

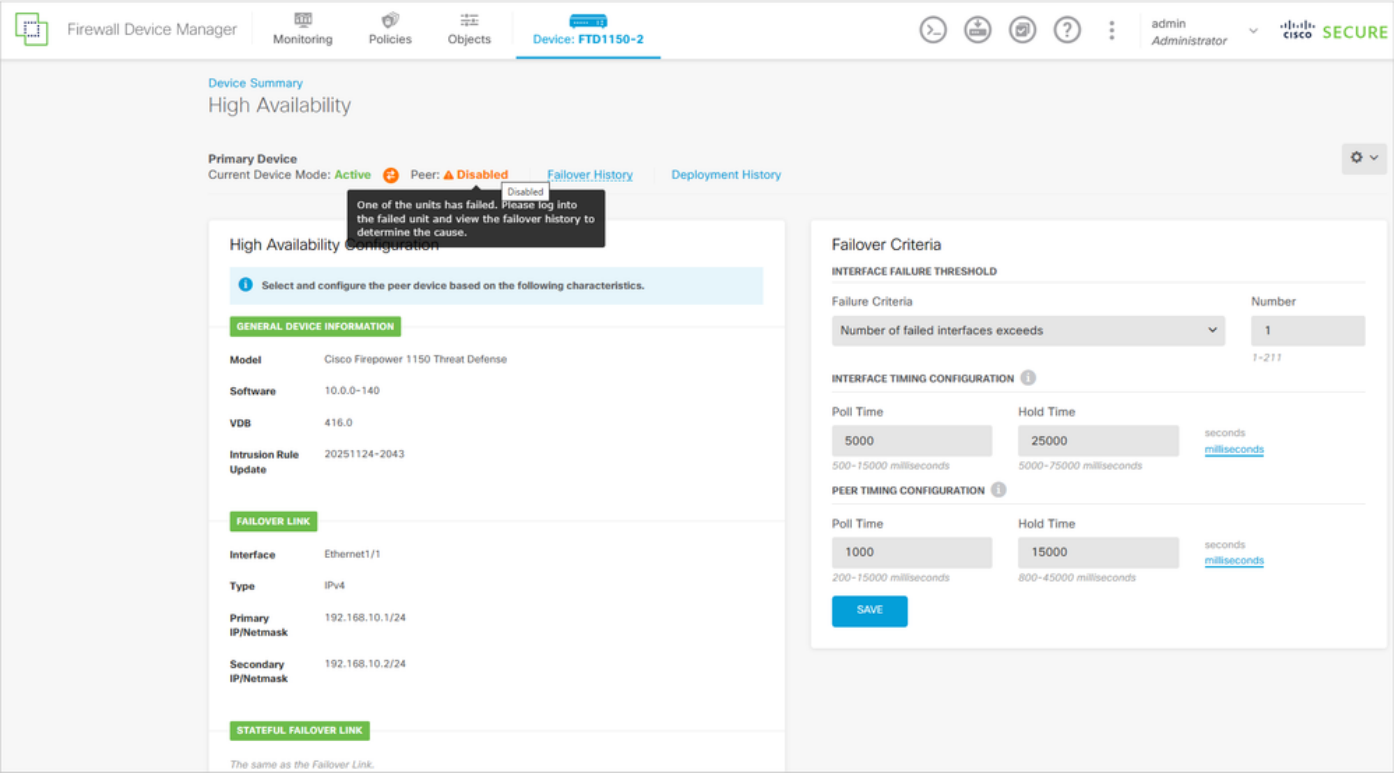
解決由於雲服務註冊不匹配導致的FDM高可用性配置故障

目錄

問題

在由防火牆裝置管理器(FDM)管理的兩台Firepower 1150裝置之間的高可用性(HA)配置失敗。 配置過程未成功完成，導致無法建立HA配對。

主裝置上的FDM UI顯示：



次要FTD裝置顯示：

Firewall Device Manager

MonitoringPoliciesObjects

Device: FTD1150-3

adminAdministrator

SECURE

Device Summary

High Availability

Secondary Device

Current Device Mode: SuspendedPeer: 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

主FTD CLI:

<#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 -

輔助FTD CLI:

<#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

環境

- 兩部Firepower 1150 FTD裝置。其他硬體平台也受到影響。
- FTD軟體版本7.2.8。其他軟體版本也受到影響。
- 兩台FTD裝置均由FDM管理並在思科雲服務中註冊。

解析

解決方案涉及在兩個防火牆之間協調雲服務註冊狀態。

主要雲服務已在美國地區註冊：

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for device FTD1150-2. The 'Cloud Services' section is active, showing the following configuration:

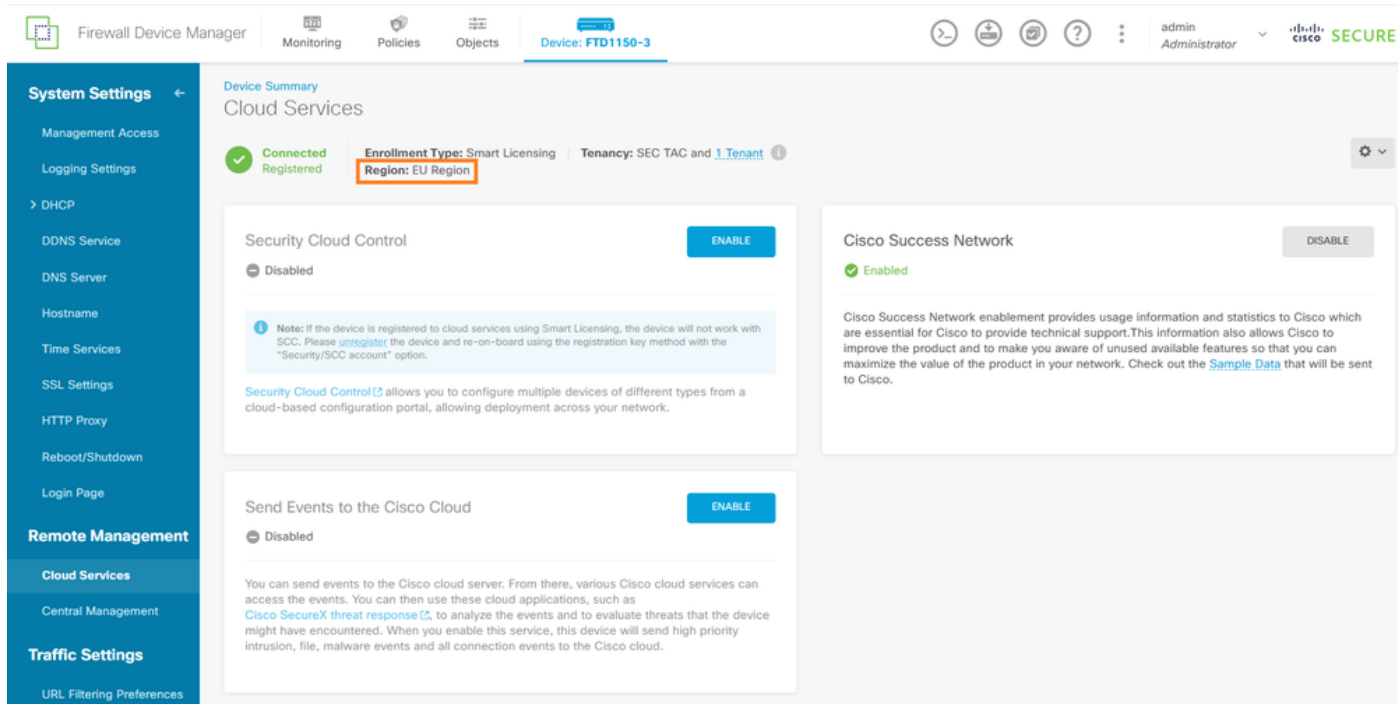
- Connected Registered:** Status is 'Connected' (green checkmark).
- Enrollment Type:** Smart Licensing.
- Tenancy:** SEC TAC and 1.Tenant.
- Region:** US Region (highlighted with a red box).

The 'Security Cloud Control' section is currently 'Disabled' (grey 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." Below this, it explains that Security Cloud Control allows configuring multiple devices from a cloud-based configuration portal.

The 'Cisco Success Network' section is currently 'Enabled' (green checkmark and 'ENABLE' button). A description states: "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."

The 'Send Events to the Cisco Cloud' section is currently 'Disabled' (grey button). A description states: "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."

輔助雲服務已在歐盟地區註冊：

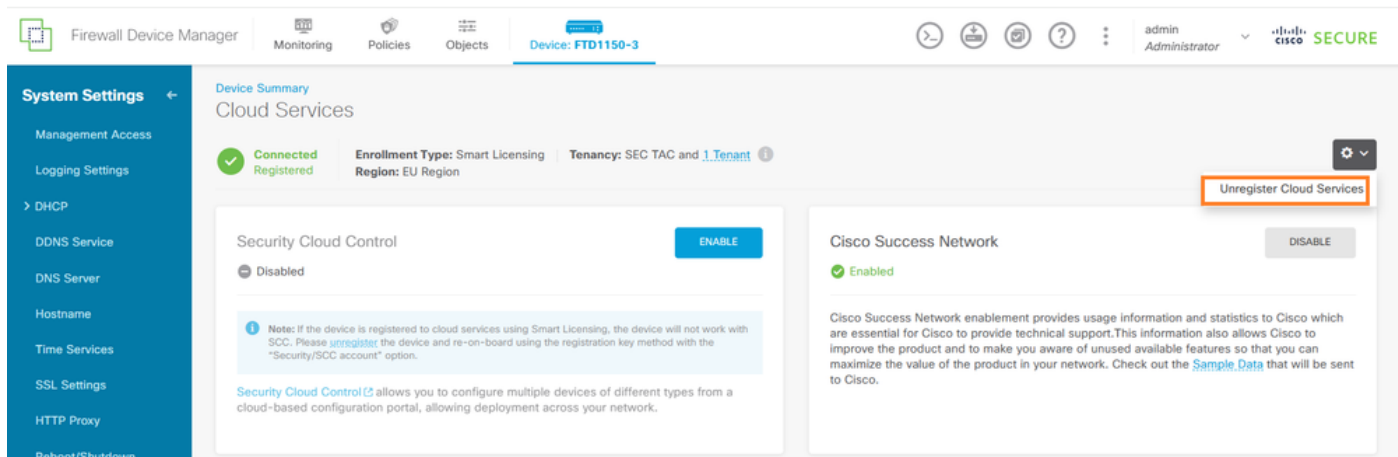


在這種情況下，使用者決定註冊輔助防火牆(FW2)以與主防火牆(FW1)相符。

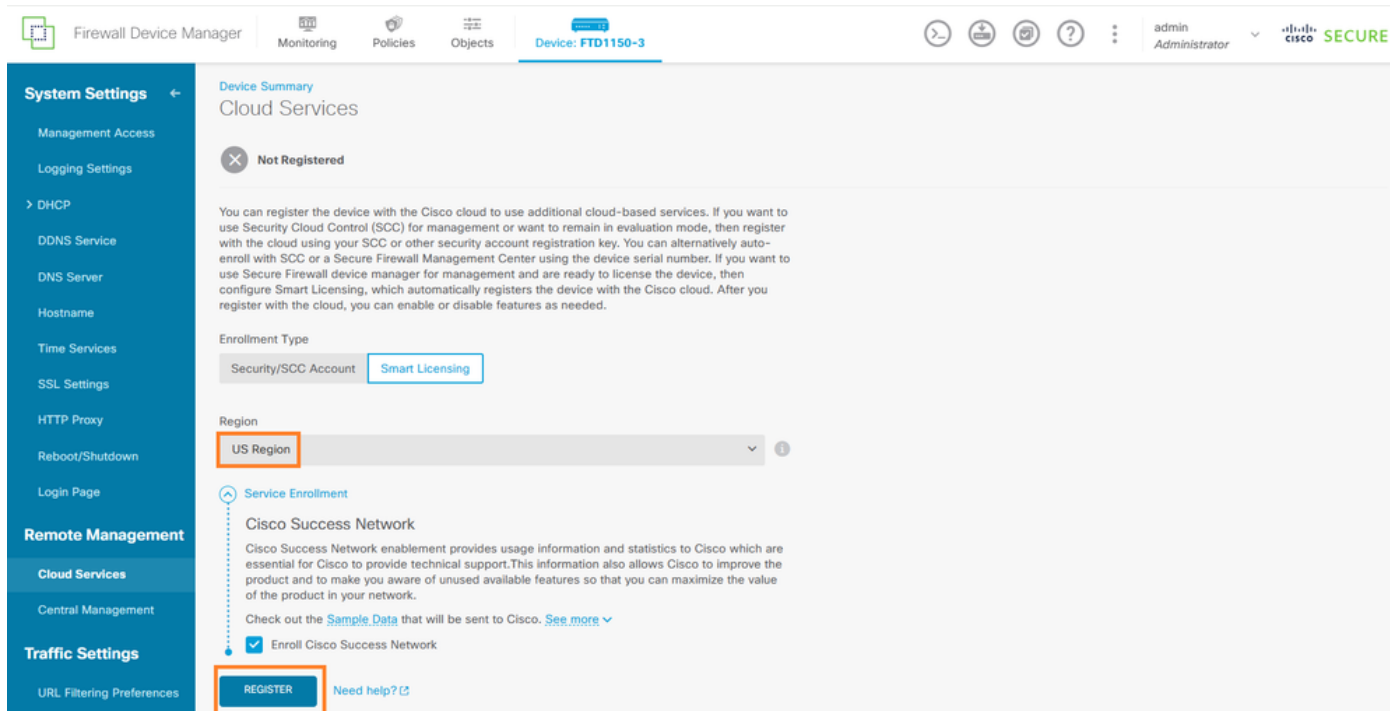
步驟 1:在思科雲服務中註冊FW2

使用與FW1（美國地區）相同的雲區域將FW2註冊到思科雲服務。

在FW2 FDM介面中，導航到Device > System Settings > Cloud Services，然後註銷雲服務：

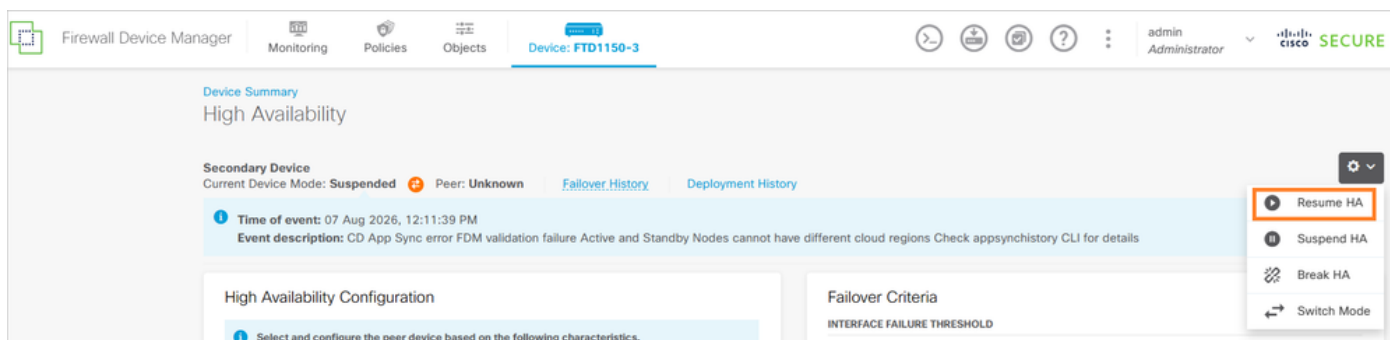


然後，將FW2註冊到FW1使用的同一區域：



步驟 2:重試HA配置

當兩台裝置顯示相同的雲註冊狀態後，請恢復HA配置：



在輔助裝置的CLI中，您會看到：

```
<#root>
```

```
>
```

Detected an Active mate

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

幾分鐘後：

```
<#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

通常，兩台裝置必須在同一思科雲服務區域中註冊，或者根本不能同時註冊兩台。

原因

根本原因是兩個Firepower 1150裝置之間的思科雲服務註冊狀態不匹配。如果一個節點已雲註冊，而另一個節點未註冊或註冊到其他區域，FDM會阻止HA應用同步。此驗證可確保HA對中的兩台裝置維持一致的雲連線和功能可用性。

具體的技術原因在於FW1註冊到Cisco Cloud Services US區域，而FW2註冊到EU區域，導致HA對形成處於不相容狀態。

相關內容

- [思科Firepower威脅防禦高可用性配置指南](#)
- [Cisco Firepower裝置管理器系統設定配置](#)
- [使用FDM配置FTD高可用性](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。