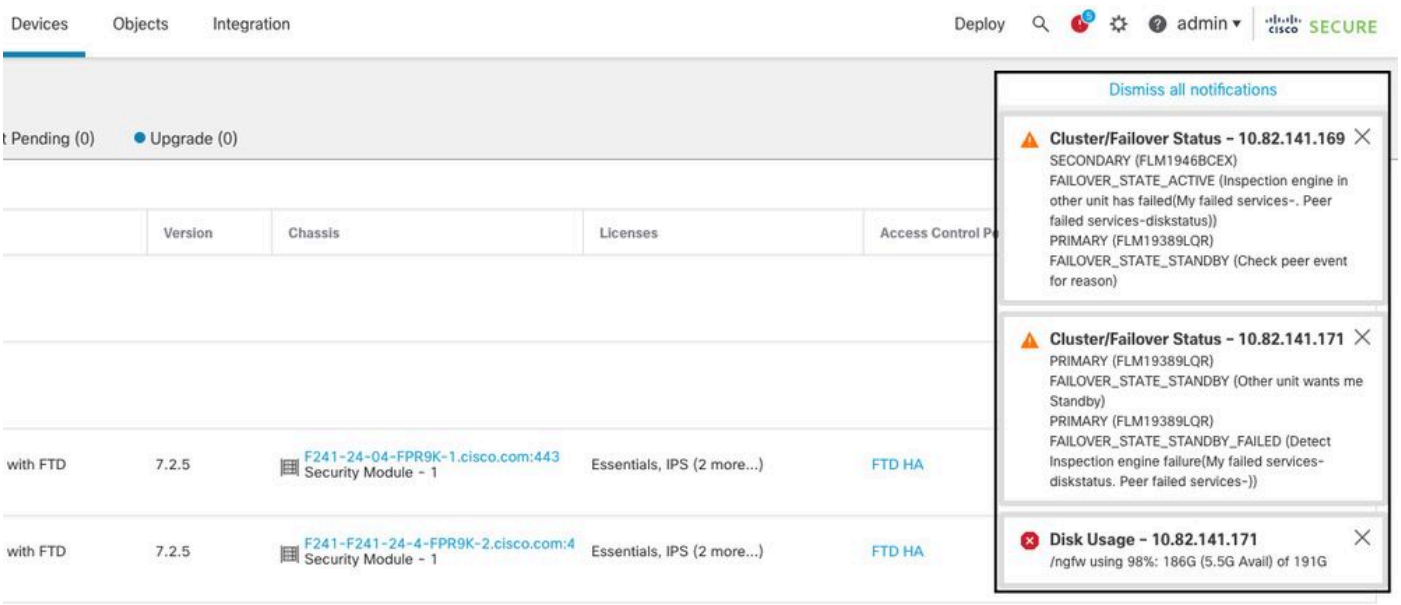
atribuição HA

Uma vez atribuída e salva a política, o FMC a aplica automaticamente ao FTD.

Etapa 3. Alertas de eventos de failover

Dependendo da configuração do HA, quando um evento de failover é acionado, os alertas pop-up que descrevem a falha de failover são mostrados.

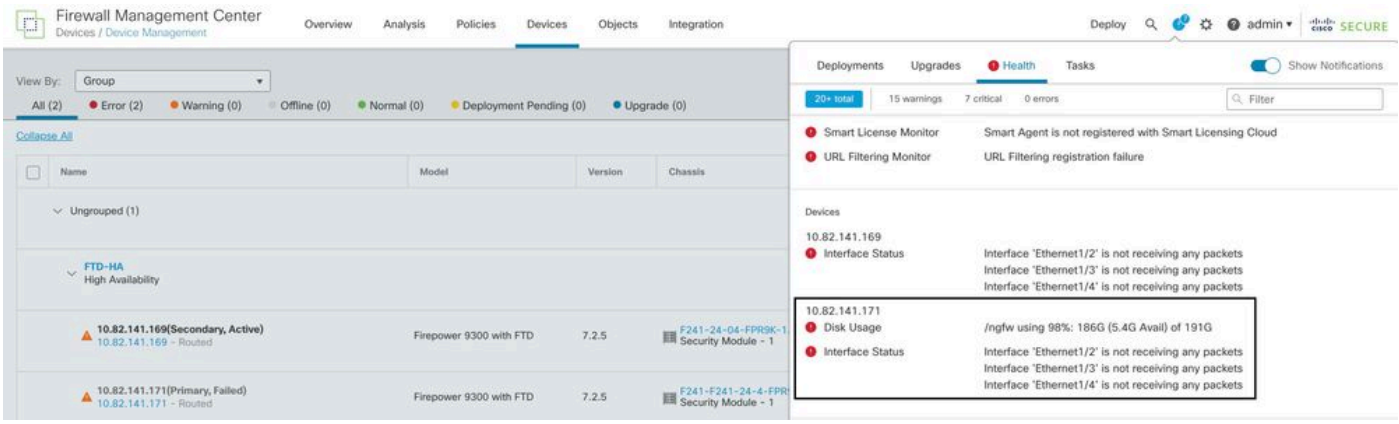
Esta imagem mostra os alertas de failover gerados:



Alertas de failover

Você também pode navegar para Notifications > Health para visualizar os alertas de integridade de failover.

Esta imagem mostra os alertas de failover em notificações:

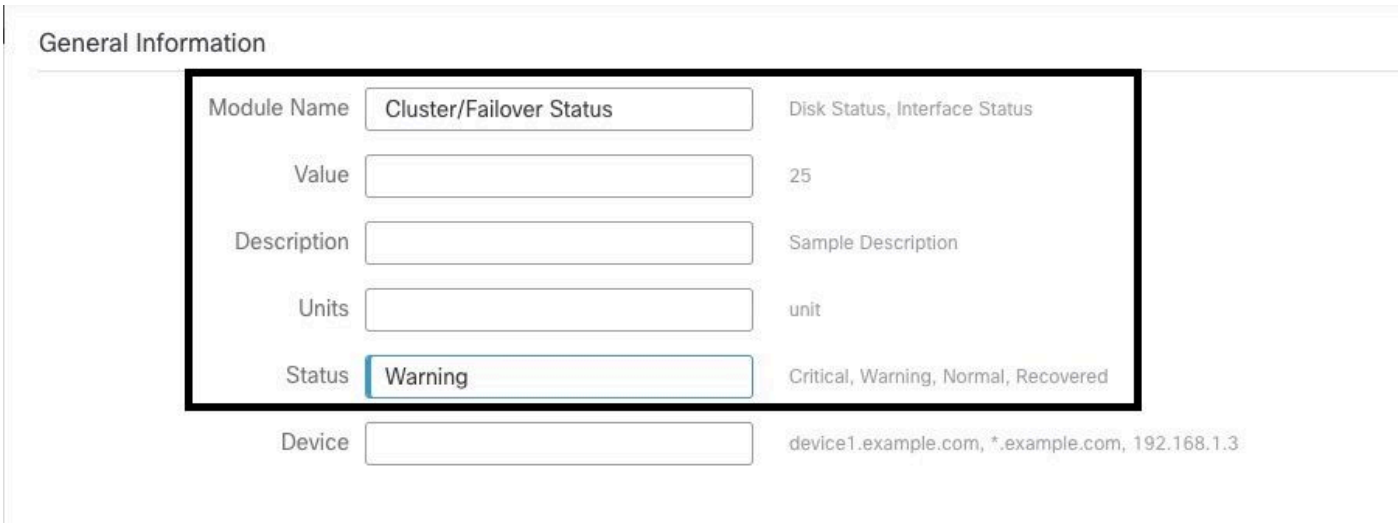


Notificações HA

Etapa 4. Eventos Históricos de Failover

O FMC fornece uma maneira de visualizar eventos de failover que ocorreram no passado. Para filtrar os eventos, navegue até System > Health > Events > Edit Search e especifique o Nome do módulo como Status do cluster/failover. Além disso, o filtro pode ser aplicado com base no Status.

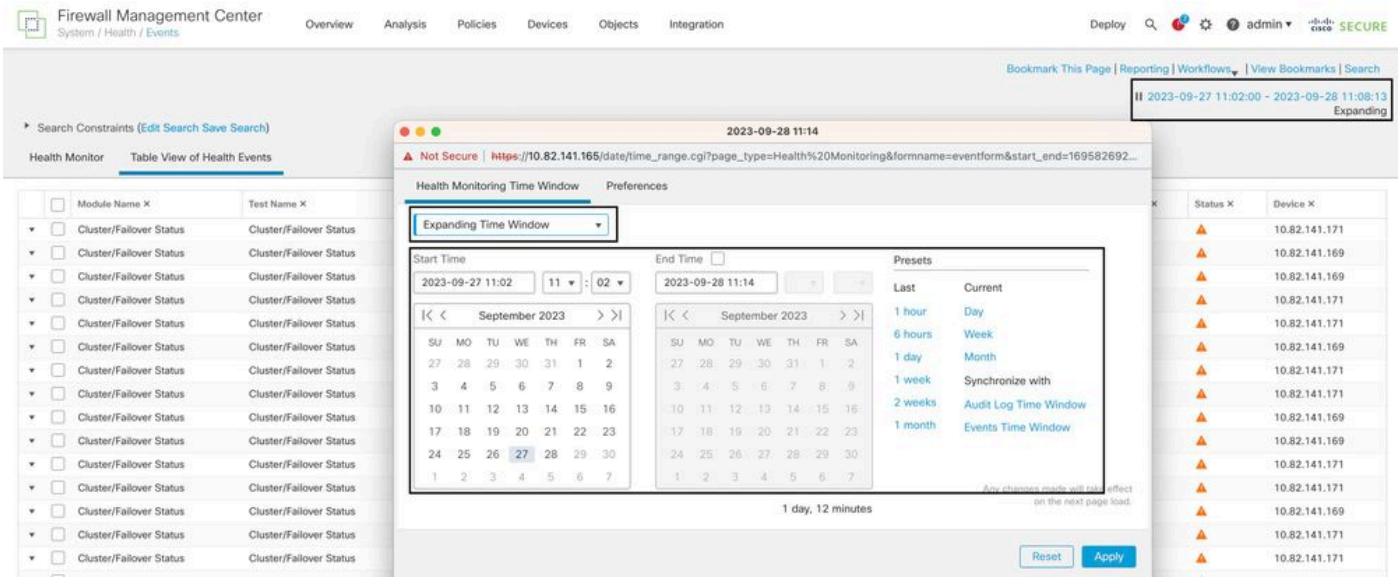
Esta imagem mostra como filtrar eventos de failover:



Mensagens de filtro de failover

Você pode ajustar as configurações de hora para exibir os eventos de uma data e hora específicas. Para modificar as configurações de hora, navegue até System > Health > Events > Time.

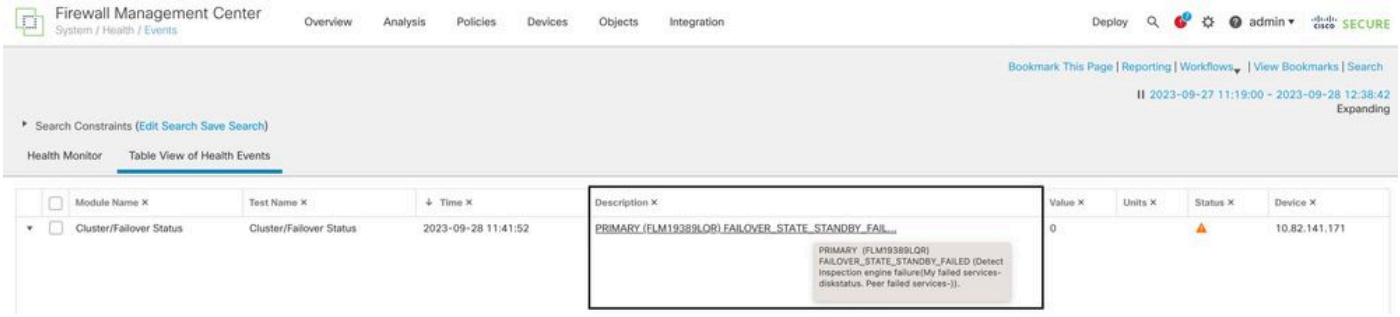
Esta imagem mostra como editar as configurações de hora:



Filtro de tempo

Uma vez identificados os eventos, para confirmar a razão do evento, aponte o cursor em Descrição.

Esta imagem mostra como o motivo do failover pode ser visto.



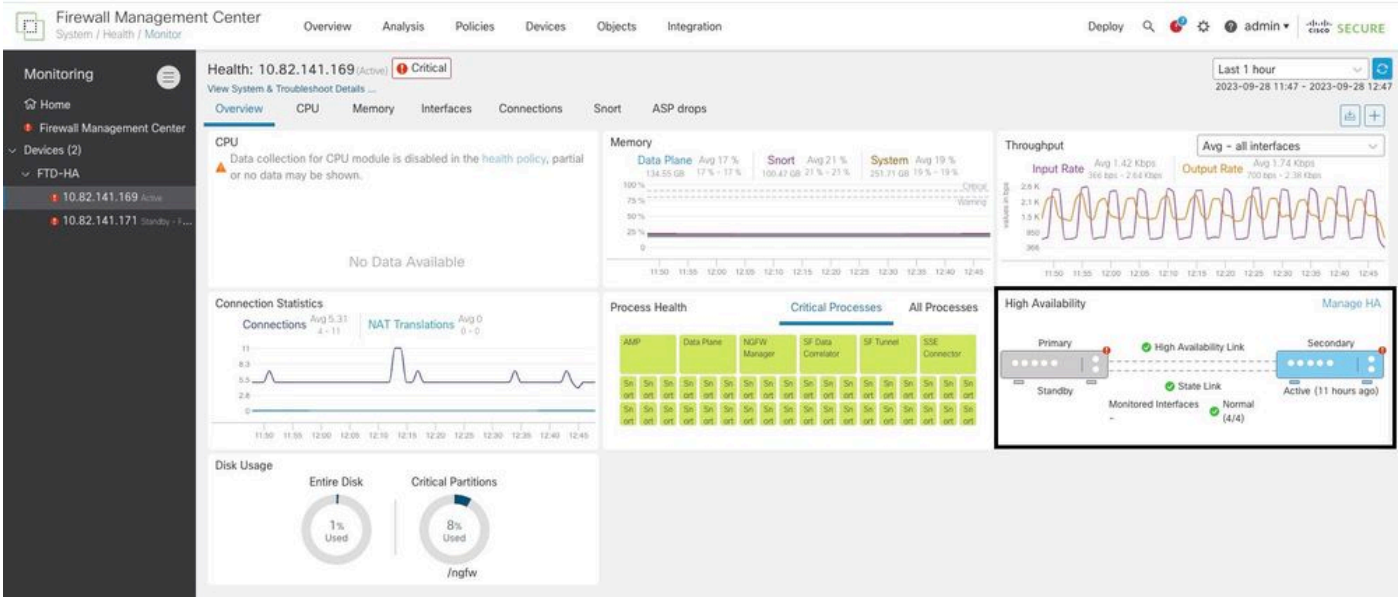
detalhes de failover

Etapa 5. Painel de Alta Disponibilidade

Outra maneira de monitorar o failover pode ser encontrada em System > Health Montitor > Select Active or Standby Unit.

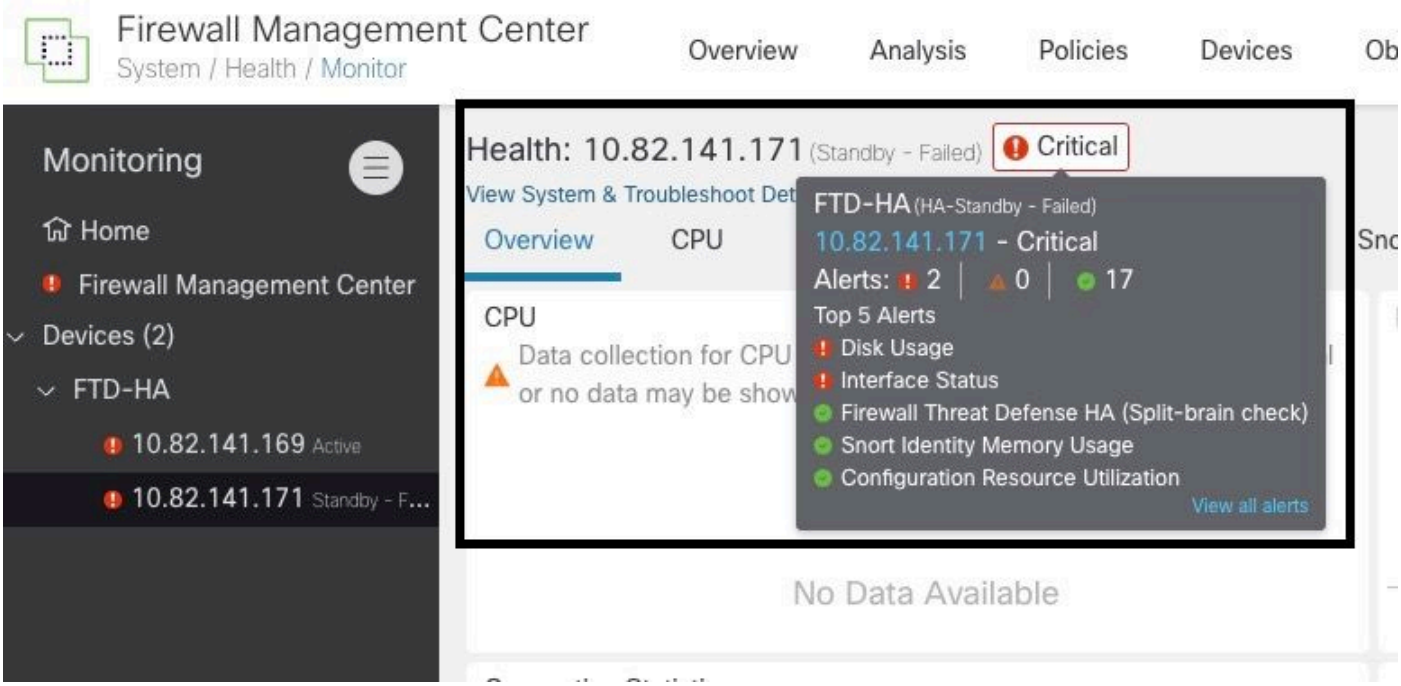
O monitor HA fornece informações sobre o status do HA e do link de estado, interfaces monitoradas, ROL e o status dos alertas em cada unidade.

Esta imagem mostra o Monitor HA:



Gráficos de integridade

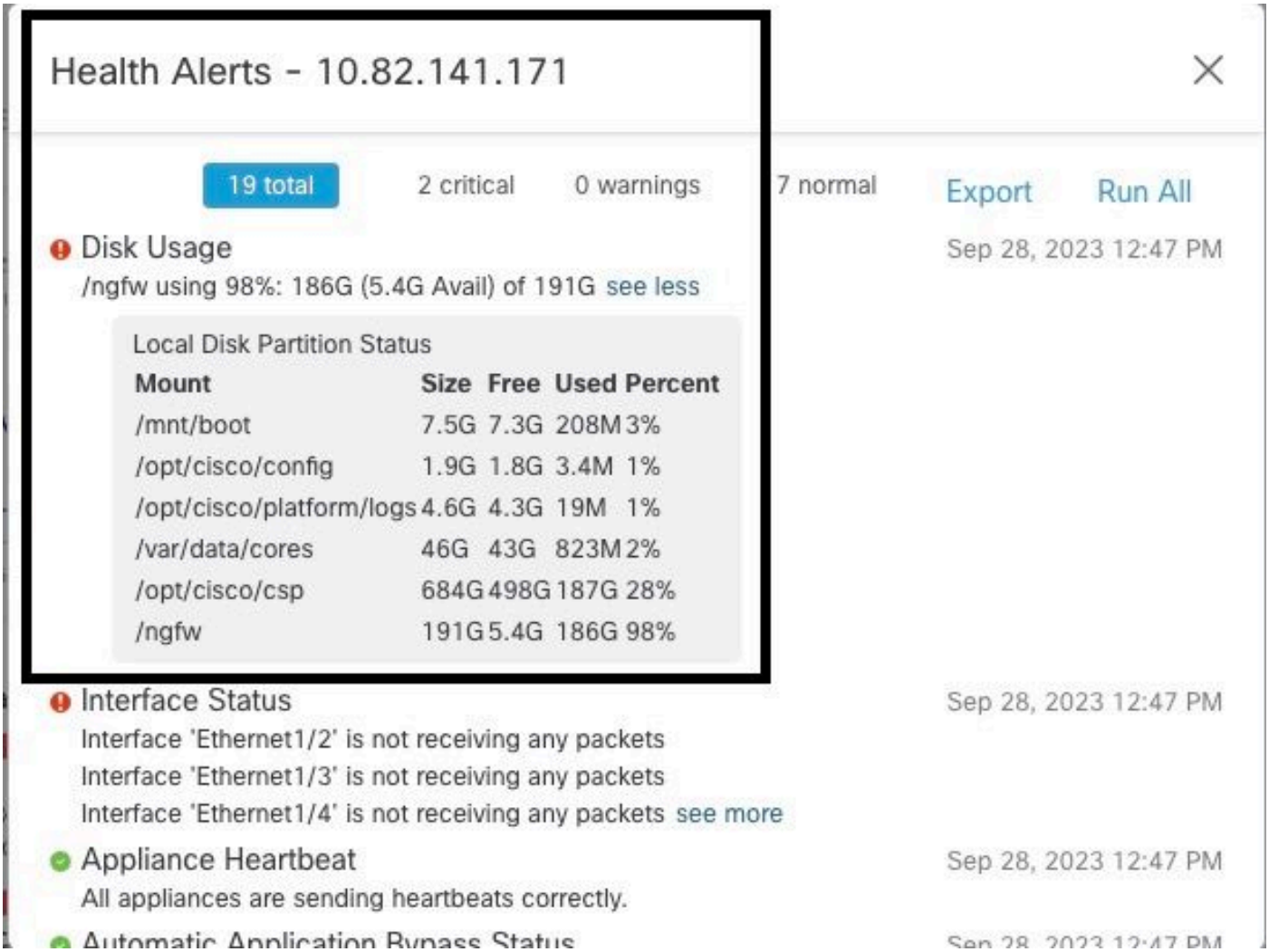
Para visualizar os alertas, navegue até System > Health Montitor > Select Active or Standby Unit > Select the Alerts.



Alertas

Para obter mais detalhes sobre os alertas, escolha View all alerts > see more.

Esta imagem mostra o status do disco que causou o failover:

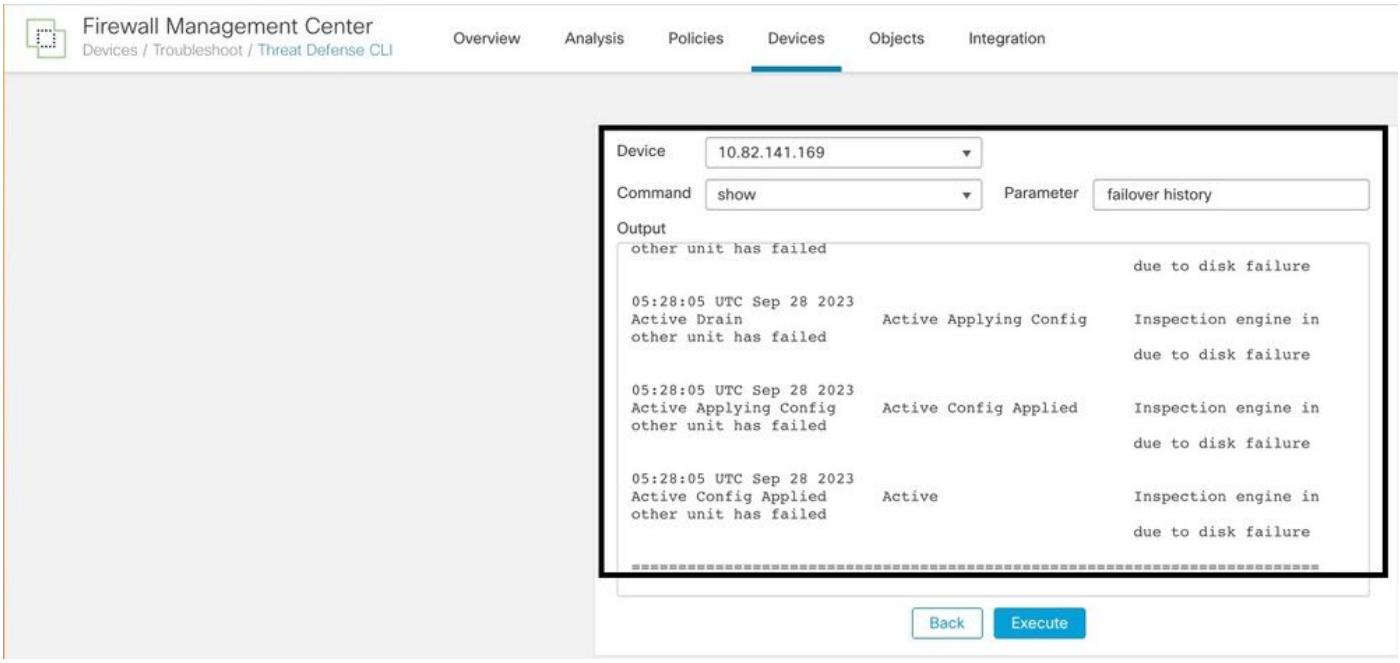


detalhes do alerta

Etapa 6. Defesa contra ameaças CLI

Por último, para recolher informações adicionais sobre o CVP, pode Devices > Troubleshoot > Threat Defense CLI. Configure os parâmetros como Dispositivo e o comando a ser executado e clique em Execute.

Esta imagem mostra um exemplo do comando show failover history que pode ser executado no FMC, onde você pode identificar a falha de failover.



histórico de failover

Informações Relacionadas

- Alta disponibilidade para FTD
- Configurar a alta disponibilidade do FTD em dispositivos Firepower
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.