

Risoluzione dei problemi di elevata disponibilità di Firepower Threat Defense

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Opzioni di progettazione](#)

[Terminologia HA](#)

[Stati HA](#)

[Diagramma di flusso dello stato HA](#)

[Verifica interfaccia utente](#)

[FTD HA gestito Firepower Management Center](#)

[FTD FDM gestito HA](#)

[ASA HA gestita da ASDM](#)

[Firepower Chassis Manager per 4100/9300 con FTD/ASA HA](#)

[Verifica della CLI](#)

[Risoluzione dei problemi](#)

[Scenari](#)

[Errore di APP-SYNC](#)

[Il nodo in standby non riesce ad accedere a HA con "Errore di sincronizzazione dell'app CD in Applicazione configurazione app non riuscita"](#)

[Il nodo in standby non riesce a unirsi a HA con "progressione stato HA non riuscita a causa del timeout di SINCRONIZZAZIONE APP"](#)

[Il nodo in standby non riesce a unirsi a HA con "Errore di sincronizzazione dell'app su CD Impossibile applicare la configurazione del provider di servizi condivisi in standby"](#)

[Controllo stato non riuscito](#)

[Spegnimento o errore del disco](#)

[Il motore di rilevamento \(istanza SNORT\) è inattivo](#)

[Il Dispositivo Mostra Un Utilizzo Elevato Del Disco](#)

[Errore della scheda di servizio](#)

[Errore heartbeat MIO](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il funzionamento, la verifica e le procedure di risoluzione dei problemi per High Availability (HA) su Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Piattaforme FTD e ASA
- Acquisizione di pacchetti su appliance FTD

Si consiglia vivamente di leggere la guida alla configurazione di Firepower [Configure FTD High Availability on Firepower Appliance](#) per una migliore comprensione dei concetti descritti in questo documento.

Componenti usati

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

- Cisco FTD
- Cisco Firepower Management Center (FMC)

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

Le informazioni e gli esempi si basano sul FTD, ma la maggior parte dei concetti sono applicabili completamente anche alle appliance ASA (Adaptive Security Appliance).

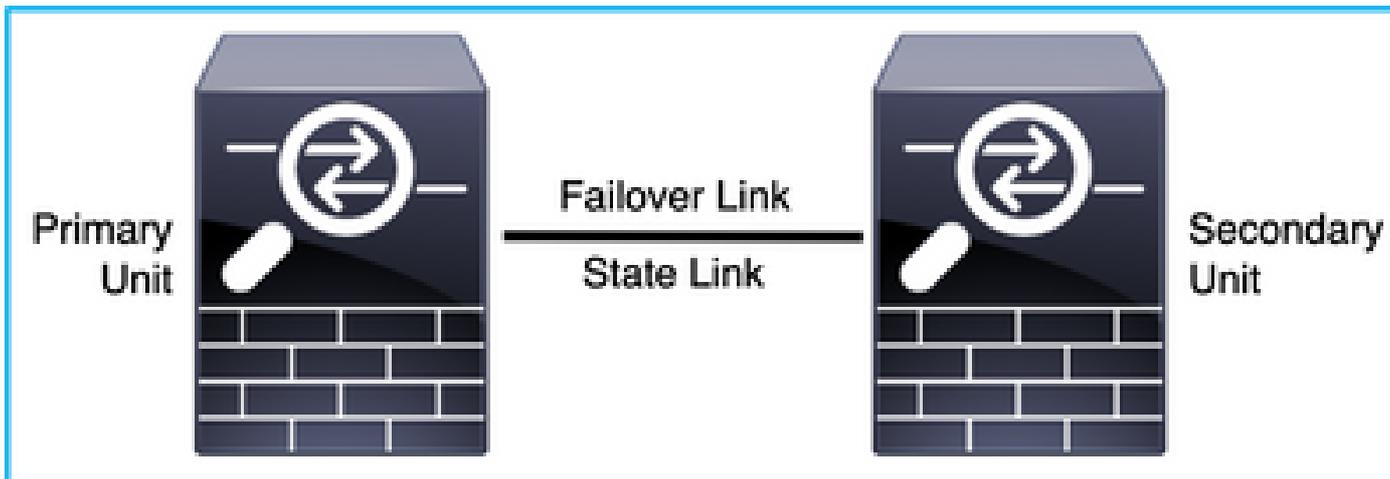
Un FTD supporta due modalità di gestione principali:

- Off-box tramite FMC (gestione remota)
- On-box tramite Firepower Device Manager (FDM), nota anche come gestione locale

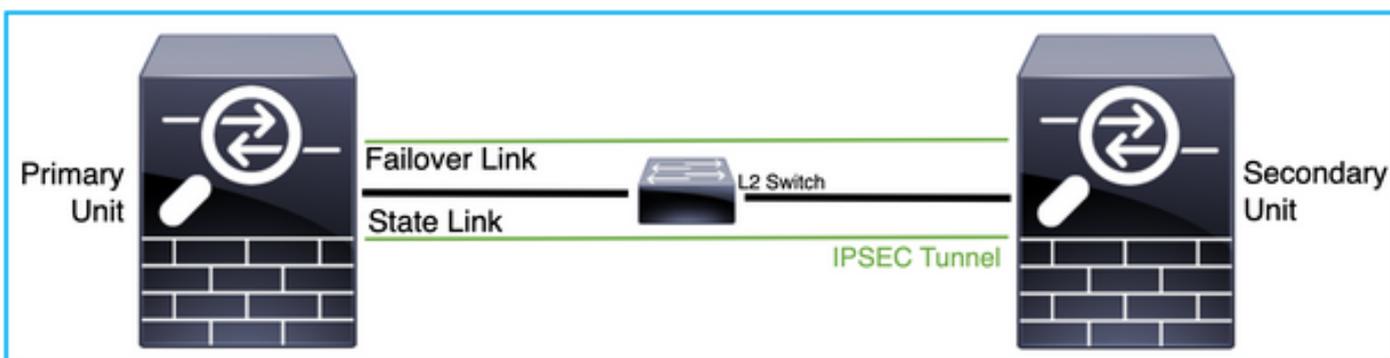
 Nota: FTD gestito tramite FDM può essere aggiunto in High Availability dal codice versione Firepower v6.3.0 in poi.

Opzioni di progettazione

Dal punto di vista della progettazione dell'FTD, è possibile collegarlo direttamente, come mostrato nella seguente immagine:



Oppure, è possibile collegarlo tramite lo switch di layer 2 (L2), come mostrato nell'immagine:



Terminologia HA

Active	L'appliance ASA attiva riceve tutti i flussi di traffico e filtra tutto il traffico di rete. Le modifiche alla configurazione vengono apportate sull'appliance ASA attiva.
Collegamento HA	<p>Le due unità di una coppia di failover comunicano costantemente tramite un collegamento di failover per determinare lo stato operativo di ogni unità e sincronizzare le modifiche alla configurazione. Le informazioni condivise tramite il collegamento sono:</p> <ul style="list-style-type: none"> • Lo stato dell'unità (attivo o standby) • Messaggi Hello (keep-alive) • Stato collegamento di rete • Scambio di indirizzi MAC • Replica e sincronizzazione della configurazione
Primario	Si tratta dell'unità generalmente configurata per prima quando si crea un HA. Il significato di ciò è che se entrambi i dispositivi di un'appliance ASA hanno uno stesso istante, il dispositivo primario assume il ruolo attivo.

Secondaria	Si tratta dell'unità generalmente configurata per seconda quando si crea un HA. Il significato di ciò è che, se entrambi i dispositivi di un'appliance ASA hanno lo stesso messaggio, il dispositivo secondario assume il ruolo di standby.
Standby	L'ASA in standby non gestisce alcun traffico in tempo reale, sincronizza le connessioni e la configurazione dal dispositivo attivo e svolge il ruolo attivo in caso di failover.
Collegamento stato	L'unità attiva utilizza il collegamento di stato per passare le informazioni sullo stato della connessione al dispositivo di standby. Pertanto, l'unità di standby può mantenere alcuni tipi di connessione e non influisce sull'utente. Queste informazioni consentono all'unità in standby di mantenere le connessioni esistenti quando si verifica un failover. NB: quando si utilizza lo stesso collegamento per il failover e il failover con conservazione dello stato, le interfacce vengono mantenute al meglio. Tuttavia, se si dispone di una configurazione di grandi dimensioni e di una rete a traffico elevato, è necessario prendere in considerazione un'interfaccia dedicata per il collegamento di stato e il collegamento di failover. È consigliabile che la larghezza di banda del collegamento di failover con stato corrisponda alla larghezza di banda più grande delle interfacce dati nel dispositivo.

Stati HA

Active	Il dispositivo attualmente gestisce il traffico in tempo reale sulla rete e tutte le modifiche di configurazione che è necessario apportare devono essere eseguite su questo dispositivo.
Sincronizzazione app	Il dispositivo in questo stato sincronizza la configurazione dal dispositivo attivo.
Sincronizzazione in blocco	Il dispositivo in questo stato sincronizza la configurazione dal dispositivo attivo.
Disabled	Il failover sull'unità è stato disabilitato (comando: nessun failover).
Negoziazione	Il dispositivo controlla la disponibilità del dispositivo attivo e assume il ruolo attivo se il dispositivo attivo non risulta pronto per lo standby.

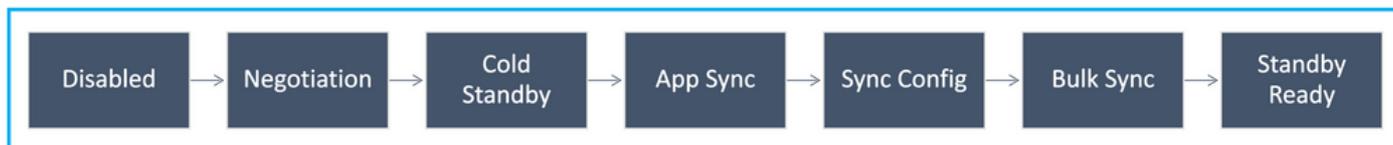
Pronto per lo standby	Il dispositivo attualmente non gestisce il traffico ma assume il ruolo attivo se il dispositivo attivo presenta problemi di controllo dello stato.
Configurazione sincronizzazione	La configurazione viene replicata dal dispositivo attivo al dispositivo di standby.
Standby a freddo	Il dispositivo assume il controllo come attivo al failover, ma non replica gli eventi di connessione.

Diagramma di flusso dello stato HA

Principale (senza peer connesso):



Secondario (con un peer connesso attivo):



Verifica interfaccia utente

FTD HA gestito Firepower Management Center

Lo stato HA FTD può essere controllato dall'interfaccia utente di FMC quando si passa a Device > Device Management, come mostrato nell'immagine seguente:

The screenshot shows the Cisco Firepower Management Center interface. The 'Devices' tab is selected, and the 'FTD-HA High Availability' group is expanded. The following table represents the data shown in the interface:

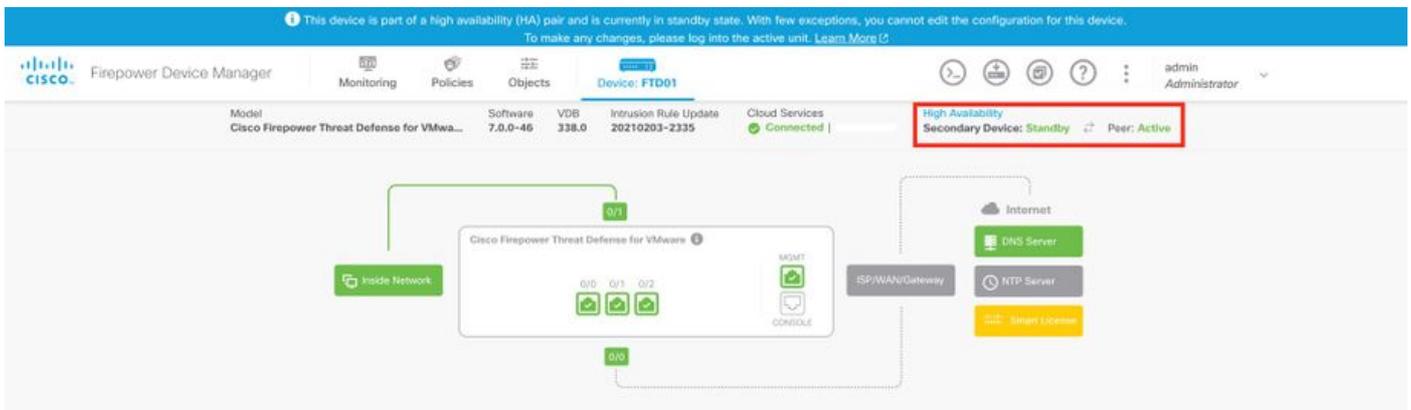
Name	Model	Version	Chassis	Licenses	Access Control Policy
FTD01(Primary, Active) Snort 3 10.197.224.69 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base
FTD02(Secondary, Standby) Snort 3 10.197.224.89 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base

FTD FDM gestito HA

Pagina Panoramica di FDM principale:



Pagina Panoramica di FDM secondario:



ASA HA gestita da ASDM

Home page ASDM sull'appliance ASA principale:

Cisco ASDM 7.12(2)14 for ASA - 10.106.47.62

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Device Dashboard

Device Information

General License Virtual Resources

Host Name: **ciscoasa**
 ASA Version: **9.12(3)12**
 ASDM Version: **7.12(2)14**
 Firewall Mode: **Routed**
 Total Flash: **8192 MB**

Device Uptime: **30d 20h 36m 28s**
 Device Type: **ASAv**
 Number of vCPUs: **8**
 Total Memory: **8192 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
backup	109.106.53.100/24	up	up	3
inside	10.106.60.55/24	up	up	1
management	10.106.47.62/24	up	up	5
outside	10.106.48.65/24	up	up	1

Select an interface to view input and output Kbps

Failover Status

This Host: **PRIMARY (Active)** Other Host: **SECONDARY (Standby Ready)**

VPN Summary

IPsec 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0

System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

Connections Per Second Usage

backlog

'backup' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

Enable Logging

Device configuration loaded successfully.

Active admin 15 25/11/21 2:40:45 AM UTC

Home page ASDM sull'appliance ASA secondaria:

Cisco ASDM 7.12(2)14 for ASA - 10.106.47.64

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Device Dashboard

Device Information

General License Virtual Resources

Host Name: **ciscoasa**
 ASA Version: **9.12(3)12**
 ASDM Version: **7.12(2)14**
 Firewall Mode: **Routed**
 Total Flash: **8192 MB**

Device Uptime: **30d 20h 39m 10s**
 Device Type: **ASAv**
 Number of vCPUs: **8**
 Total Memory: **8192 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
backup	no ip address	up	up	2
inside	no ip address	up	up	1
management	10.106.47.64/24	up	up	89
outside	no ip address	up	up	1

Select an interface to view input and output Kbps

Failover Status

This Host: **SECONDARY (Standby Ready)** Other Host: **PRIMARY (Active)**

VPN Summary

IPsec 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0

System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

Connections Per Second Usage

backlog

'backup' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

Enable Logging

Device configuration loaded successfully.

Standby admin 15 25/11/21 2:43:25 AM UTC

Firepower Chassis Manager per 4100/9300 con FTD/ASA HA

Pagina Dispositivo logico FCM primario:

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (1 Instance) 0% (0 of 70) Cores Available Refresh Add

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
ASA	9.12.4.18		10.197.216.7	10.197.216.1	Ethernet1/7	Online

Interface Name	Type	Attributes
Ethernet1/1	data	Cluster Operational Status : not-applicable
Ethernet1/2	data	HA-LINK-INTF : Ethernet3/7
Ethernet1/3	data	HA-LAN-INTF : Ethernet3/7
Ethernet1/4	data	HA-ROLE : active
Ethernet1/5	data	
Ethernet1/6	data	
Ethernet1/8	data	
Ethernet3/7	data	
Ethernet3/8	data	

Pagina Dispositivo logico FCM secondario:

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (1 Instance) 0% (0 of 70) Cores Available Refresh Add

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
ASA	9.12.4.18		10.197.216.8	10.197.216.1	Ethernet1/7	Online

Interface Name	Type	Attributes
Ethernet1/1	data	Cluster Operational Status : not-applicable
Ethernet1/2	data	HA-LINK-INTF : Ethernet3/7
Ethernet1/3	data	HA-LAN-INTF : Ethernet3/7
Ethernet1/4	data	HA-ROLE : standby
Ethernet1/5	data	
Ethernet1/6	data	
Ethernet1/8	data	
Ethernet3/7	data	
Ethernet3/8	data	

Verifica della CLI

<#root>

>

```
show running-config failover
```

```
failover
```

```
failover lan unit secondary
```

```
failover lan interface failover-link GigabitEthernet0/2
```

```
failover replication http
```

```
failover link failover-link GigabitEthernet0/2
```

```
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89
```

I punti importanti da considerare in questo contesto sono i seguenti:

failover

failover unità lan secondaria —> se l'unità è primaria o secondaria

failover interfaccia lan collegamento di failover Gigabit Ethernet0/2 —> collegamento di failover

interfaccia fisica sul dispositivo

http per la replica di failover

collegamento di failover collegamento di failover Gigabit Ethernet0/2

failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89 —> indirizzo ip del collegamento di failover del dispositivo primario e del dispositivo di standby.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(0)26, Mate 9.16(0)26
Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12
Last Failover at: 01:18:19 UTC Nov 25 2021
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys)
    Interface outside (0.0.0.0): Normal (Not-Monitored)
    Interface inside (192.168.45.2): Normal (Not-Monitored)
    Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
  Other host: Primary - Active
    Active time: 707216 (sec)
    Interface outside (0.0.0.0): Normal (Not-Monitored)
    Interface inside (192.168.45.1): Normal (Not-Monitored)
    Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
```

Stateful Failover Logical Update Statistics

```
Link : failover-link GigabitEthernet0/2 (up)
Stateful Obj      xmit      xerr      rcv      rerr
General          95752      0         115789    0
sys cmd          95752      0         95752     0
up time           0          0          0         0
RPC services      0          0          0         0
TCP conn          0          0          0         0
UDP conn          0          0          0         0
ARP tbl           0          0         20036     0
Xlate_Timeout     0          0          0         0
IPv6 ND tbl       0          0          0         0
VPN IKEv1 SA      0          0          0         0
VPN IKEv1 P2      0          0          0         0
VPN IKEv2 SA      0          0          0         0
VPN IKEv2 P2      0          0          0         0
VPN CTCP upd      0          0          0         0
VPN SDI upd       0          0          0         0
VPN DHCP upd      0          0          0         0
SIP Session       0          0          0         0
SIP Tx            0          0          0         0
```

SIP Pinhole	0	0	0	0
Route Session	0	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	1	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Rule DB B-Sync	0	0	0	0
Rule DB P-Sync	0	0	0	0
Rule DB Delete	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	5	504656
Xmit Q:	0	1	95752

Failover attivato: il failover è attivato o disattivato.

Host: secondario - pronto per lo standby. Ruolo del dispositivo e stati delle interfacce.

Altri host: Primary - Active. L'altro dispositivo è in stato Attivo e comunica con il dispositivo corrente.

<#root>

>

show failover history

```

=====
From State                To State                Reason
=====
01:18:14 UTC Nov 25 2021
Not Detected              Negotiation              No Error

01:18:27 UTC Nov 25 2021
Negotiation               Just Active              No Active unit found

01:18:27 UTC Nov 25 2021
Just Active               Active Drain              No Active unit found

01:18:27 UTC Nov 25 2021
Active Drain              Active Applying Config    No Active unit found

01:18:27 UTC Nov 25 2021
Active Applying Config    Active Config Applied     No Active unit found

01:18:27 UTC Nov 25 2021
Active Config Applied     Active                    No Active unit found
=====

```

Utilizzare questa opzione per verificare gli stati cronologici dei dispositivi e i motivi di tali

cambiamenti:

<#root>

>

```
show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Secondary Standby Ready	None	
Other host -	Primary Active	None	

====Configuration State====

Sync Done - STANDBY

====Communication State====

Mac set

Controllare gli stati correnti dei dispositivi e il motivo dell'ultimo failover:

Campo	Descrizione
Stato configurazione	<p>Visualizza lo stato della sincronizzazione della configurazione.</p> <p>Possibili stati di configurazione per l'unità di standby:</p> <ul style="list-style-type: none">• Config Syncing - STANDBY - Impostato durante l'esecuzione della configurazione sincronizzata.• Sincronizzazione configurazione interfaccia - STANDBY• Sync Done - STANDBY - Imposta quando l'unità di standby ha completato la sincronizzazione della configurazione dall'unità attiva. <p>Possibili stati di configurazione per l'unità attiva:</p> <ul style="list-style-type: none">• Sincronizzazione configurazione — impostata sull'unità attiva quando esegue una sincronizzazione della configurazione con l'unità di standby.• Sincronizzazione configurazione interfaccia• Sincronizzazione completata - Impostata quando l'unità attiva ha completato una corretta sincronizzazione della configurazione con l'unità di standby.• Pronto per la sincronizzazione della configurazione —Impostato sull'unità

Campo	Descrizione
	attiva quando l'unità di standby segnala che è pronta per ricevere una sincronizzazione della configurazione.
Stato comunicazione	<p>Visualizza lo stato della sincronizzazione degli indirizzi MAC.</p> <ul style="list-style-type: none"> • Mac set - Gli indirizzi MAC sono stati sincronizzati dall'unità peer all'unità. • Mac aggiornato - Utilizzato quando un indirizzo MAC viene aggiornato e deve essere sincronizzato con l'altra unità. Utilizzato anche al momento della transizione, in cui l'unità aggiorna gli indirizzi MAC locali sincronizzati dall'unità peer.
Data/ora	Visualizza la data e l'ora dell'errore.
Motivo ultimo errore	<p>Visualizza il motivo dell'ultimo errore segnalato. Queste informazioni non vengono cancellate, anche se la condizione di errore viene cancellata. Queste informazioni cambiano solo quando si verifica un failover.</p> <p>Possibili motivi:</p> <ul style="list-style-type: none"> • Errore interfaccia: il numero di interfacce che non hanno soddisfatto i criteri di failover e hanno causato il failover. • Errore di comunicazione: il collegamento di failover non è riuscito o il peer non è attivo. • Errore backplane
State	Visualizza lo stato Principale/Secondario e Attivo/Standby per l'unità.
Host corrente/altri host	Questo host indica le informazioni relative al dispositivo su cui è stato eseguito il comando. Un altro host indica le informazioni relative all'altro dispositivo nella coppia di failover.

<#root>

>

show failover descriptor

outside send: 00020000ffff0000 receive: 00020000ffff0000
inside send: 00020100ffff0000 receive: 00020100ffff0000

diagnostic send: 01020000ffff0000 receive: 01020000ffff0000

Risoluzione dei problemi

Debug

<#root>

>

debug fover ?

cable	Failover LAN status
cmd-exec	Failover EXEC command execution
fail	Failover internal exception
fmsg	Failover message
ifc	Network interface status trace
open	Failover device open
rx	Failover Message receive
rxdump	Failover rcv message dump (serial console only)
rxip	IP network failover packet rcv
snort	Failover NGFW mode snort processing
switch	Failover Switching status
sync	Failover config/command replication
tx	Failover Message xmit
txdump	Failover xmit message dump (serial console only)
txip	IP network failover packet xmit
verify	Failover message verify

Clip:

Acquisizioni interfaccia di failover:

È possibile fare riferimento a questa acquisizione per determinare se i pacchetti hello di failover vengono inviati sul collegamento di failover alla velocità alla quale vengono inviati.

<#root>

>

show capture

```
capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
```

>

show capture capfail

15 packets captured

```
1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

Acquisizione ARP sul collegamento di failover:

È possibile eseguire questa acquisizione per verificare se i peer dispongono di voci Mac nella tabella ARP.

```
<#root>
```

```
>
```

```
show capture
```

```
capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes]
>
```

```
show capture caparp
```

22 packets captured

```
1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
```

```
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
>
```

Scenari

Se l'unità peer non riesce a unirsi al gruppo HA oppure si verifica un errore durante la distribuzione delle modifiche dall'unità attiva, accedere all'unità guasta, passare alla pagina Alta disponibilità e fare clic sul collegamento Cronologia failover.

Errore di APP-SYNC

Se l'output show failover history indica un errore di sincronizzazione dell'app, si è verificato un problema al momento della fase di convalida HA, in cui il sistema verifica che le unità possano funzionare correttamente come gruppo ad alta disponibilità.

Viene visualizzato il messaggio "Tutte le convalide passate" quando lo stato Da è Sincronizzazione app e il nodo passa allo stato Pronto per standby.

In caso di errore di convalida, il peer passa allo stato Disabilitato (Non riuscito). Risolvere i problemi per fare in modo che i peer funzionino di nuovo come gruppo a disponibilità elevata.

Si noti che se si corregge un errore di sincronizzazione dell'app e si apportano modifiche all'unità attiva, è necessario distribuirle e quindi riprendere HA affinché il nodo peer possa essere aggiunto.

I messaggi indicano gli errori e spiegano come risolvere i problemi. Questi errori possono verificarsi in un join di nodo e in ogni distribuzione successiva.

Al momento dell'aggiunta di un nodo, il sistema esegue un controllo rispetto all'ultima configurazione distribuita sull'unità attiva.

Il nodo in standby non riesce ad accedere a HA con "Errore di sincronizzazione dell'app CD in Applicazione configurazione app non riuscita"

Sulla riga di comando di Standby FTD, /ngfw/var/log/action_queue.log deve avere il motivo dell'errore di configurazione.

Correzione: una volta identificato l'errore di configurazione, dopo aver apportato le modifiche necessarie, è possibile riprendere la funzione HA.

Vedere Cisco bug [IDCSCvu1561](#).

<#root>

```

=====
From State          To State          Reason
=====
15:10:16 CDT Sep 28 2021
Not Detected       Disabled          No Error
15:10:18 CDT Sep 28 2021
Disabled          Negotiation      Set by the config command
15:10:24 CDT Sep 28 2021
Negotiation       Cold Standby     Detected an Active mate
15:10:25 CDT Sep 28 2021
Cold Standby      App Sync         Detected an Active mate
15:10:55 CDT Sep 28 2021
App Sync          Disabled
CD App Sync error is App Config Apply Failed
=====

```

Il nodo in standby non riesce a unirsi a HA con "progressione stato HA non riuscita a causa del timeout di SINCRONIZZAZIONE APP"

Sulla riga di comando di Standby FTD, /ngfw/var/log/ngfwmanager.log deve avere il motivo per il timeout di app-sync.

In questa fase, anche le distribuzioni dei criteri hanno esito negativo perché l'unità attiva ritiene che la sincronizzazione delle app sia ancora in corso.

La distribuzione dei criteri genera l'errore: "poiché il processo di aggiunta a newNode/AppSync è in corso, le modifiche alla configurazione non sono consentite e pertanto la richiesta di distribuzione viene rifiutata. Riprovare la distribuzione in un secondo momento"

Risoluzione: talvolta, quando si riprende la disponibilità elevata sul nodo Standby, il problema può essere risolto.

Vedere l'ID bug Cisco [CSCvt48941](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvt48941)

Vedere l'ID bug Cisco [CSCvx1636](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvx1636)

<#root>

```

=====
From State          To State          Reason
=====
19:07:01 EST MAY 31 2021
Not Detected       Disabled          No Error
19:07:04 EST MAY 31 2021
Disabled          Negotiation      Set by the config command
19:07:06 EST MAY 31 2021
Negotiation       Cold Standby     Detected an Active mate
19:07:07 EST MAY 31 2021
Cold Standby      App Sync         Detected an Active mate
21:11:18 EST Jun 30 2021
App Sync          Disabled
HA state progression failed due to APP SYNC timeout
=====

```

Il nodo in standby non riesce a unirsi a HA con "Errore di sincronizzazione dell'app su CD
Impossibile applicare la configurazione del provider di servizi condivisi in standby"

Sulla riga di comando di Standby FTD, /ngfw/var/log/ngfwmanager.log deve avere la causa esatta dell'errore.

Correzione: talvolta, quando si riattiva la disponibilità elevata sul nodo Standby, il problema può essere risolto.

Vedere ID bug Cisco [CSCvy 04965](#)

<#root>

```
=====
From State          To State          Reason
=====
04:15:15 UTC Apr 17 2021
Not Detected        Disabled           No Error
04:15:24 UTC Apr 17 2021
Disabled            Negotiation       Set by the config command
04:16:12 UTC Apr 17 2021
Negotiation         Cold Standby      Detected an Active mate
04:16:13 UTC Apr 17 2021
Cold Standby        App Sync          Detected an Active mate
04:17:44 UTC Apr 17 2021
App Sync            Disabled
CD App Sync error is Failed to apply SSP config on standby
=====
```

Controllo stato non riuscito

"HELLO non sentito da mate" indica che il mate è offline o che il collegamento di failover non comunica i messaggi HELLO keepalive.

Provare ad accedere all'altro dispositivo. Se il protocollo SSH non funziona, accedere alla console e verificare che il dispositivo sia operativo o offline.

Se operativo, identificare la causa dell'errore con il comando show failover state.

Se non è operativo, provare a riavviare normalmente e verificare se sono presenti registri di avvio sulla console. In caso contrario, il dispositivo può essere considerato guasto hardware.

<#root>

```

=====
From State                To State                Reason
=====
04:53:36 UTC Feb 6 2021
Failed                    Standby Ready

Interface check

02:12:46 UTC Jul 11 2021
Standby Ready            Just Active             HELLO not heard from mate
02:12:46 UTC Jul 11 2021
Active Config Applied    Active                  HELLO not heard from mate
=====

```

Spegnimento o errore del disco

Se l'FTD riporta questo errore, "Rileva errore del motore di ispezione a causa di un guasto del disco", ci sono 2 possibilità.

Il motore di rilevamento (istanza SNORT) è inattivo

È possibile convalidare questa condizione con il comando sul lato Linux, `pmtool status | grep-i de`

Correzione: se una delle istanze è inattiva, verificare la presenza di `/ngfw/var/log/messages` e identificare la causa.

Il Dispositivo Mostra Un Utilizzo Elevato Del Disco

È possibile convalidare questa condizione con il comando `df -Th` sul lato Linux.

Risoluzione: identificare la directory che utilizza la maggior parte del disco e contattare TAC per eliminare i file indesiderati.

<#root>

```

=====
From State                To State                Reason
=====
Active Config Applied    Active                  No Active unit found
16:07:18 UTC Dec 5 2020
Active                    Standby Ready          Other unit wants me Standby
16:07:20 UTC Dec 5 2020
Standby Ready            Failed

Detect Inspection engine failure due to disk failure

16:07:29 UTC Dec 5 2020
Failed                    Standby Ready          My Inspection engine is as good as peer due to di
=====

```

Errore della scheda di servizio

Questi problemi vengono generalmente segnalati a causa di un errore del modulo Firepower sui dispositivi ASA 5500-X. Verificare l'integrità del modulo tramite show module sfr details.

Correzione: raccogliere il syslog ASA intorno all'ora dell'errore, che può contenere dettagli quali l'errore del controllo o del piano dati.

Ciò può essere dovuto a diversi motivi nel modulo SFR. Si consiglia di aprire TAC per trovare la causa principale di questo problema sull'IPS.

<#root>

```
=====
From State          To State          Reason
=====
21:48:19 CDT Aug 1 2021
Active              Standby Ready     Set by the config command
21:48:19 CDT Aug 1 2021
Standby Ready      Just Active
Service card in other unit has failed

21:48:19 CDT Aug 1 2021
Active Config Applied Active             Service card in other unit has failed
=====
```

Errore heartbeat MIO

Firepower Threat Defense/ASA segnala un guasto causato da "MIO-blade heartbeat failure" su FPR1K, 2K, 4K, 9K.

Vedere ID bug Cisco [CSCvy1484](#)

Vedere ID bug Cisco [CSCvh2647](#)

<#root>

```
=====
From State          To State          Reason
=====
20:14:45 EDT Apr 14 2021
Active Config Applied Active             No Active unit found
20:15:18 EDT Apr 14 2021
Active              Failed
MIO-blade heartbeat failure

20:15:19 EDT Apr 14 2021
Failed              Negotiation      MIO-blade heartbeat recovered
=====
```

Informazioni correlate

- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html>
- https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185
- [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).