# 解決Nexus 9000交換機上的MACSec MKA PDU完整性檢查故障

## 目錄

## 問題

在Nexus 9000交換機之間配置的介質訪問控制安全(MACSec)將MACsec金鑰協定(MKA)會話顯示為「安全」，但大約每兩秒生成一次重複錯誤消息。以下模式將泛洪系統日誌：

```
device# %CTS-5-CTS_MKPDU_ICV_SUCCESS: MACSec: MKPDU verified. Primary keys match for Interface
device# %CTS-4-CTS_MKPDU_ICV_FAILURE: MACSec: MKA PDU integrity check failed for Interface
```

這些交替的成功和失敗消息會建立過多日誌條目，需要在維護MACSec功能的同時進行修復。

## 環境

- 產品：Cisco Nexus交換機
- 技術：MACSec（鏈路加密）

## 解析

要解決此問題，請修改回退金鑰鏈配置以使用與主金鑰鏈中配置的金鑰ID不同的金鑰ID:

1.使用此命令檢查現有的MACSec金鑰鏈配置，以確定主金鑰鏈和備用金鑰鏈之間的匹配金鑰ID。

```
device# show running-configuration
...
```

```
key chain primary macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
key chain fallback macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
...
```

2.使用這些命令將回退金鑰鏈更改為使用不同的金鑰ID。例如，如果主金鑰鏈使用金鑰ID 01，請將回退金鑰鏈配置為使用金鑰ID 10。

```
device# configure terminal
device(config)# key chain fallback macsec
device(config)# no key 01
device(config)# key 10
device(config)# key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
```

3.監控系統日誌，以確認不再出現交替的CTS_MKPDU_ICV_SUCCESS和CTS_MKPDU_ICV_FAILURE消息。

## 原因

根本原因是配置衝突，其中回退金鑰鏈使用與主金鑰鏈相同的金鑰ID。這會在MKA協定中造成歧義，導致完整性檢查隨著系統在評估主鍵和回退鍵之間進行切換而交替成功和失敗。Nexus MACSec配置指南規定「回退金鑰ID不應與主金鑰鏈中的任何金鑰ID匹配」可防止此衝突。

## 相關內容

- Nexus MACSec配置指南
- 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）。