

Identificare e analizzare gli eventi di failover FTD su FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Eventi di failover in FMC](#)

[Passaggio 1. Configurazione criteri di integrità](#)

[Passaggio 2. Assegnazione criteri](#)

[Passaggio 3. Avvisi sugli eventi di failover](#)

[Passaggio 4. Eventi di failover cronologici](#)

[Passaggio 5. Dashboard ad alta disponibilità](#)

[Passaggio 6. CLI di Threat Defense](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come identificare e analizzare gli eventi di failover per Secure Firewall Threat Defense sull'interfaccia utente di Secure Firewall Management Center.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di alta disponibilità (HA) per Cisco Secure Firewall Threat Defense (FTD)
- Usabilità di base di Cisco Firewall Management Center (FMC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Oltre a fornire funzionalità di gestione e configurazione, la console centrale di gestione dei dispositivi Firepower fornisce anche un'interfaccia grafica che consente di analizzare registri ed eventi in tempo reale e passato.

Quando si parla di failover, l'interfaccia presenta nuovi miglioramenti che consentono di analizzare gli eventi di failover per comprendere gli errori.

Eventi di failover in FMC

Passaggio 1. Configurazione criteri di integrità

Lo stato di errore del cluster/HA del modulo è abilitato per impostazione predefinita nel criterio di integrità, ma è inoltre possibile abilitare l'opzione di controllo Split-Brain.

Per abilitare le opzioni per HA nella politica sanitaria, passare a `System > Health > Policy > Firewall Threat Defense Health Policy > High Availability`.

Questa immagine descrive la configurazione HA del criterio di integrità:

Firewall Management Center
System / Health / Policy

Overview Analysis Policies Devices Objects Integration

Initial_Health_Policy 2023-08-29 15:26:44 ✎
Initial Health Policy

Health Modules Run Time Intervals

Disk Usage

Monitors disk usage

Warning threshold % Critical threshold %

Warning Threshold (secondary HD) % Critical Threshold (secondary HD) %

High Availability

Cluster/HA Failure Status
Monitors cluster and HA members for their availability failure

Firewall Threat Defense HA (Split-brain check)
Monitors Firewall Threat Defense HA for split-brain (Both HA members are in active state)

Integration

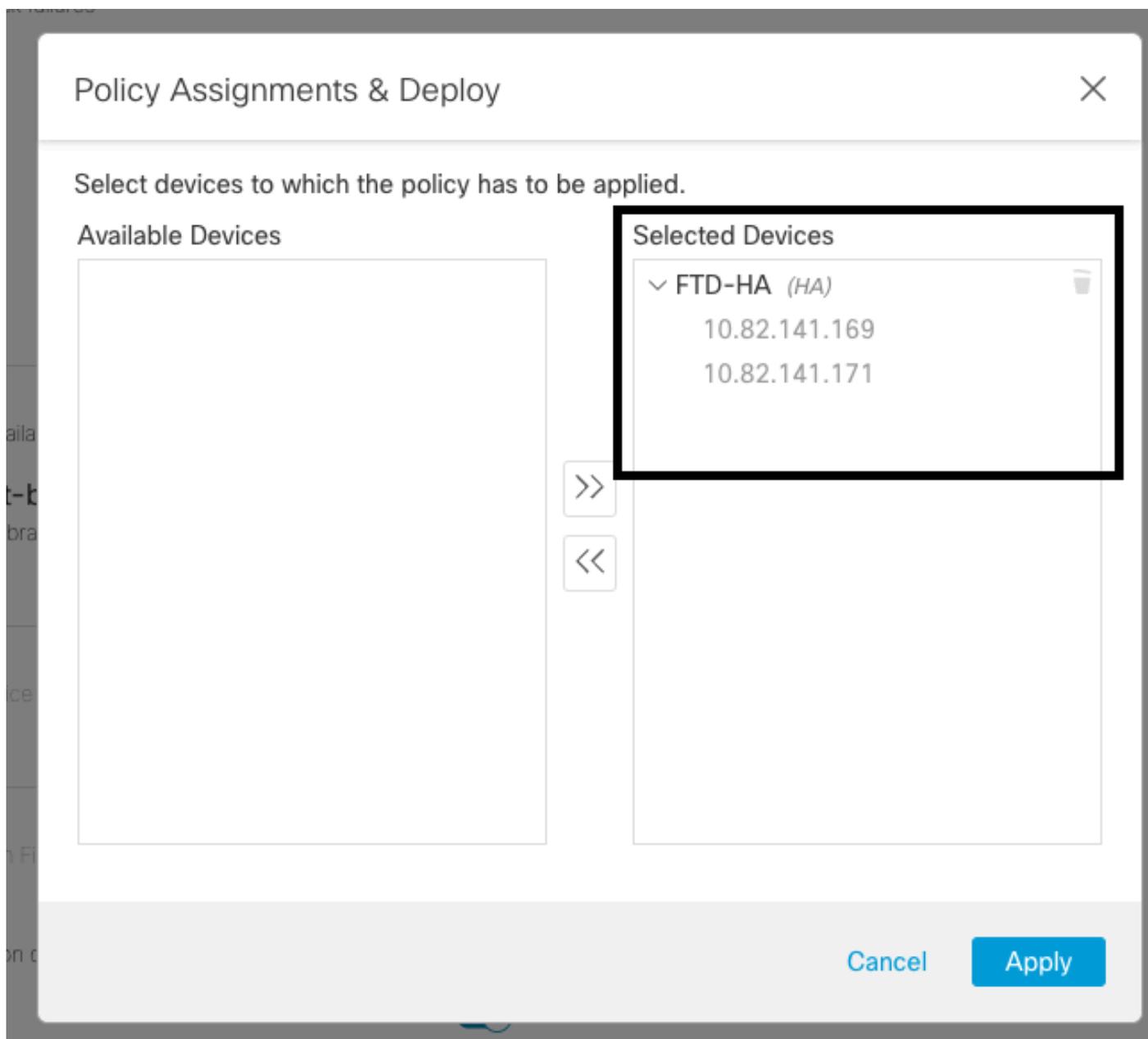
Impostazioni integrità alta disponibilità

Passaggio 2. Assegnazione criteri

Assicurarsi che il criterio di integrità sia assegnato alle coppie HA che si desidera monitorare dal CCP.

Per assegnare il criterio, passare a System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

In questa immagine viene illustrato come assegnare il criterio di integrità alla coppia HA:



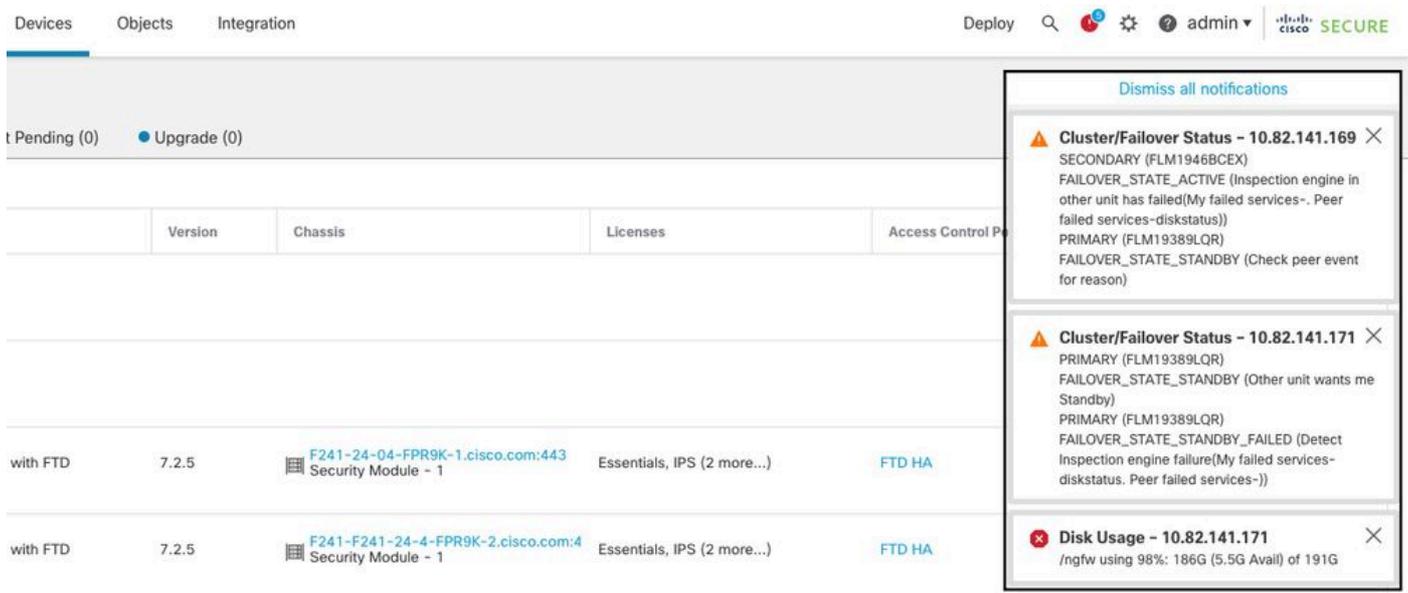
Assegnazione HA

Una volta assegnata e salvata la polizza, la FMC la applica automaticamente all'FTD.

Passaggio 3. Avvisi sugli eventi di failover

A seconda della configurazione di HA, dopo l'attivazione di un evento di failover vengono visualizzati gli avvisi popup che descrivono l'errore di failover.

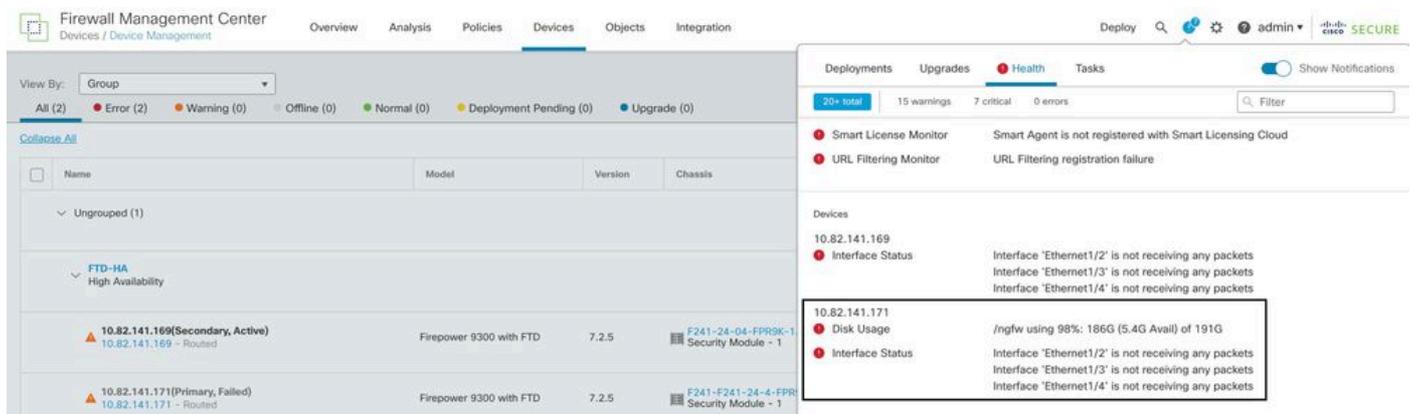
In questa immagine sono illustrati gli avvisi di failover generati:



Avvisi di failover

È inoltre possibile passare a [Notifications > Health](#) per visualizzare gli avvisi di integrità del failover.

In questa immagine sono illustrati gli avvisi di failover nelle notifiche:



Notifiche HA

Passaggio 4. Eventi di failover cronologici

In FMC è possibile visualizzare gli eventi di failover che si sono verificati in passato. Per filtrare gli eventi, passare a [System > Health > Events > Edit Search](#) e specificare il nome del modulo come Stato cluster/failover. Inoltre, il filtro può essere applicato in base allo stato.

In questa immagine viene illustrato come filtrare gli eventi di failover:

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

Messaggi filtro di failover

È possibile regolare le impostazioni dell'ora per visualizzare gli eventi relativi a una data e a un'ora specifiche. Per modificare le impostazioni dell'ora, passare a System > Health > Events > Time.

Nell'immagine viene mostrato come modificare le impostazioni relative all'ora:

The screenshot shows the Firewall Management Center interface. The main content area displays a table of health events with columns for 'Module Name X' and 'Test Name X'. A modal dialog titled 'Health Monitoring Time Window' is open, showing the 'Expanding Time Window' dropdown menu. The 'Start Time' is set to 2023-09-27 11:02 and the 'End Time' is set to 2023-09-28 11:14. The 'Presets' section shows options like '1 hour', '6 hours', '1 day', '1 week', '2 weeks', and '1 month'. The 'Current' preset is set to 'Day'. The 'Last' preset is set to 'Synchronize with'. The 'Events Time Window' is set to 'Audit Log Time Window'. The 'Apply' button is highlighted.

Filtro ora

Una volta identificati gli eventi, per confermare il motivo dell'evento, posizionare il cursore su Descrizione.

In questa immagine viene illustrato il motivo per cui è stato eseguito il failover.

Firewall Management Center
System / Health / Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

Bookmark This Page | Reporting | Workflows | View Bookmarks | Search

2023-09-27 11:19:00 - 2023-09-28 12:38:42 Expanding

Search Constraints (Edit Search Save Search)

Health Monitor Table View of Health Events

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

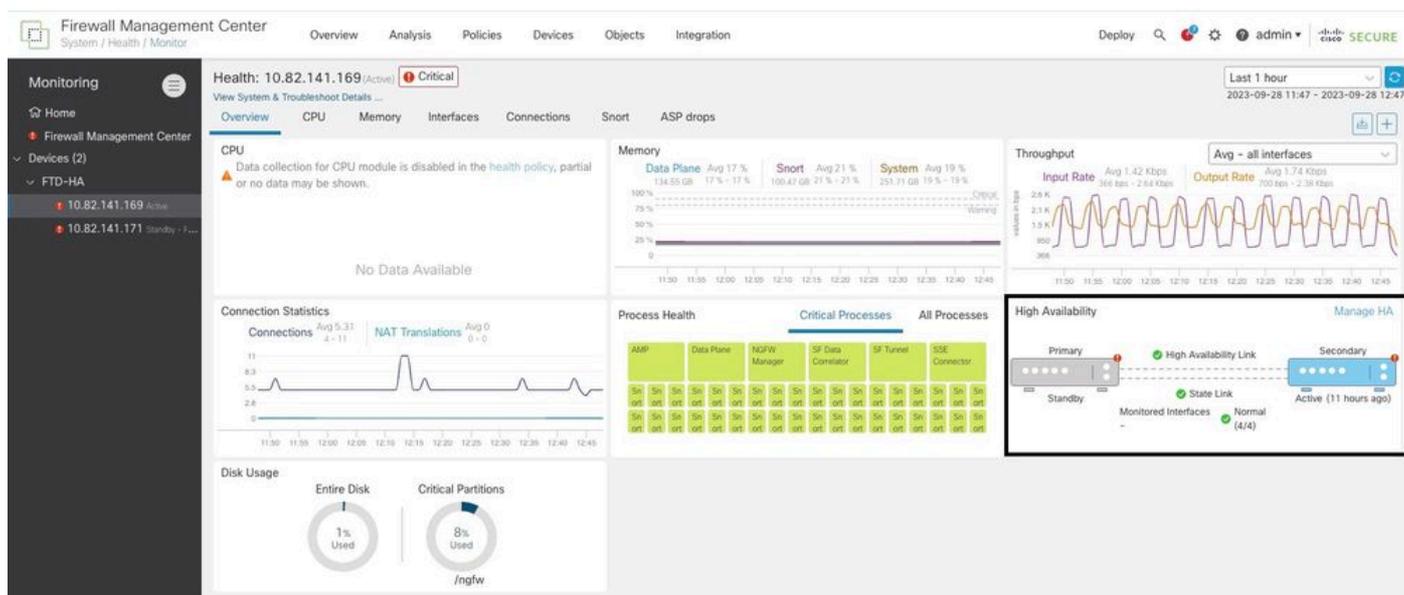
dettagli failover

Passaggio 5. Dashboard ad alta disponibilità

Un altro modo per monitorare il failover è disponibile in System > Health Monitor > Select Active or Standby Unit.

Il monitor HA fornisce informazioni sullo stato dell'HA e del collegamento di stato, sulle interfacce monitorate, sul ROL e sullo stato degli allarmi su ciascuna unità.

L'immagine mostra il monitor HA:



Grafica dello stato

Per visualizzare gli avvisi, passare a System > Health Monitor > Select Active or Standby Unit > Select the Alerts.



Monitoring

- Home
- Firewall Management Center
- Devices (2)
 - FTD-HA
 - 10.82.141.169 Active
 - 10.82.141.171 Standby - F...

Health: 10.82.141.171 (Standby - Failed) **Critical**

View System & Troubleshoot Det

Overview CPU

CPU

Data collection for CPU or no data may be show

FTD-HA (HA-Standby - Failed)

10.82.141.171 - Critical

Alerts: 2 | 0 | 17

Top 5 Alerts

- Disk Usage
- Interface Status
- Firewall Threat Defense HA (Split-brain check)
- Snort Identity Memory Usage
- Configuration Resource Utilization

[View all alerts](#)

No Data Available

Avvisi

Per ulteriori dettagli sugli avvisi, scegliere [View all alerts > see more.](#)

In questa immagine viene mostrato lo stato del disco che ha causato il failover:

Health Alerts - 10.82.141.171

19 total 2 critical 0 warnings 7 normal

[Export](#) [Run All](#)

Sep 28, 2023 12:47 PM

Disk Usage

/ngfw using 98%: 186G (5.4G Avail) of 191G [see less](#)

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%

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 [see more](#)

Appliance Heartbeat

All appliances are sending heartbeats correctly.

Automatic Application Runas Status

Sep 28, 2023 12:47 PM

Passaggio 6. CLI di Threat Defense

Infine, per raccogliere ulteriori informazioni su FMC, è possibile passare a `Devices > Troubleshoot > Threat Defense CLI`. Configurare i parametri come Device e il comando da eseguire, quindi fare clic su `Execute`.

Nell'immagine è illustrato un esempio del comando `show failover history` che possono essere eseguiti sul CCP in cui è possibile identificare il guasto del failover.

Firewall Management Center
Devices / Troubleshoot / Threat Defense CLI

Overview Analysis Policies **Devices** Objects Integration

Device: 10.82.141.169
Command: show
Parameter: failover history

Output

```
other unit has failed                                due to disk failure  
  
05:28:05 UTC Sep 28 2023  
Active Drain                                         Active Applying Config  Inspection engine in  
other unit has failed                                due to disk failure  
  
05:28:05 UTC Sep 28 2023  
Active Applying Config                               Active Config Applied    Inspection engine in  
other unit has failed                                due to disk failure  
  
05:28:05 UTC Sep 28 2023  
Active Config Applied                               Active                   Inspection engine in  
other unit has failed                                due to disk failure  
=====
```

Back Execute

cronologia di failover

Informazioni correlate

- [Alta disponibilità per FTD](#)
- [Configurazione della funzionalità FTD High Availability nei dispositivi Firepower](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).