

Identifizieren und Analysieren von FTD-Failover-Ereignissen auf FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Failover-Ereignisse auf FMC](#)

[Schritt 1: Konfiguration der Integritätsrichtlinie](#)

[Schritt 2: Richtlinienzuweisung](#)

[Schritt 3: Failover-Ereigniswarnungen](#)

[Schritt 4: Verlaufereignisse für Failover](#)

[Schritt 5: Hochverfügbarkeits-Dashboard](#)

[Schritt 6: Threat Defence-CLI](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Failover-Ereignisse für die sichere Firewall-Bedrohungsabwehr auf der Benutzeroberfläche des Secure Firewall Management Center identifiziert und analysiert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Hochverfügbarkeits-Setup für Cisco Secure Firewall Threat Defense (FTD)
- Grundlegende Benutzerfreundlichkeit des Cisco Firewall Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FMC v7.2.5
- Cisco Firepower der Serie 9300 v7.2.5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das FMC ist nicht nur das Verwaltungszentrum für FirePOWER-Geräte, es bietet neben den Verwaltungs- und Konfigurationsoptionen auch eine grafische Oberfläche, mit der Protokolle und Ereignisse in Echtzeit und in der Vergangenheit analysiert werden können.

Wenn wir über Failover sprechen, hat die Schnittstelle neue Verbesserungen, die helfen, Failover-Ereignisse zu analysieren, um die Fehler zu verstehen.

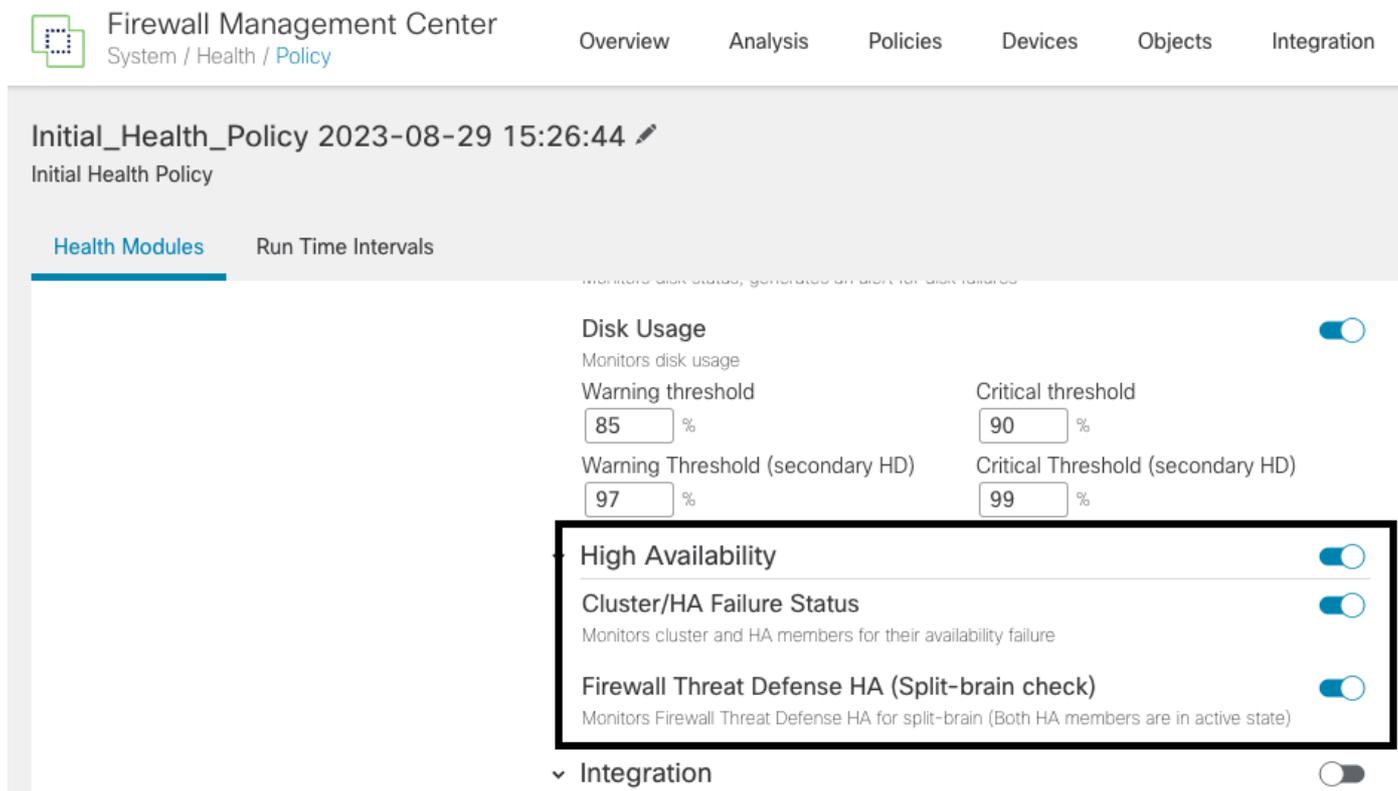
Failover-Ereignisse auf FMC

Schritt 1: Konfiguration der Integritätsrichtlinie

Das Modul Cluster-/HA-Fehlerstatus ist standardmäßig in der Integritätsrichtlinie aktiviert. Zusätzlich können Sie die Option Split-brain check aktivieren.

Um die Optionen für HA in der Integritätsrichtlinie zu aktivieren, navigieren Sie zu `System > Health > Policy > Firewall Threat Defense Health Policy > High Availability`.

Dieses Bild beschreibt die HA-Konfiguration der Integritätsrichtlinie:



The screenshot shows the FMC interface for configuring the 'Initial Health Policy'. The 'Health Modules' section is active, and the 'High Availability' section is highlighted with a red box. The following table summarizes the configuration details:

Module	Description	Status
Disk Usage	Monitors disk usage	Enabled
Warning threshold	85 %	
Critical threshold	90 %	
Warning Threshold (secondary HD)	97 %	
Critical Threshold (secondary HD)	99 %	
High Availability		Enabled
Cluster/HA Failure Status	Monitors cluster and HA members for their availability failure	Enabled
Firewall Threat Defense HA (Split-brain check)	Monitors Firewall Threat Defense HA for split-brain (Both HA members are in active state)	Enabled
Integration		Disabled

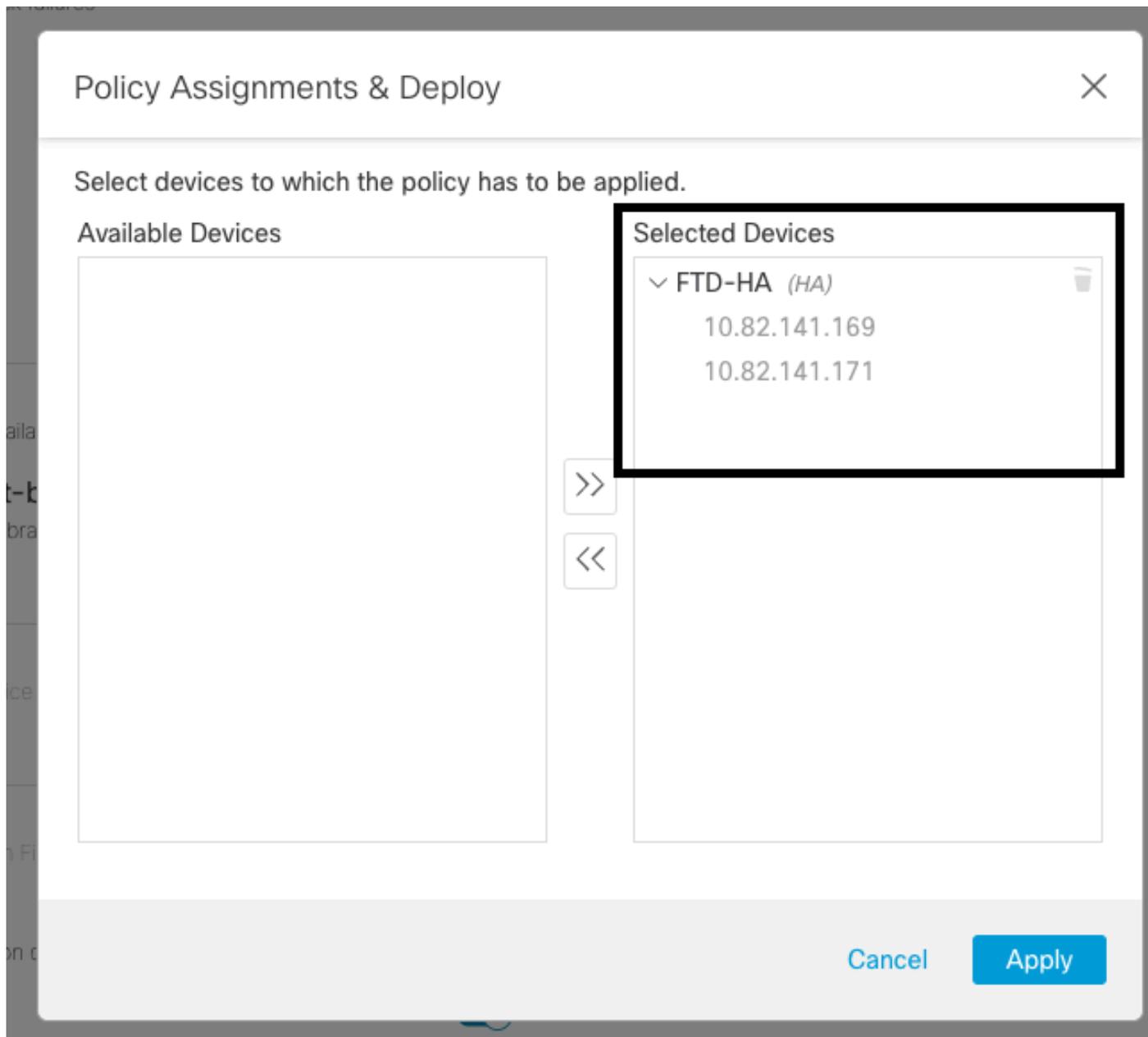
Einstellungen für Hochverfügbarkeit

Schritt 2: Richtlinienzuweisung

Stellen Sie sicher, dass die Integritätsrichtlinie den HA-Paaren zugewiesen ist, die Sie vom FMC aus überwachen möchten.

Um die Richtlinie zuzuweisen, navigieren Sie zu `System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy`.

Dieses Bild zeigt, wie Sie die Integritätsrichtlinie dem HA-Paar zuweisen:



HA-Zuweisung

Sobald die Richtlinie zugewiesen und gespeichert wurde, wendet das FMC sie automatisch auf das FTD an.

Schritt 3: Failover-Ereigniswarnungen

Je nach HA-Konfiguration werden nach Auslösung eines Failover-Ereignisses die eingeblendeten Warnfenster angezeigt, die den Failover-Fehler beschreiben.

Dieses Bild zeigt die generierten Failover-Warnungen:

The screenshot shows the FMC interface with a table of devices and a notification panel. The table has columns for Name, Version, Chassis, Licenses, and Access Control Policy. The notification panel on the right contains three alerts:

- Cluster/Failover Status - 10.82.141.169**: SECONDARY (FLM1946BCEX) FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services-. Peer failed services-diskstatus)) PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY (Check peer event for reason)
- Cluster/Failover Status - 10.82.141.171**: PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY (Other unit wants me Standby) PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY_FAILED (Detect Inspection engine failure(My failed services-diskstatus. Peer failed services-))
- Disk Usage - 10.82.141.171**: /ngfw using 98%: 186G (5.5G Avail) of 191G

Failover-Warmmeldungen

Sie können auch zu navigieren Notifications > Health um die Failover-Integritätswarnungen darzustellen.

Dieses Bild zeigt die Failover-Warnungen unter "Benachrichtigungen":

The screenshot shows the FMC interface with the 'Health' section selected. The left pane shows a list of devices with status indicators. The right pane shows a list of health alerts:

- Smart License Monitor**: Smart Agent is not registered with Smart Licensing Cloud
- URL Filtering Monitor**: URL Filtering registration failure
- Interface Status**: Interface 'Ethernet1/2' is not receiving any packets, Interface 'Ethernet1/3' is not receiving any packets, Interface 'Ethernet1/4' is not receiving any packets
- Disk Usage**: /ngfw using 98%: 186G (5.4G Avail) of 191G

HA-Benachrichtigungen

Schritt 4: Verlaufereignisse für Failover

Das FMC bietet eine Möglichkeit, Failover-Ereignisse zu visualisieren, die in der Vergangenheit aufgetreten sind. Um die Ereignisse zu filtern, navigieren Sie zu System > Health > Events > Edit Search und geben Sie den Modulnamen als Cluster-/Failover-Status an. Darüber hinaus kann der Filter basierend auf dem Status angewendet werden.

Dieses Bild zeigt, wie Failover-Ereignisse gefiltert werden:

General Information

Module Name	<input type="text" value="Cluster/Failover Status"/>	Disk Status, Interface Status
Value	<input type="text"/>	25
Description	<input type="text"/>	Sample Description
Units	<input type="text"/>	unit
Status	<input type="text" value="Warning"/>	Critical, Warning, Normal, Recovered
Device	<input type="text"/>	device1.example.com, *.example.com, 192.168.1.3

Failover-Filtermeldungen

Sie können die Zeiteinstellungen anpassen, um die Ereignisse für ein bestimmtes Datum und eine bestimmte Uhrzeit anzuzeigen. Um die Zeiteinstellungen zu ändern, navigieren Sie zu **System > Health > Events > Time**.

Dieses Bild zeigt, wie Sie die Zeiteinstellungen bearbeiten:

The screenshot shows the Firewall Management Center interface. The main window displays the 'Health Monitor' section with a 'Table View of Health Events'. A modal dialog titled 'Health Monitoring Time Window' is open, showing the 'Expanding Time Window' configuration. The dialog includes fields for 'Start Time' (2023-09-27 11:02) and 'End Time' (2023-09-28 11:14), along with calendar views for both. A 'Presets' section offers options like '1 hour', '6 hours', '1 day', '1 week', '2 weeks', and '1 month'. The 'Current' preset is set to 'Day'. The dialog also shows a 'Synchronize with' section with options for 'Audit Log Time Window' and 'Events Time Window'. The background shows a table of health events with columns for 'Module Name', 'Test Name', 'Status', and 'Device'.

Zeitfilter

Zeigen Sie nach der Identifizierung der Ereignisse mit dem Cursor unter Beschreibung, um den Grund für das Ereignis zu bestätigen.

Dieses Bild zeigt, wie der Grund für den Failover zu erkennen ist.

Module Name X	Test Name X	Time X	Description X	Value X	Units X	Status X	Device X
Cluster/Failover Status	Cluster/Failover Status	2023-09-28 11:41:52	PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAIL... PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure(My failed services-diskstatus. Peer failed services-)).	0		🚨	10.82.141.171

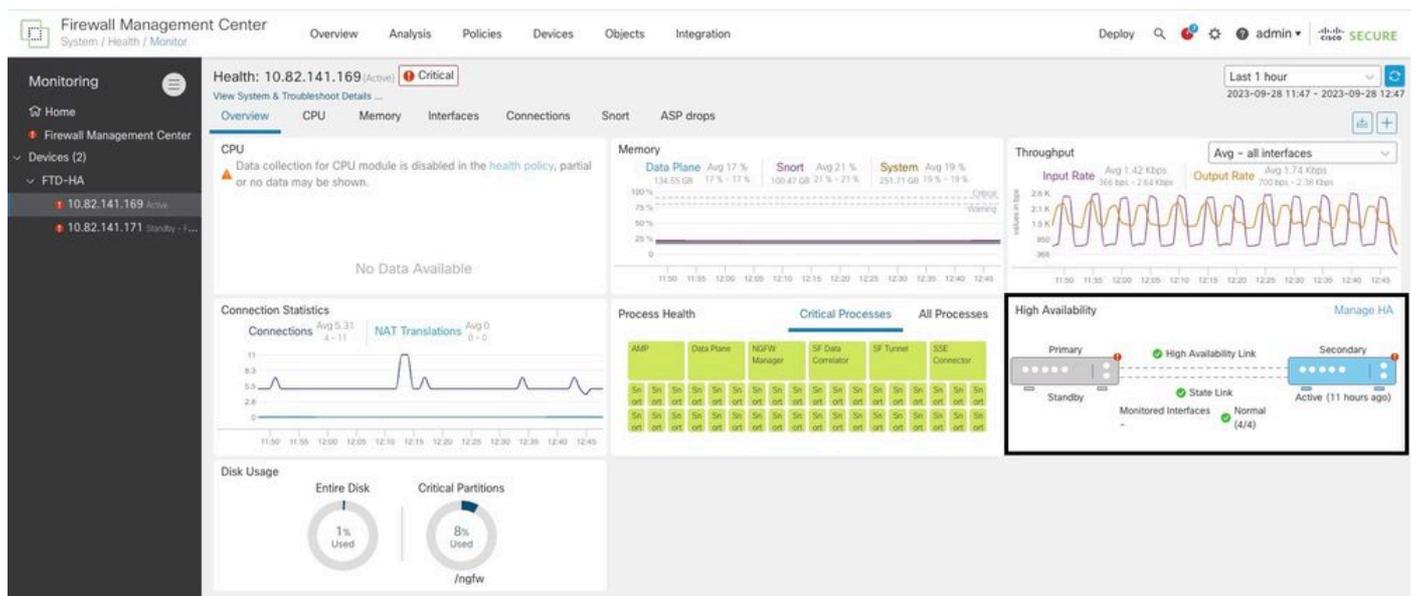
Failover-Details

Schritt 5: Hochverfügbarkeits-Dashboard

Eine weitere Möglichkeit zur Failover-Überwachung finden Sie unter System > Health Monitor > Select Active or Standby Unit.

Der HA-Monitor liefert Informationen über den Status der HA- und Statusverbindung, überwachte Schnittstellen, ROL und den Status der Warnmeldungen für jedes Gerät.

Dieses Bild zeigt den HA-Monitor:



Gesundheitsgrafik

Um die Warnungen anzuzeigen, navigieren Sie zu System > Health Monitor > Select Active or Standby Unit > Select the Alerts.



The screenshot shows the 'Monitoring' sidebar on the left with a menu icon. The main content area displays the health status for device 10.82.141.171, which is in a 'Standby - Failed' state and has a 'Critical' alert. A tooltip is open, showing details for 'FTD-HA (HA-Standby - Failed)' with 2 critical alerts and 17 warnings. The top 5 alerts listed are: Disk Usage, Interface Status, Firewall Threat Defense HA (Split-brain check), Snort Identity Memory Usage, and Configuration Resource Utilization. Below the tooltip, the text 'No Data Available' is visible.

Warnungen

Um weitere Details zu den Warnmeldungen zu erhalten, wählen Sie [View all alerts > see more](#).

Das folgende Bild zeigt den Festplattenstatus, der den Failover verursacht hat:

The screenshot shows a detailed view of health alerts for device 10.82.141.171. It indicates 19 total alerts, with 2 critical and 0 warnings. The primary alert is 'Disk Usage', where the /ngfw partition is 98% full (186G used, 5.4G available) out of 191G. A table provides the local disk partition status:

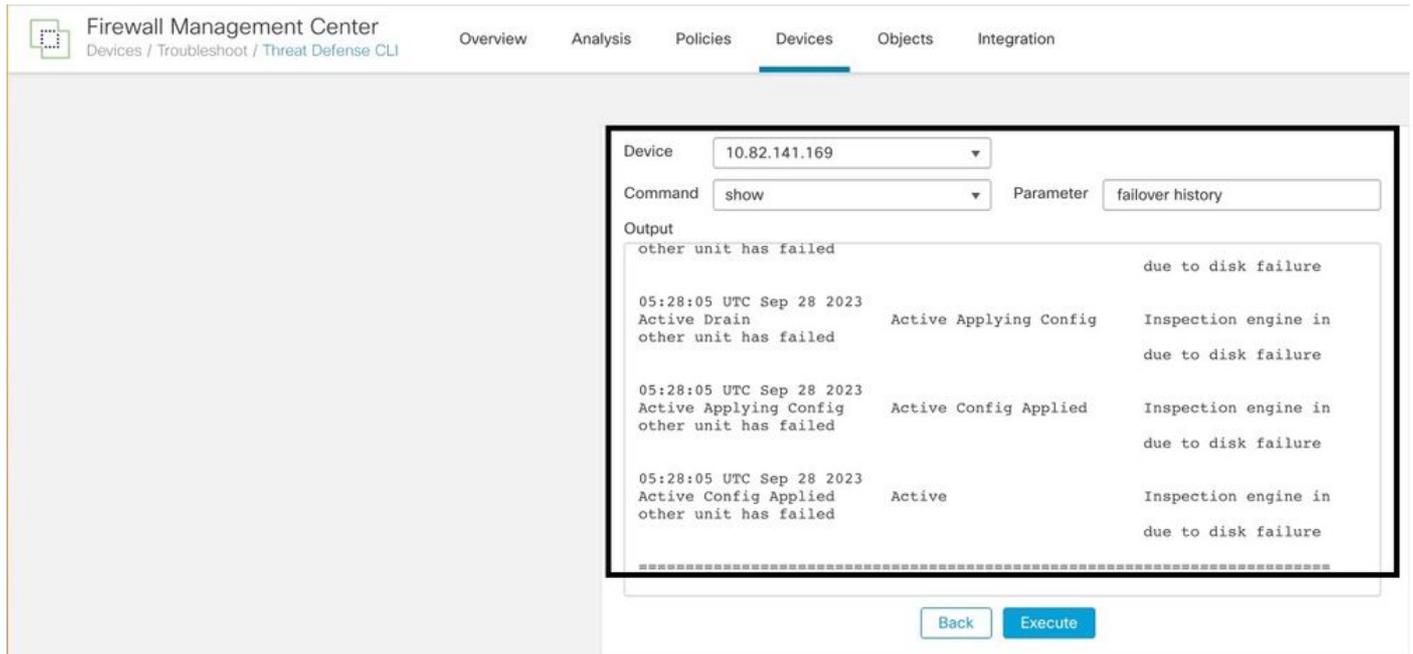
Mount	Size	Free	Used	Percent
/mnt/boot	7.5G	7.3G	208M	3%
/opt/cisco/config	1.9G	1.8G	3.4M	1%
/opt/cisco/platform/logs	4.6G	4.3G	19M	1%
/var/data/cores	46G	43G	823M	2%
/opt/cisco/csp	684G	498G	187G	28%
/ngfw	191G	5.4G	186G	98%

Other alerts include 'Interface Status' (Ethernet1/2, 1/3, and 1/4 are not receiving packets) and 'Appliance Heartbeat' (All appliances are sending heartbeats correctly).

Schritt 6: Threat Defence-CLI

Um weitere Informationen über FMC zu sammeln, können Sie abschließend unter `Devices > Troubleshoot > Threat Defense CLI`. Konfigurieren Sie die Parameter wie Gerät und den auszuführenden Befehl, und klicken Sie auf `Execute`.

Dieses Bild zeigt ein Beispiel für den Befehl `show failover history` die auf dem FMC ausgeführt werden kann, wo Sie den Ausfall eines Failovers identifizieren können.



Failover-Verlauf

Zugehörige Informationen

- [Hohe Verfügbarkeit für FTD](#)
- [Konfigurieren von FTD-Hochverfügbarkeit auf Firepower-Appliances](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.