Resolva falhas de verificação de integridade da PDU MACSec MKA em switches Nexus 9000

Contents

Problema

O Media Access Control Security (MACSec) configurado entre os switches Nexus 9000 mostra a sessão do MACsec Key Agreement (MKA) como "segura", mas gera mensagens de erro repetidas aproximadamente a cada dois segundos. O padrão a seguir inunda os logs do sistema:

```
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
```

Essas mensagens alternadas de êxito e falha criam entradas de registro excessivas que precisam ser corrigidas enquanto se mantém a funcionalidade MACSec.

Ambiente

- Produto: Switches Cisco Nexus
- Tecnologia: MACSec (criptografia de link)

Resolução

Para resolver esse problema, modifique a configuração do conjunto de chaves de fallback para usar IDs de chave diferentes dos configurados no conjunto de chaves primário:

1. Revise suas configurações de conjunto de chaves MACSec existentes para identificar IDs de

chave correspondentes entre os conjuntos de chaves principal e de fallback com este comando.

```
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. Altere o conjunto de chaves de fallback para usar um ID de chave diferente com esses comandos. Por exemplo, se o conjunto de chaves principal usar o ID de chave 01, configure o conjunto de chaves de fallback para usar o ID de chave 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. Monitore os logs do sistema para confirmar que as mensagens CTS_MKPDU_ICV_SUCCESS e CTS_MKPDU_ICV_FAILURE alternadas não serão mais exibidas.

Causa

A causa raiz é um conflito de configuração em que o conjunto de chaves de fallback usa o mesmo ID de chave que o conjunto de chaves primário. Isso cria ambiguidade no protocolo MKA, fazendo com que a verificação de integridade seja alternadamente bem-sucedida e falhe à medida que o sistema alterna entre avaliar as chaves primária e de fallback. O Guia de configuração do Nexus MACSec afirma: "O ID da chave de fallback não deve corresponder a nenhum ID de chave de um conjunto de chaves primário" para evitar esse conflito.

Conteúdo relacionado

- Guia de configuração do Nexus MACSec

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.