

# 排除FDM上的高可用性配对故障

## 目录

---

## 问题

在应用同步期间，运行FTD 7.4.2.4的两台Cisco Firepower 1120设备之间的高可用性(HA)配对失败，由于许可证注册模式不匹配，辅助节点始终进入“失败”状态。遇到的特定错误消息如下：

```
CD App Sync error FDM validation failure License registration mode mismatch between Primary and Secondary
```

show app-sync-history命令显示重复失败的消息，例如：

```
App Sync Status: FAILURE  
Failed Reason: FDM validation failure - License agent compliance mismatch between Primary and Secondary
```

在两个防火墙重置后、配置从备份恢复、软件更新到FTD版本7.4.2.4、VDB和Snort版本更新以及许可证重新应用新的令牌后出现此问题。辅助防火墙仍处于“失败”状态，从而阻止HA完成并影响防火墙冗余。

## 环境

- 为高可用性配置的Cisco Firepower 1120 NGFW设备
- Firepower威胁防御(FTD)版本7.4.2.4-9
- Snort检测引擎：3.1.53.203 - 175
- VDB:425.0
- 地理位置数据库：2026-03-07-053
- 设备从智能许可转换为PLR (永久许可证保留) 模式

- 在PLR转换后尝试云连接的主设备
- 两台设备均从备份还原

## 分辨率

解决方法涉及识别并纠正主设备和辅助设备之间的许可证注册模式不匹配、执行云注销以及完成完整部署。

### 步骤 1：确定许可证注册模式不匹配

通过检查应用同步历史记录以验证两台设备上的许可证注册模式，了解具体的故障原因：

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

输出显示的故障表明：

```
FDM validation failure - License registration mode mismatch between Primary and Secondary node
```

### 步骤 2：执行云注销

由于主设备在从智能许可模式转换到PLR模式后仍在尝试云连接，因此需要进行云注销。

在FDM UI中配置临时代理（如果未配置代理）：

导航到System Settings > See More > HTTP Proxy选项卡，并临时配置虚拟代理[稍后可将其删除]。

通过SSH连接到FTD设备并执行连接器脚本：

```
ssh admin@<device-ip>
expert
sudo su
/ngfw/var/sf/bin/connector.sh
```

### 步骤 3：解决端口8989冲突

如果连接器脚本因以下错误而失败：

```
Error: listen tcp :8989: bind: address already in use
```

使用端口8989 (通常为Cisco Success Network ) 识别和终止流程：

```
netstat -tulpn | grep 8989
kill <pid>
```

### 步骤 4：完成云注销

解决端口冲突后重新运行连接器脚本：

```
/ngfw/var/sf/bin/connector.sh
```

成功执行必须显示类似以下内容的输出：

```
Starting connector
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: https_proxy=http://1xx.xx.x
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: http_proxy=http://1xx.xx.x
```

转到FDM GUI“系统设置”(System Settings)>“云服务”(Cloud Services)>“云服务”(Cloud Services)，然后点击取消注册选项。验证设备是否已从云服务注销。

## 步骤 5：执行完全部署并恢复HA

在云取消注册后，如果HA配对仍然失败，并出现相同的许可证不匹配错误，请通过FDM接口在主用设备上执行完全部署。

导航到部署>立即部署，完成部署过程。

部署完成后，请重试HA形成。设备必须成功形成接口已连接且处于就绪状态的主用 — 备用HA对。

## 步骤 6：验证HA状态

确认成功形成HA:

```
show failover
```

输出必须显示两个单元处于正确的高可用性状态，并且同步成功。

## 原因

根本原因是主Firepower 1120设备和辅助Firepower 1120设备之间的许可证注册模式不匹配。设备已从智能许可模式转换为PLR（永久许可证保留）模式；但是，主设备继续尝试云连接，导致HA验证期间许可证代理/出口合规性状态不匹配。这会在应用程序同步期间导致重复的FDM/FIM验证失败。此外，云注销最初被与Cisco Success Network相关的端口8989冲突阻止，需要解决此冲突才能继续注销。

## 相关内容

- [在气隙网络中应用永久许可证](#)
- [重新映像安全防火墙威胁防御](#)

- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。