Sostituzione dell'unità difettosa in Secure Firewall Threat Defense of High Availability

Sommario

Introduzione

In questo documento viene descritto come sostituire un modulo Secure Firewall Threat Defense difettoso che fa parte di una configurazione ad alta disponibilità (HA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Management Center (FMC)
- Sistema operativo Cisco Firepower eXtensible (FXOS)
- Cisco Secure Firewall Threat Defense (FTD)

Componenti usati

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

- Firepower 4110 esegue FXOS v2.12(0.498)
- Il dispositivo logico esegue Cisco Secure Firewall v7.2.5
- Secure Firewall Management Center 2600 con versione 7.4
- Conoscenze SCP (Secure Copy Protocol)

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

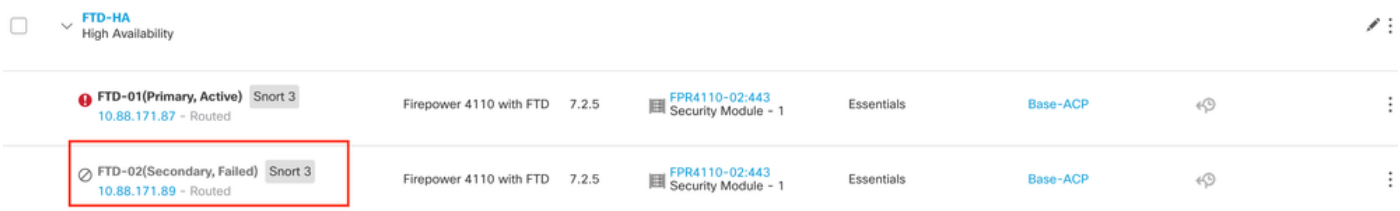
Questa procedura è supportata sugli accessori:

- Appliance Cisco Secure Firewall serie 1000
- Appliance Cisco Secure Firewall serie 2100
- Appliance Cisco Secure Firewall serie 3100
- Appliance Cisco Secure Firewall serie 4100
- Appliance Cisco Secure Firewall serie 4200
- Appliance Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defense per VMWare

Operazioni preliminari

Questo documento richiede che la nuova unità sia configurata con le stesse versioni FXOS e FTD.

Identificazione dell'unità difettosa

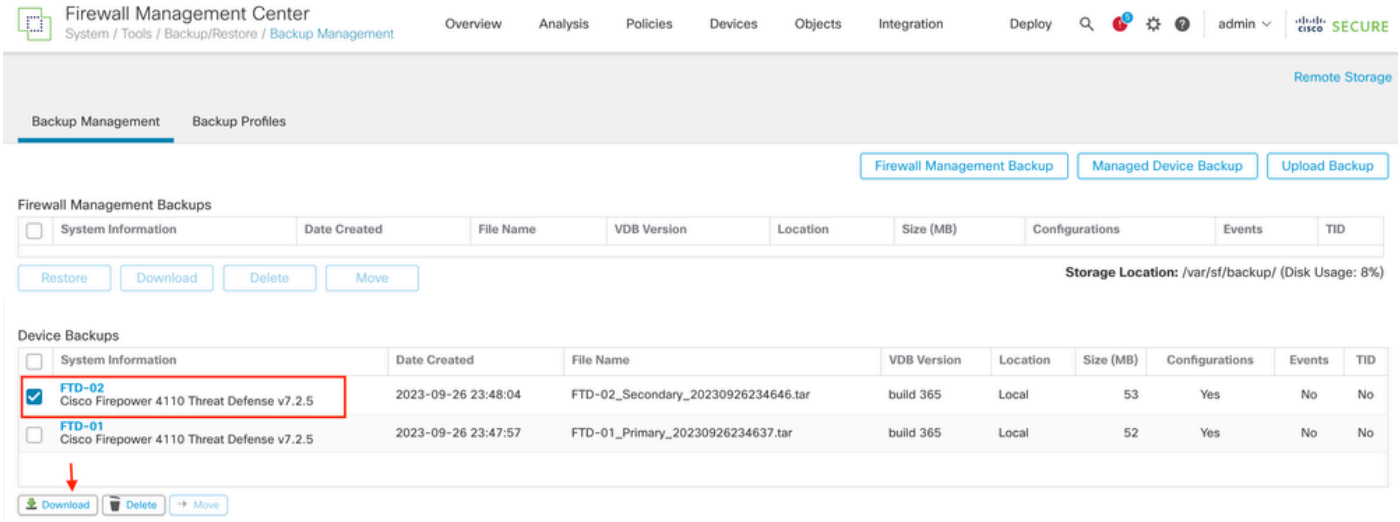


In questo scenario, l'unità secondaria (FTD-02) è in stato di errore.

Sostituzione di un'unità difettosa con un backup

È possibile utilizzare questa procedura per sostituire l'unità principale o secondaria. In questa guida si presume che l'utente disponga di una copia di backup dell'unità guasta che intende sostituire.

Passaggio 1. Scaricare il file di backup da FMC. Passare a Sistema > Strumenti > Ripristina > Backup dispositivi e selezionare il backup corretto. Fare clic su Download:



Passaggio 2. Caricare il backup FTD nella directory /var/sf/backup/ del nuovo FTD:

2.1 Dal test-pc (client SCP) caricare il file di backup nel FTD nella directory /var/tmp/:

```
@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/
```

2.2 Dalla modalità FTD CLI Expert, spostare il file di backup da /var/tmp/ a /var/sf/backup/:

```
root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/
```

Passaggio 3. Ripristinare il backup FTD-02, applicando il comando successivo dalla modalità clish:

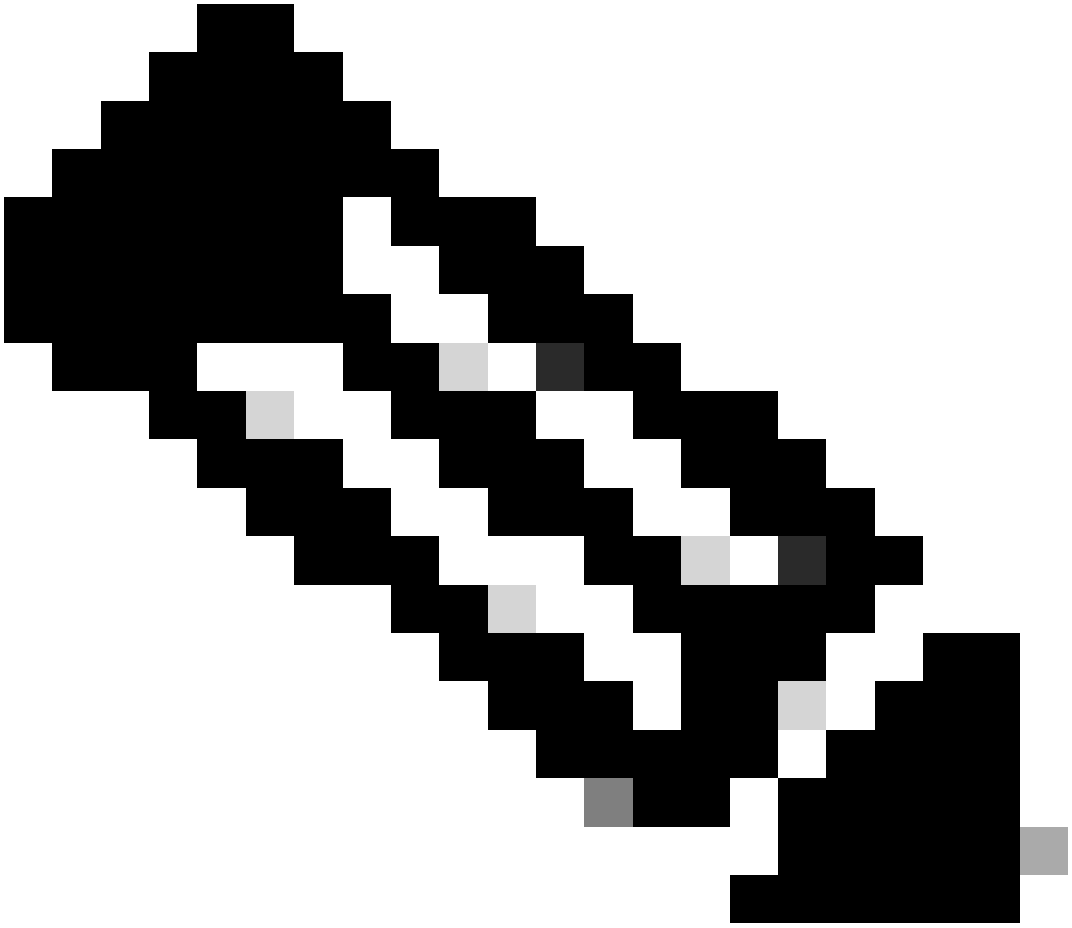
```
>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar

Device model from backup :: Cisco Firepower 4110 Threat Defense
This Device Model  :: Cisco Firepower 4110 Threat Defense
************************************************
Backup Details
************************************************
Model = Cisco Firepower 4110 Threat Defense
Software Version = 7.2.5
Serial = FLM22500791
Hostname = firepower
Device Name = FTD-02_Secondary
IP Address = 10.88.171.89
Role = SECONDARY
VDB Version = 365
SRU Version =
FXOS Version = 2.12(0.498)
Manager IP(s) = 10.88.243.90
Backup Date = 2023-09-26 23:46:46
Backup Filename = FTD-02_Secondary_20230926234646.tar
************************************************

********************* Caution ***************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest be
Restore operation will overwrite all configurations on this device with configurations in backup.
If this restoration is being performed on an RMA device then ensure old device is removed from network
************************************************************
Are you sure you want to continue (Y/N)Y
Restoring device . . . . . .
Added table audit_log with table_id 1
Added table health_alarm_syslog with table_id 2
Added table dce_event with table_id 3
Added table application with table_id 4
Added table rna_scan_results_tableview with table_id 5
Added table rna_event with table_id 6
Added table ioc_state with table_id 7
Added table third_party_vulns with table_id 8
Added table user_ioc_state with table_id 9
Added table rna_client_app with table_id 10
Added table rna_attribute with table_id 11
Added table captured_file with table_id 12
Added table rna_ip_host with table_id 13
Added table flow_chunk with table_id 14
Added table rua_event with table_id 15
Added table wl_dce_event with table_id 16
Added table user_identities with table_id 17
Added table whitelist_violations with table_id 18
Added table remediation_status with table_id 19
Added table syslog_event with table_id 20
Added table rna_service with table_id 21
Added table rna_vuln with table_id 22
Added table SRU_import_log with table_id 23
Added table current_users with table_id 24

Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023):

The system is going down for reboot NOW!
```

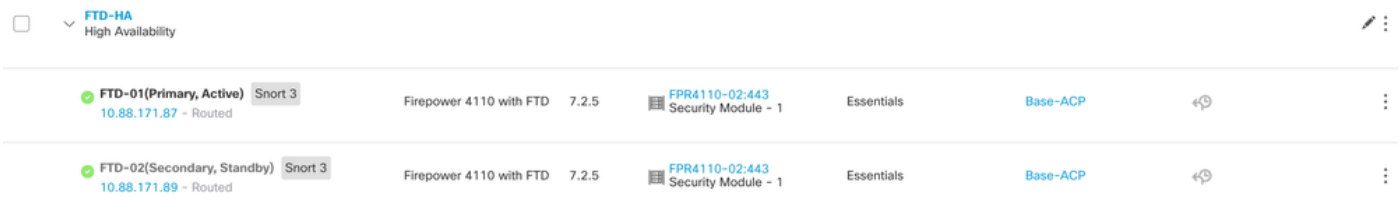


Nota: Al termine del ripristino, il dispositivo esegue la disconnessione dalla CLI, si riavvia e si connette automaticamente al FMC. A questo punto, il dispositivo non sarà più aggiornato.

Passaggio 4. Riprendere la sincronizzazione HA. Dalla CLI FTD, immettere configure high-availability resume:

```
>configure high-availability resume
```

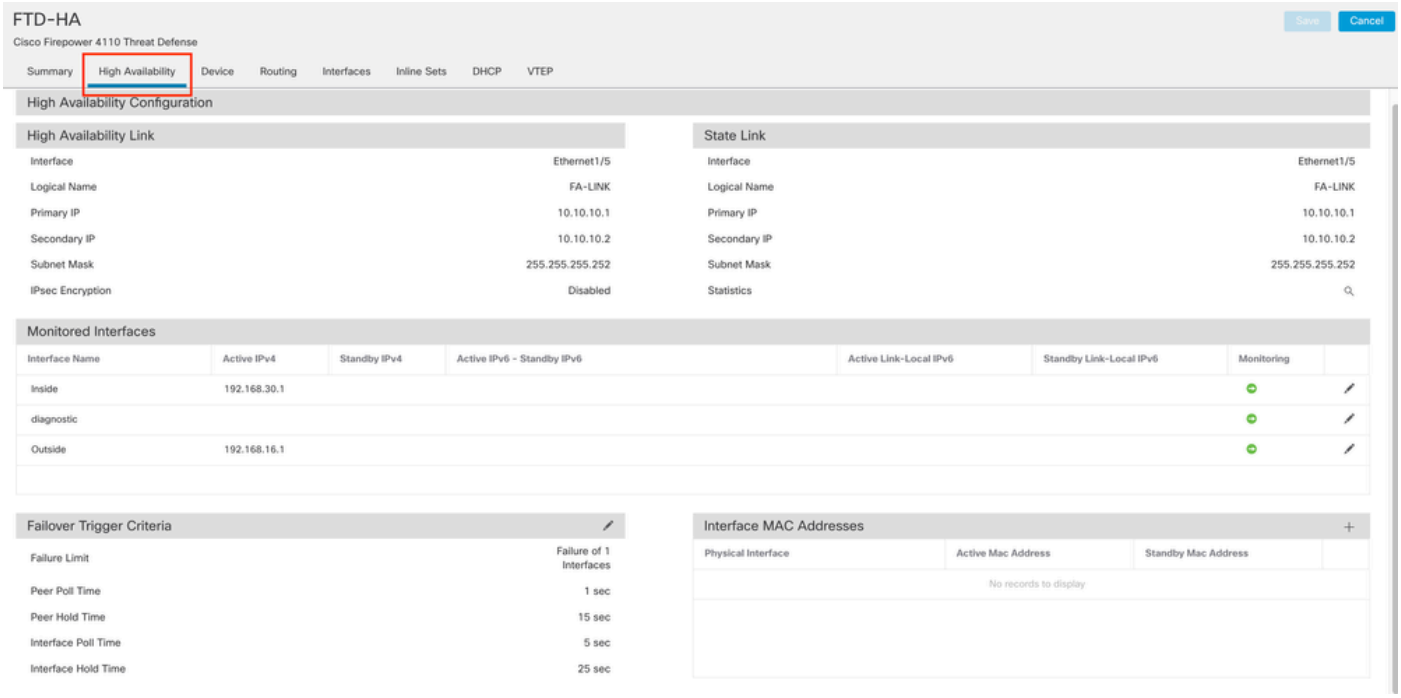
La configurazione dell'alta disponibilità FTD è ora completata:



Sostituzione di un'unità difettosa senza backup

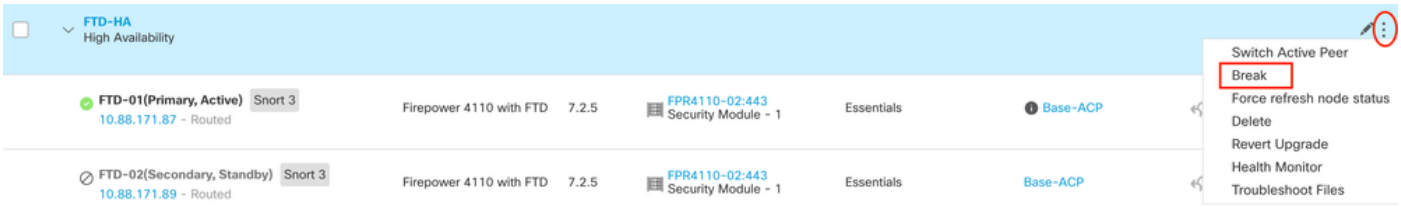
Se non si dispone di una copia di backup del dispositivo guasto, è possibile procedere con questa guida. È possibile sostituire l'unità principale o secondaria,il processo varia a seconda che il dispositivo sia primario o secondario. Tutte le operazioni descritte in questa guida consistono nel ripristinare un'unità secondaria difettosa. Se si desidera ripristinare un'unità principale difettosa, al punto 5 configurare la disponibilità elevata utilizzando l'unità secondaria/attiva esistente come dispositivo principale e il dispositivo sostitutivo come dispositivo secondario/standby durante la registrazione.

Passaggio 1. Acquisire una schermata (backup) della configurazione ad alta disponibilità passando a Device > Device Management. Modificare la coppia FTD HA corretta (fare clic sull'icona a forma di matita), quindi fare clic sull'opzione Alta disponibilità:

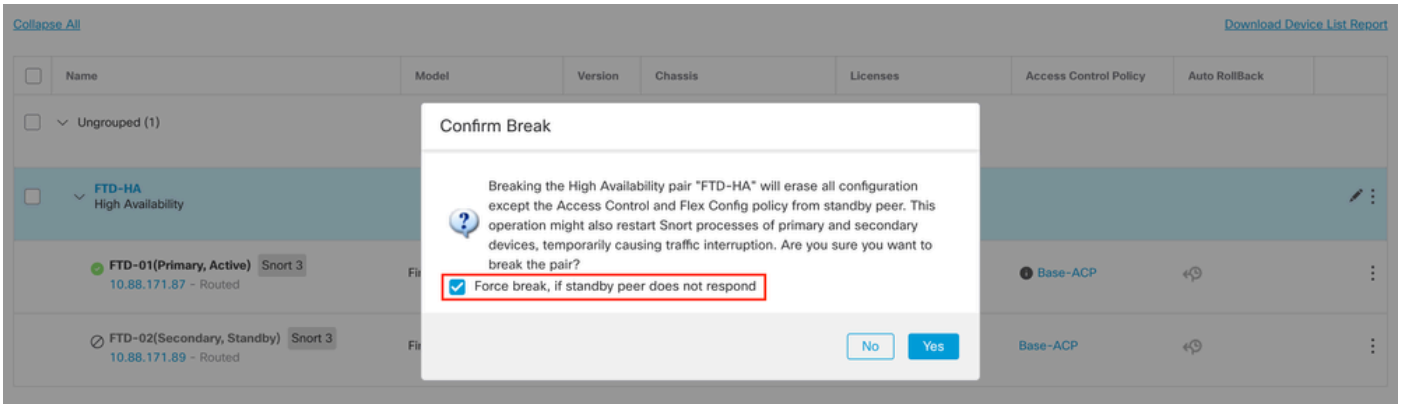


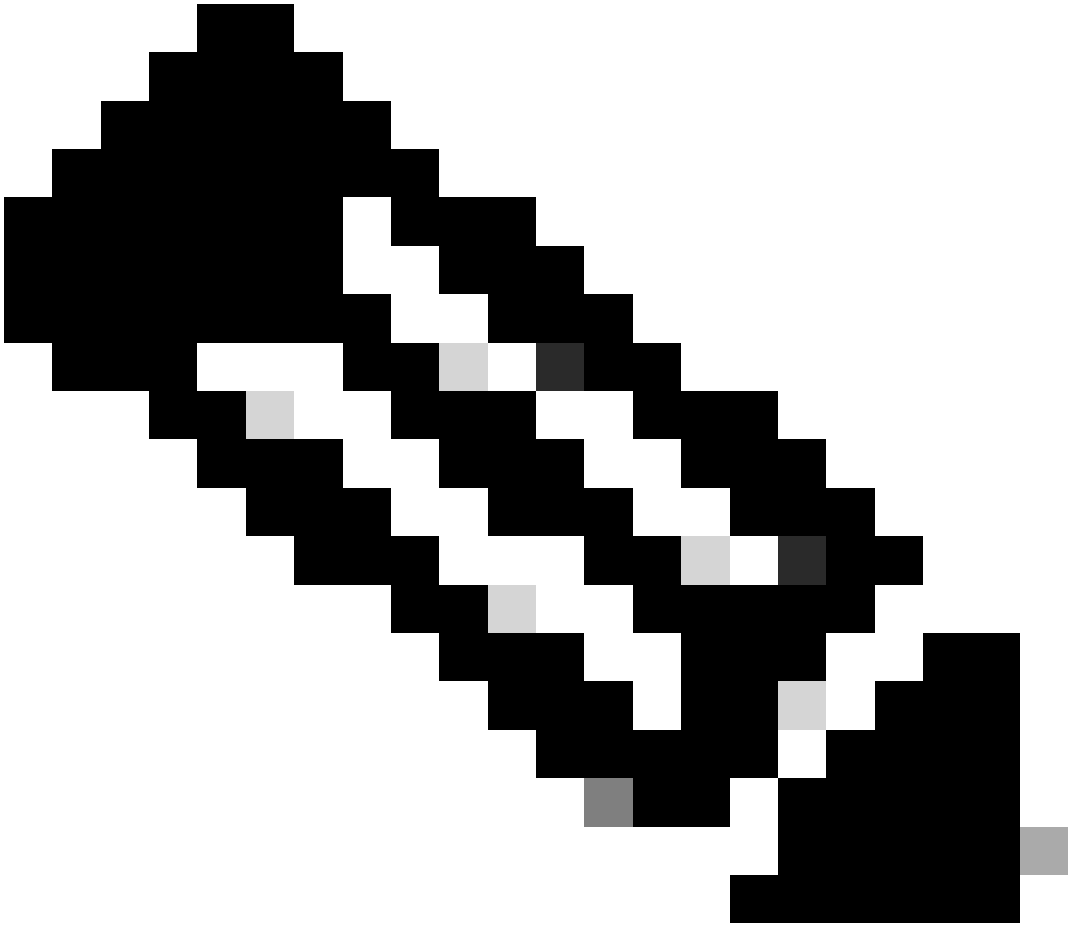
Passaggio 2. Interrompere HA.

2.1 Passare a Dispositivi > Gestione dispositivi e fare clic sul menu a tre punti nell'angolo superiore destro. Quindi fare clic sull'opzione Break:



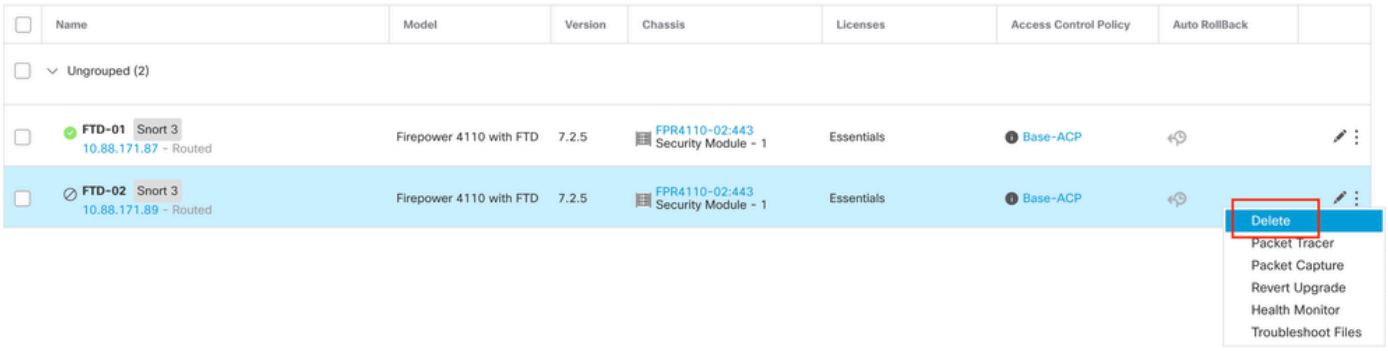
2.2. Selezionare Forza interruzione se il peer in standby non risponde all'opzione:





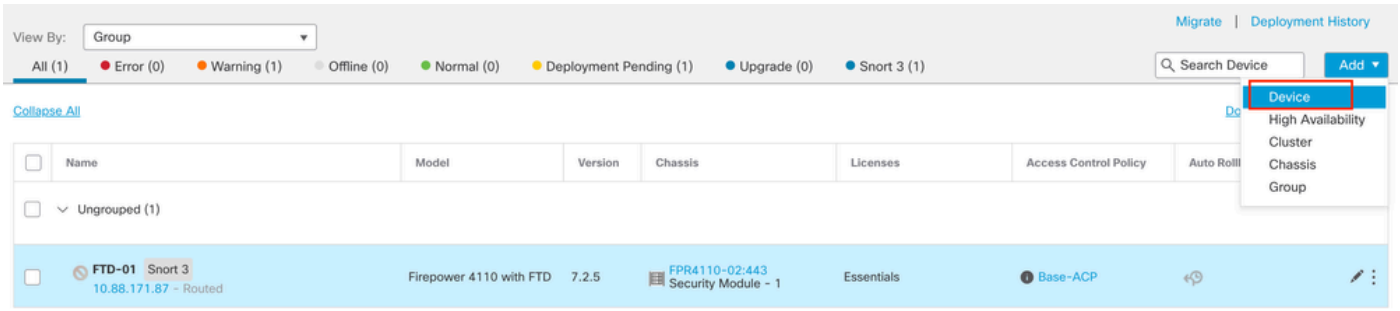
Nota: Poiché l'unità non risponde, è necessario forzare l'interruzione della disponibilità elevata. Quando si interrompe una coppia di disponibilità elevata, il dispositivo attivo mantiene la funzionalità distribuita completa. Il dispositivo in standby perde il failover e le configurazioni dell'interfaccia e diventa un dispositivo autonomo.

Passaggio 3. Eliminare l'FTD difettoso. Identificare l'FTD da sostituire, quindi fare clic sul menu a tre punti. Fare clic su Elimina:



Passaggio 4. Aggiungere il nuovo FTD.

4.1. Passare a Dispositivi > Gestione dispositivi > Aggiungi e fare clic su Dispositivo:



4.2. Selezionare il metodo di provisioning, in questo caso Chiave di registrazione, configurare Host, Nome visualizzato, Chiave di registrazione. Configurare i criteri di controllo di accesso e fare clic su Registra.

Add Device

Select the Provisioning Method:

(•) Registration Key ( ) Serial Number

[ ] CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:*

••••••••

Group:

None

Access Control Policy:*

Base-ACP

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier

[ ] Carrier
[ ] Malware Defense
[ ] IPS
[ ] URL

Advanced

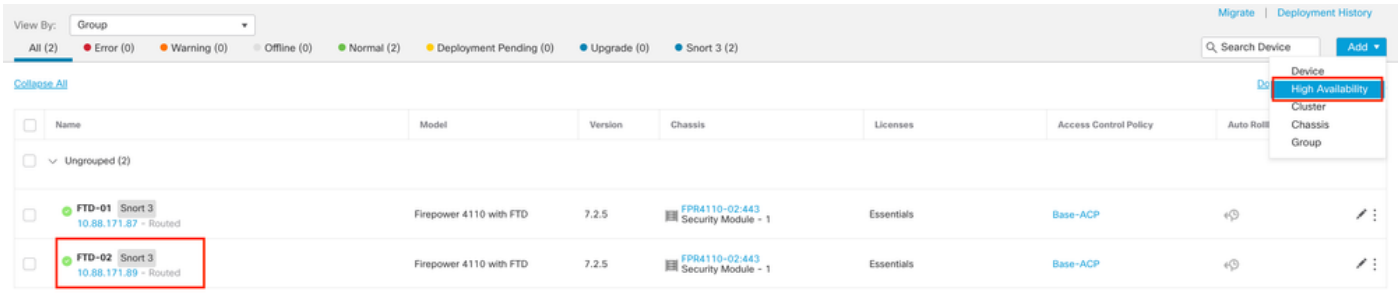
Unique NAT ID:†

[ ] Transfer Packets

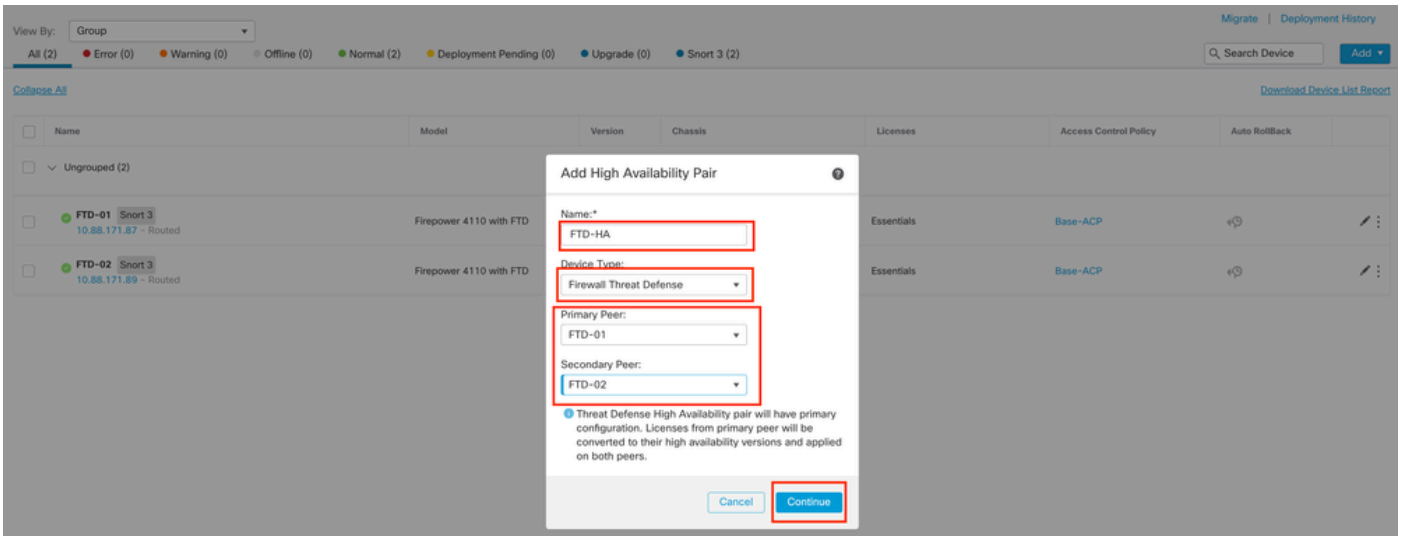
Cancel Register

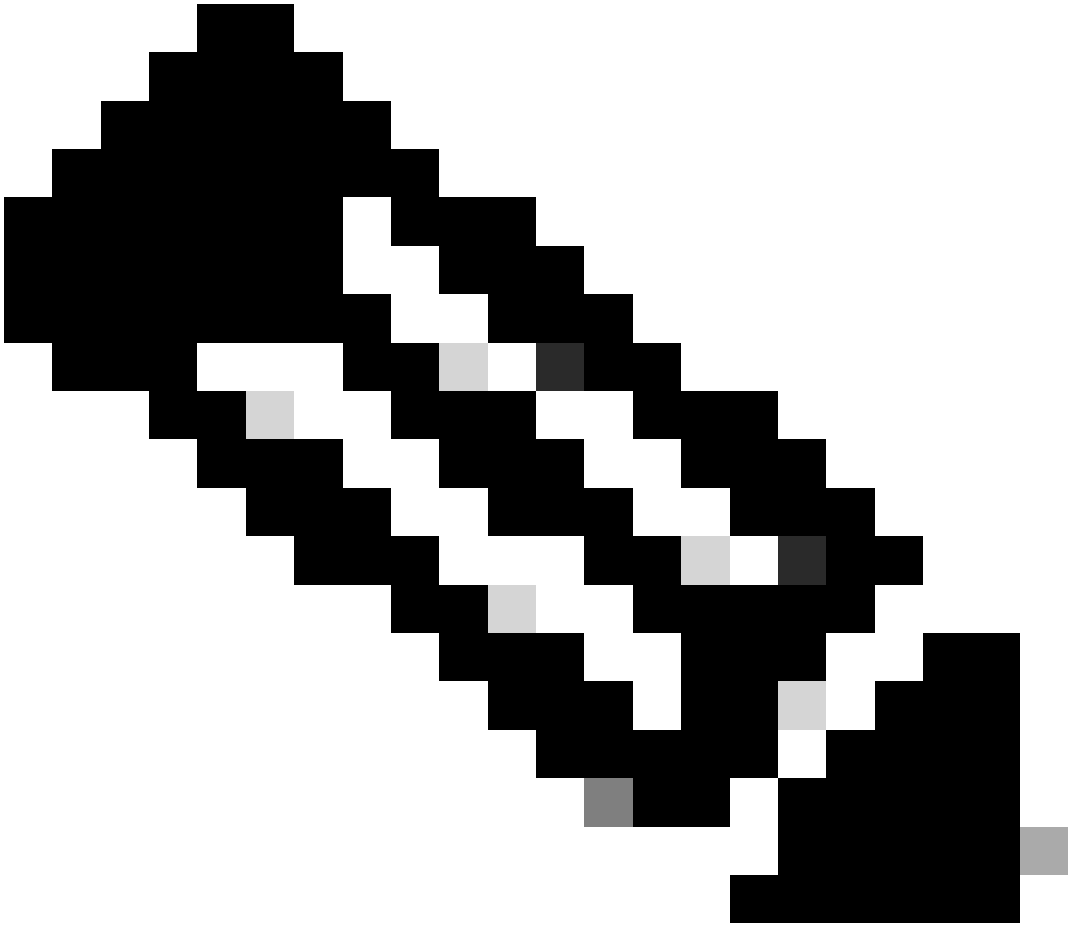
Passaggio 5. Creare HA.

5.1 Passare a Dispositivi > Gestione dispositivi > Aggiungi e fare clic su Alta disponibilità opzione.



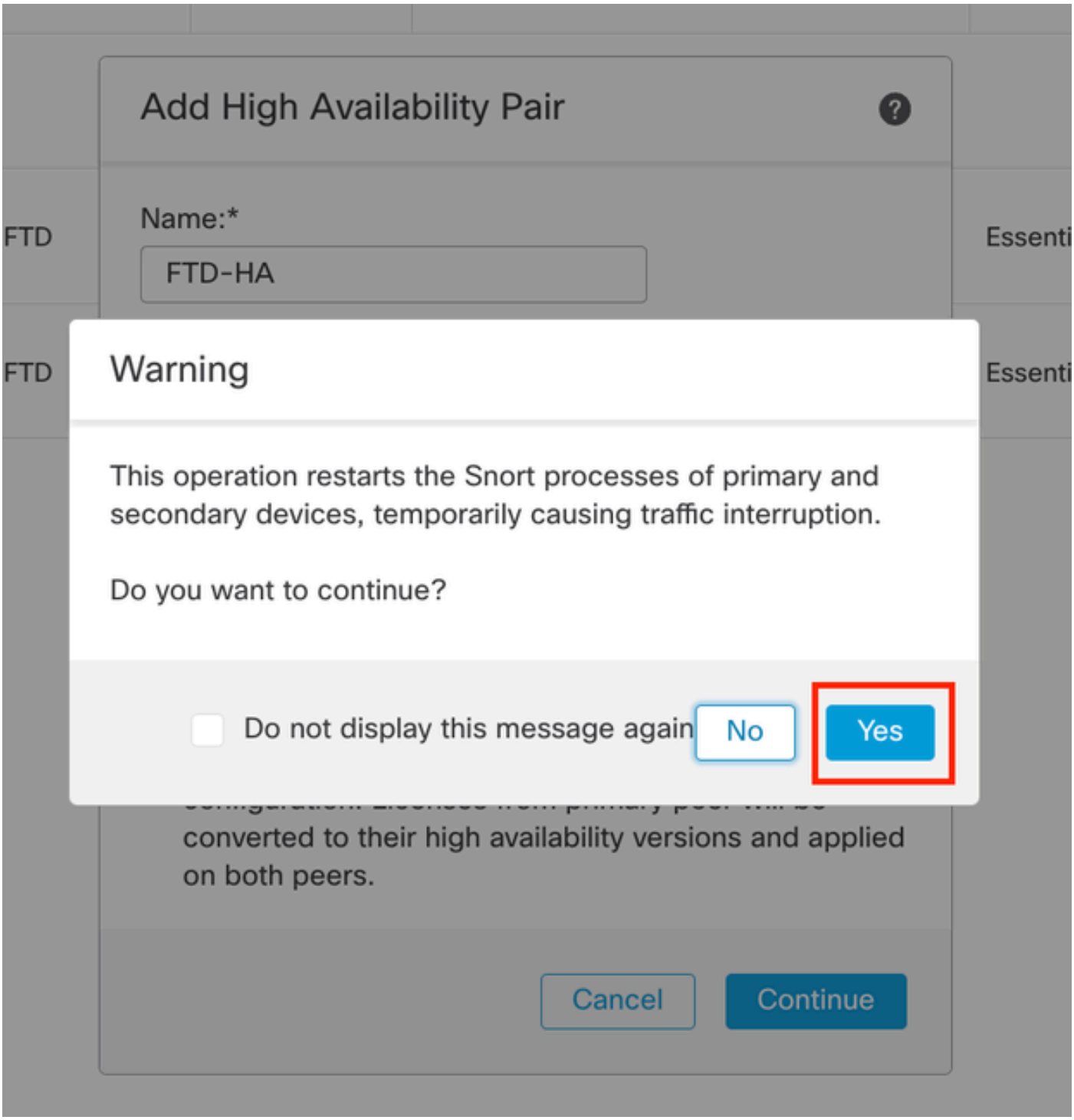
5.2. Configurare l'opzione Aggiungi coppia ad alta disponibilità. Configurare il nome, il tipo di dispositivo, selezionare FTD-01 come peer primario e FTD-02 come peer secondario e fare clic su Continua.

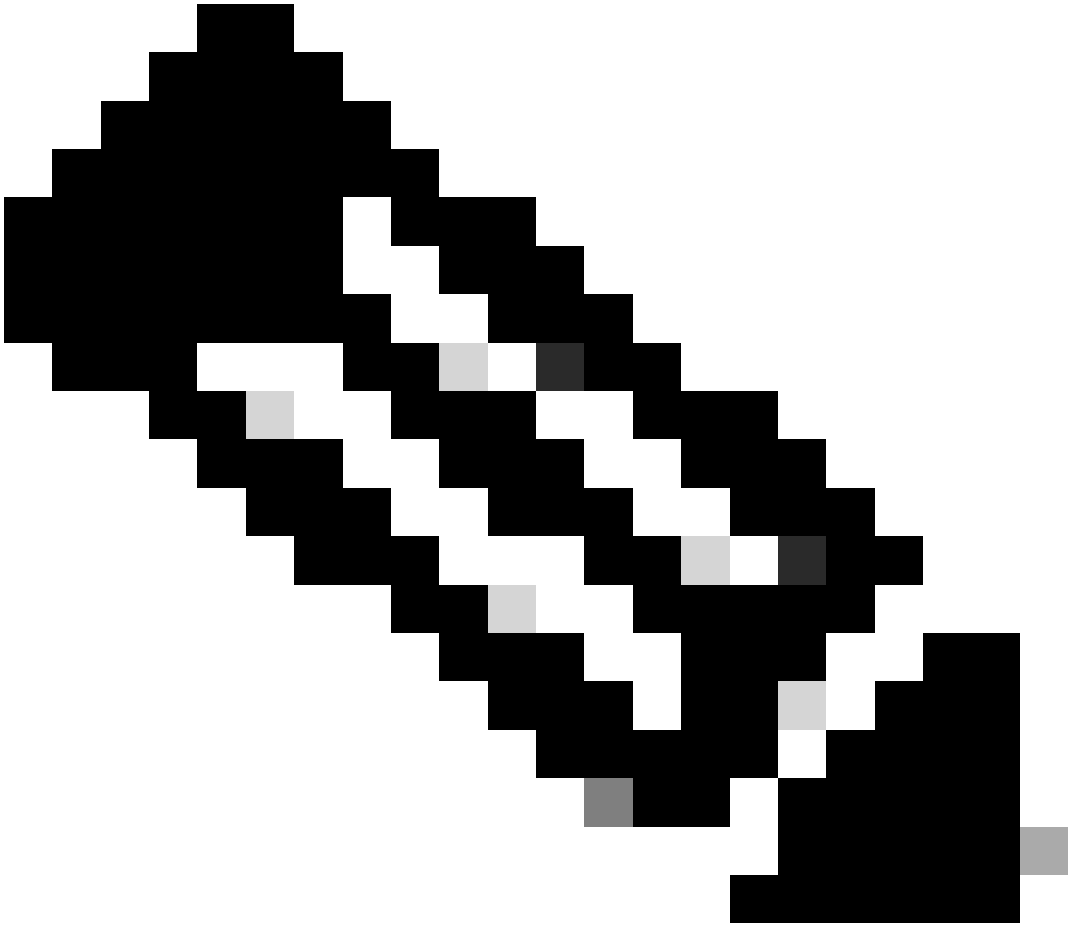




Nota: Ricordarsi di selezionare l'unità principale come il dispositivo che dispone ancora della configurazione, in questo caso, FTD-01.

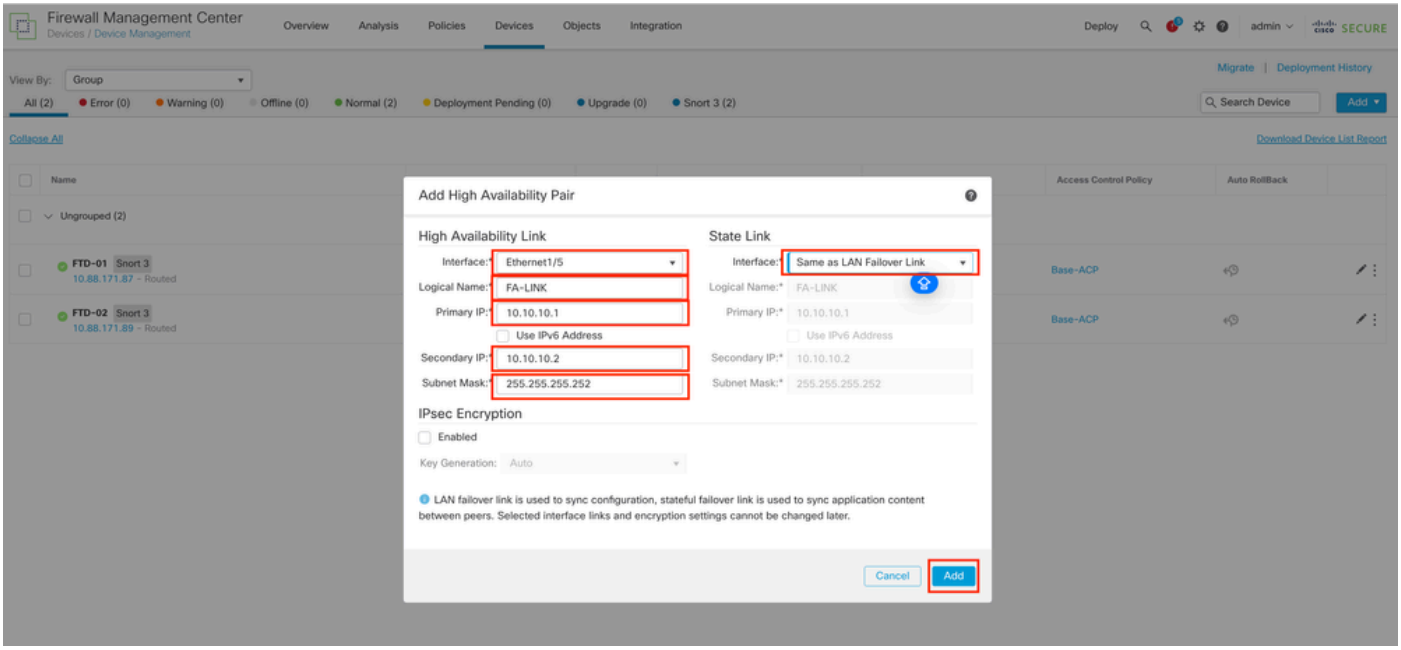
5.3. Confermare la creazione di HA, quindi fare clic su Sì.


Add High Availability Pair
Name:*
FTD-HA
FTD
Essenti
FTD
Essenti
Warning
This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.
Do you want to continue?
Do not display this message again
No
Yes
converted to their high availability versions and applied on both peers.
Cancel
Continue

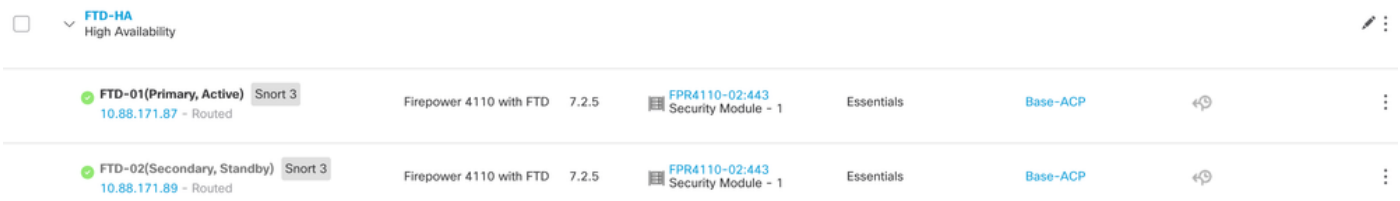


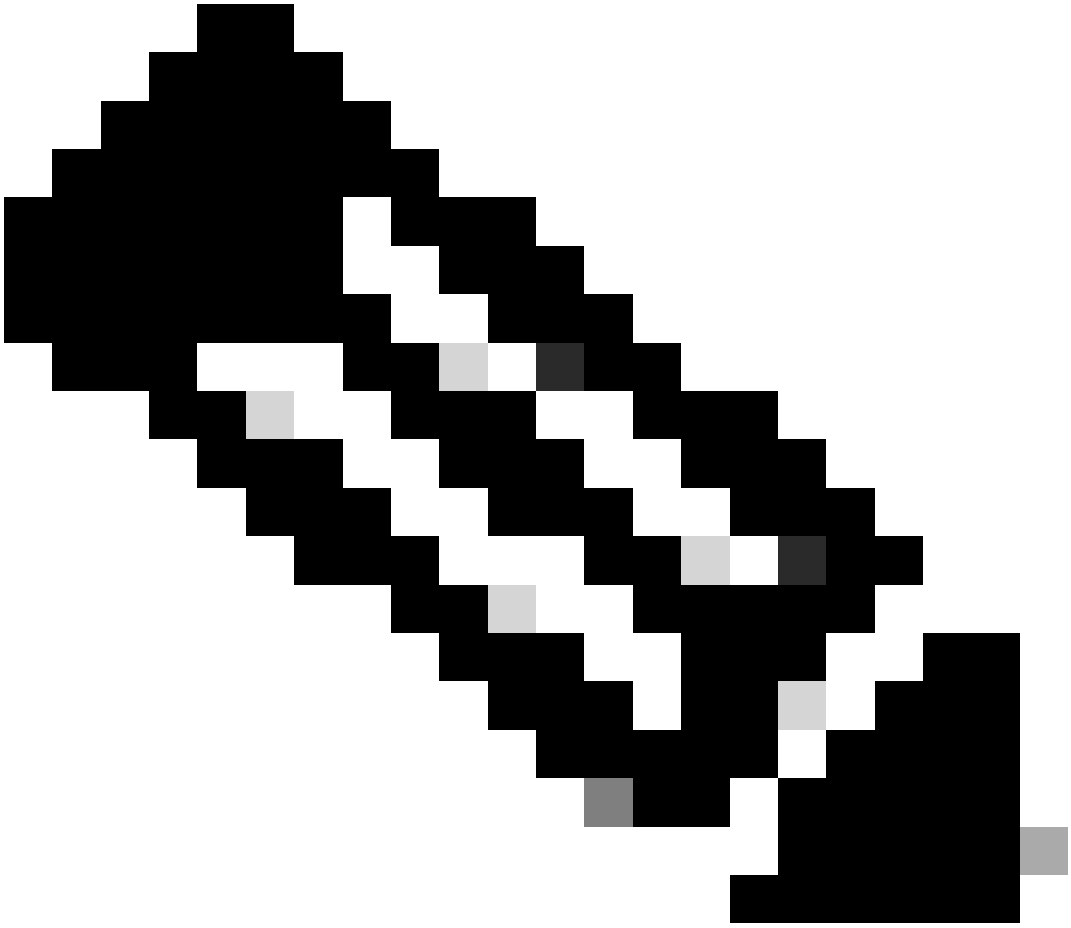
Nota: La configurazione dell'alta disponibilità riavvia il motore di snort di entrambe le unità e può causare l'interruzione del traffico.

5.4. Configurare i parametri di alta disponibilità indicati nel passaggio 2, quindi fare clic sull'opzione Add:



6. La configurazione dell'alta disponibilità FTD è ora completata:





Nota: Se non si configurano indirizzi MAC virtuali, è necessario cancellare le tabelle ARP sui router connessi per ripristinare il flusso di traffico in caso di sostituzione dell'unità primaria. Per ulteriori informazioni, vedere Indirizzi MAC e indirizzi IP in Alta disponibilità.

Informazioni correlate

- Supporto tecnico Cisco e download

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).