解决Nexus 9000交换机上的MACSec MKA PDU完整性检查故障

目录

问题

在Nexus 9000交换机之间配置的介质访问控制安全(MACSec)将MACsec密钥协议(MKA)会话显示为“安全”，但大约每两秒生成一次重复的错误消息。以下模式会泛洪系统日志：

```
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
```

这些交替的成功和失败消息会创建过多日志条目，需要在维护MACSec功能的同时进行补救。

环境

- 产品：Cisco Nexus交换机
- 技术：MACSec（链路加密）

分辨率

要解决此问题，请修改回退密钥链配置以使用与主密钥链中配置的密钥ID不同的密钥ID:

1.使用此命令检查现有的MACSec密钥链配置，以确定主密钥链和回退密钥链之间的匹配密钥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.使用这些命令将回退密钥链更改为使用不同的密钥ID。例如，如果主密钥链使用密钥ID 01，请将回退密钥链配置为使用密钥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.监控系统日志，以确认不再出现交替出现的CTS_MKPDU_ICV_SUCCESS和CTS_MKPDU_ICV_FAILURE消息。

原因

根本原因是配置冲突，其中回退密钥链使用与主密钥链相同的密钥ID。这会在MKA协议中造成歧义，导致完整性检查交替成功和失败，因为系统会在评估主键和回退键之间切换。Nexus MACSec配置指南规定，“回退密钥ID不应与主密钥链中的任何密钥ID匹配”可防止此冲突。

相关内容

- Nexus MACSec配置指南
- 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）。