Resolver errores de comprobación de integridad de MKA PDU MACSec en switches Nexus 9000

Contenido

Problema

Media Access Control Security (MACSec) configurado entre switches Nexus 9000 muestra la sesión MACsec Key Agreement (MKA) como "segura", pero genera mensajes de error repetidos aproximadamente cada dos segundos. El siguiente patrón inunda los registros del 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
```

Estos mensajes de error y de éxito alternos crean entradas de registro excesivas que deben remediarse mientras se mantiene la funcionalidad de MACSec.

Entorno

- Producto: switches Nexus de Cisco
- Tecnología: MACSec (cifrado de enlaces)

Resolución

Para resolver este problema, modifique la configuración de la cadena de claves de reserva para utilizar ID de clave diferentes de las configuradas en la cadena de claves principal:

1. Revise las configuraciones de MACSec keychain existentes para identificar ID de clave

coincidentes entre las cadenas de clave principal y de reserva con 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. Cambie el llavero de reserva para utilizar un identificador de clave diferente con estos comandos. Por ejemplo, si el llavero principal utiliza el identificador de clave 01, configure el llavero de reserva para que utilice el identificador de clave 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. Supervise los logs del sistema para confirmar que los mensajes CTS_MKPDU_ICV_SUCCESS y CTS_MKPDU_ICV_FAILURE alternativos ya no aparecen.

Causa

La causa principal es un conflicto de configuración en el que la cadena de claves de reserva utiliza el mismo ID de clave que la cadena de claves principal. Esto crea ambigüedad en el protocolo MKA, lo que hace que la comprobación de integridad se realice correctamente y falle alternativamente a medida que el sistema cambia entre la evaluación de las claves principal y de reserva. La Guía de configuración de Nexus MACSec establece que "el ID de clave de reserva no debe coincidir con ningún ID de clave de un key chain principal" para evitar este conflicto.

Contenido relacionado

- Guía de configuración de Nexus MACSec

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).