

Dépannage de l'échec de configuration de haute disponibilité FDM en raison d'une incompatibilité d'inscription de services cloud

Table des matières

Problème

La configuration de la haute disponibilité (HA) échoue entre deux périphériques Firepower 1150 gérés par Firewall Device Manager (FDM). Le processus de configuration ne s'est pas terminé correctement, ce qui empêche l'établissement d'une paire haute disponibilité.

L'interface utilisateur FDM de l'unité principale indique :

Firewall Device Manager

Monitoring Policies Objects Device: FTD1150-2

admin Administrator

Secure

Device Summary

High Availability

Primary Device

Current Device Mode: Active Peer: Disabled

Failover History Deployment History

One of the units has failed. Pressing into the failed unit and view the failover history to determine the cause.

High Availability Configuration

Select and configure the peer device based on the following characteristics.

GENERAL DEVICE INFORMATION

Model Cisco Firepower 1150 Threat Defense

Software 10.0.0-140

VDB 416.0

Intrusion Rule Update 20251124-2043

FAILOVER LINK

Interface Ethernet1/1

Type IPv4

Primary IP/Netmask 192.168.10.1/24

Secondary IP/Netmask 192.168.10.2/24

STATEFUL FAILOVER LINK

The same as the Failover Link.

Failover Criteria

INTERFACE FAILURE THRESHOLD

Failure Criteria

Number of failed interfaces exceeds 1

7-211

INTERFACE TIMING CONFIGURATION

Poll Time 5000 Hold Time 25000 seconds milliseconds

500-15000 milliseconds 5000-75000 milliseconds

PEER TIMING CONFIGURATION

Poll Time 1000 Hold Time 15000 seconds milliseconds

200-15000 milliseconds 800-45000 milliseconds

SAVE

L'unité FTD secondaire affiche :

Firewall Device Manager

Monitoring Policies Objects Device: FTD1150-3

admin Administrator

Device Summary High Availability

Secondary Device
Current Device Mode: **Suspended** Peer: **Unknown** [Failover History](#) [Deployment History](#)

Time of event: 07 Aug 2026, 12:11:39 PM
Event description: CD App Sync error FDM validation failure Active and Standby Nodes cannot have different cloud regions Check appsynchistory CLI for details

High Availability Configuration

Select and configure the peer device based on the following characteristics.

GENERAL DEVICE INFORMATION

Model	Cisco Firepower 1150 Threat Defense
Software	10.0.0-140
VDB	416.0
Intrusion Rule Update	20251124-2043

FAILOVER LINK

Interface	Ethernet1/1
Type	IPv4
Primary IP/Netmask	192.168.10.1/24
Secondary IP/Netmask	192.168.10.2/24

Failover Criteria

INTERFACE FAILURE THRESHOLD

Failure Criteria	Number
Number of failed interfaces exceeds	1

1-211

INTERFACE TIMING CONFIGURATION

Poll Time	Hold Time	seconds
5000	25000	milliseconds

500-15000 milliseconds 5000-75000 milliseconds

PEER TIMING CONFIGURATION

Poll Time	Hold Time	seconds
1000	15000	milliseconds

200-15000 milliseconds 800-45000 milliseconds

SAVE

CLI FTD principale :

```
<#root>
```

```
>
```

```
show app-sync-history
```

```
=====APP SYNC HISTORY=====
-----
App Sync Time: 10:11:10 UTC Aug 07 2026
Role: Active Unit
App Sync Status: FAILURE
Failed Phase: WaitRemoteConfigApply
```

```
Failure Reason: Cluster App Un Archive failure on Standby/Slave Unit Node Id: 1 FDM validation failure -
```

CLI FTD secondaire :

```
<#root>
```

```
device#
```

```
show failover
```

Failover Off (pseudo-Standby)

Failover unit Secondary
Failover LAN Interface: failover-link Ethernet1/1 (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 2 of 1288 maximum
MAC Address Move Notification Interval not set
failover replication http

>

show app-sync-history

=====APP SYNC HISTORY=====

App Sync Time: 10:11:06 UTC Aug 07 2026
Role: Standby Unit
App Sync Status: FAILURE
Failed Phase: OnBoxValidators

Failure Reason: FDM validation failure - Active and Standby Nodes cannot have different cloud regions.

device#

show failover history

From State	To State	Reason
08:45:29 UTC Aug 7 2026 Not Detected	Disabled	No Error
10:10:49 UTC Aug 7 2026 Disabled	Negotiation	Set by the config command (failover)
10:10:50 UTC Aug 7 2026 Negotiation	Cold Standby	Detected an Active peer
10:10:52 UTC Aug 7 2026 Cold Standby	App Sync	Detected an Active peer
10:11:39 UTC Aug 7 2026 App Sync	Disabled	

CD App Sync error

FDM validation failure - Active and Standby Nodes cannot have different cloud regions.. Check app-sync-h

Environnement

- Deux unités Firepower 1150 FTD. D'autres plates-formes matérielles sont également concernées.
- Logiciel FTD version 7.2.8. Les autres versions logicielles sont également affectées.
- Les deux unités FTD sont gérées par FDM et sont inscrites aux services cloud Cisco.

Résolution

La résolution implique l'alignement de l'état d'inscription des services cloud entre les deux pare-feu.

Les principaux services cloud sont actuellement enregistrés dans la région des États-Unis :

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for device FTD1150-2. The left sidebar contains navigation links for System Settings, Management Access, Logging Settings, DHCP, DDNS Service, DNS Server, Hostname, Time Services, SSL Settings, HTTP Proxy, Reboot/Shutdown, Login Page, Remote Management, Cloud Services, Central Management, and Traffic Settings. The main content area is titled 'Device Summary' and 'Cloud Services'. It shows a status of 'Connected Registered' with a green checkmark. Below this, it lists 'Enrollment Type: Smart Licensing', 'Region: US Region' (highlighted with an orange box), and 'Tenancy: SEC TAC and 1 Tenant'. There are three service cards: 'Security Cloud Control' (Disabled), 'Cisco Success Network' (Enabled), and 'Send Events to the Cisco Cloud' (Disabled). Each card has an 'ENABLE' button. A note states: 'Note: If the device is registered to cloud services using Smart Licensing, the device will not work with SCC. Please [unregister](#) the device and re-on-board using the registration key method with the "Security/SCC account" option.' The bottom card, 'Send Events to the Cisco Cloud', includes a description: 'You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as [Cisco SecureX threat response](#), to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.'

Les services cloud secondaires sont enregistrés dans la région de l'UE :

Firewall Device Manager | Monitoring | Policies | Objects | **Device: FTD1150-3**

System Settings ← | Management Access | Logging Settings | > DHCP | DDNS Service | DNS Server | Hostname | Time Services | SSL Settings | HTTP Proxy | Reboot/Shutdown | Login Page

Remote Management | **Cloud Services** | Central Management | Traffic Settings | URL Filtering Preferences

Device Summary
Cloud Services

Connected Registered | Enrollment Type: Smart Licensing | Tenancy: SEC TAC and 1 Tenant | Region: EU Region

Security Cloud Control [ENABLE] [DISABLED]

Note: If the device is registered to cloud services using Smart Licensing, the device will not work with SCC. Please unregister the device and re-on-board using the registration key method with the "Security/SCC account" option.

Security Cloud Control allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

Cisco Success Network [ENABLE] [DISABLED]

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the Sample Data that will be sent to Cisco.

Send Events to the Cisco Cloud [ENABLE] [DISABLED]

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco SecureX threat response, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.

Dans ce cas, l'utilisateur décide d'inscrire le pare-feu secondaire (FW2) pour correspondre au pare-feu principal (FW1).

Étape 1: Inscrivez FW2 aux services cloud Cisco

Inscrivez FW2 aux services cloud Cisco en utilisant la même région cloud que FW1 (région des États-Unis).

Dans l'interface FDM FW2, accédez à Device > System Settings > Cloud Services et annulez l'inscription des services cloud :

Firewall Device Manager | Monitoring | Policies | Objects | **Device: FTD1150-3**

System Settings ← | Management Access | Logging Settings | > DHCP | DDNS Service | DNS Server | Hostname | Time Services | SSL Settings | HTTP Proxy | Reboot/Shutdown

Remote Management | **Cloud Services** | Central Management | Traffic Settings | URL Filtering Preferences

Device Summary
Cloud Services

Connected Registered | Enrollment Type: Smart Licensing | Tenancy: SEC TAC and 1 Tenant | Region: EU Region

Security Cloud Control [ENABLE] [DISABLED]

Note: If the device is registered to cloud services using Smart Licensing, the device will not work with SCC. Please unregister the device and re-on-board using the registration key method with the "Security/SCC account" option.

Security Cloud Control allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

Cisco Success Network [ENABLE] [DISABLED]

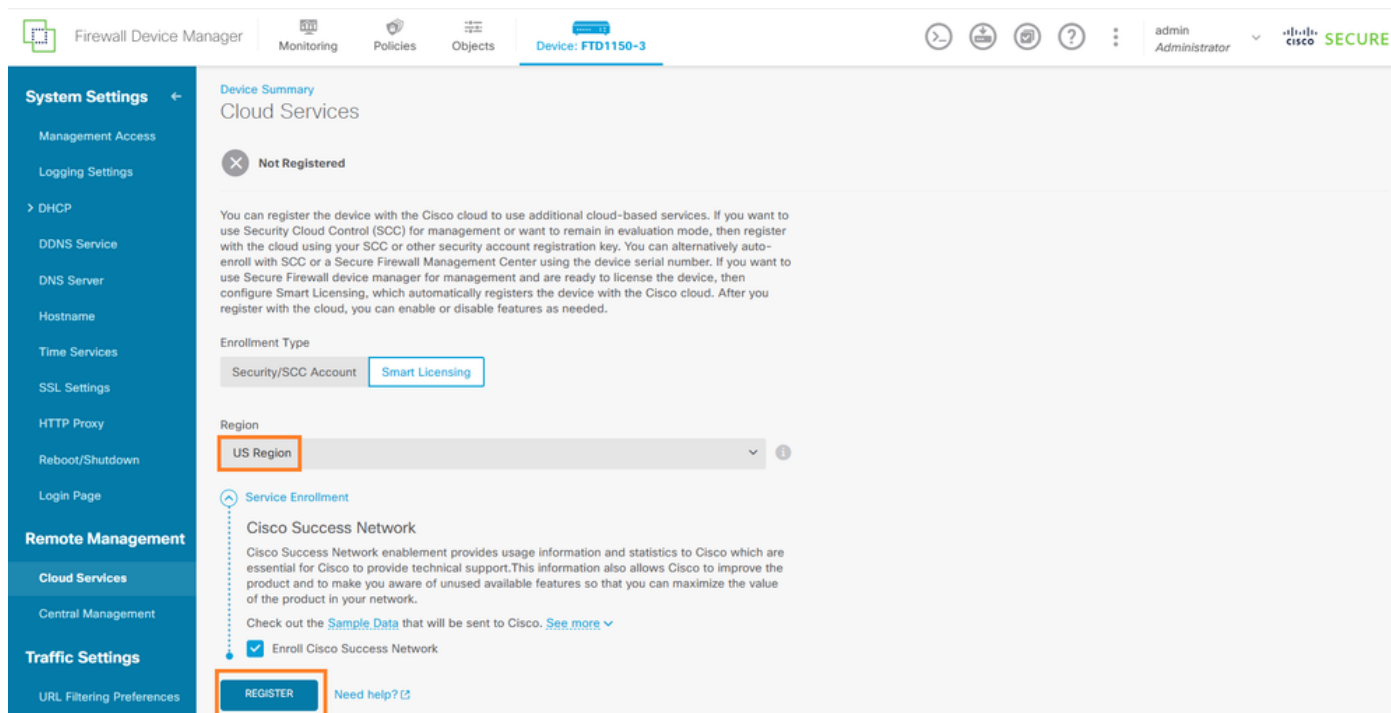
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the Sample Data that will be sent to Cisco.

Send Events to the Cisco Cloud [ENABLE] [DISABLED]

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco SecureX threat response, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.

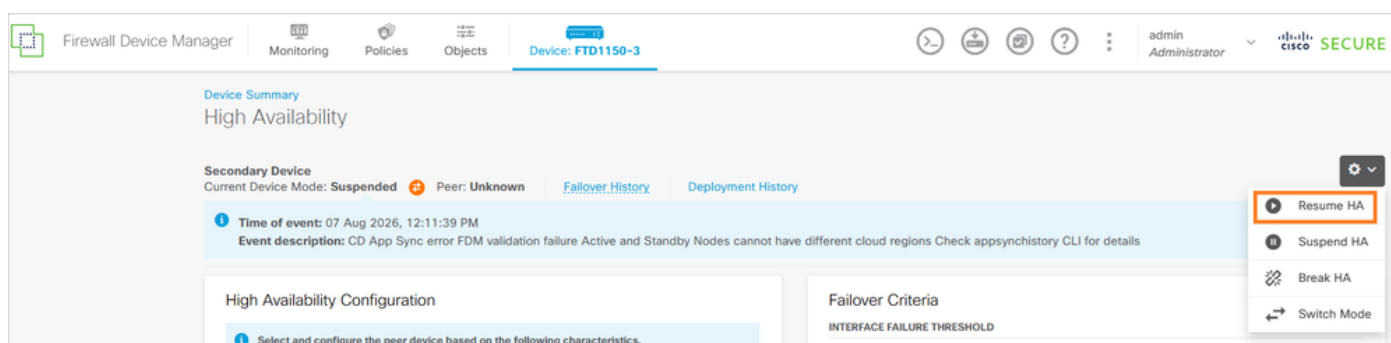
Unregister Cloud Services

Inscrivez ensuite FW2 dans la même région que celle utilisée par FW1 :



Étape 2: Réessayer la configuration haute disponibilité

Une fois que les deux périphériques affichent le même état d'inscription au cloud, reprenez la configuration de haute disponibilité :



Dans l'interface de ligne de commande du périphérique secondaire, vous voyez :

```
<#root>
```

```
>
```

```
Detected an Active mate
```

Secondary: Switching to Ok for reason Detected an Active peer.

et quelques minutes plus tard :

```
<#root>
```

```
device#
```

```
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

En règle générale, les deux périphériques doivent être inscrits dans la même région de services cloud Cisco, ou les deux ne doivent pas être inscrits du tout.

Motif

La cause principale est une non-concordance de l'état d'inscription aux services cloud Cisco entre les deux périphériques Firepower 1150. FDM bloque HA App Sync lorsqu'un noeud est inscrit dans le cloud et que l'autre n'est pas inscrit ou est inscrit dans une autre région. Cette validation garantit que les deux périphériques d'une paire haute disponibilité maintiennent une connectivité

cloud et une disponibilité des fonctionnalités cohérentes.

La cause technique spécifique est que FW1 était inscrit dans la région des États-Unis des services cloud Cisco alors que FW2 était inscrit dans la région de l'UE, ce qui entraîne un état incompatible pour la formation de paires HA.

Autres informations utiles

- [Guide de configuration de la haute disponibilité de Cisco Firepower Threat Defense](#)
- [Configuration des paramètres système de Cisco Firepower Device Manager](#)
- [Configuration de la haute disponibilité FTD avec FDM](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.