Risoluzione dei problemi di controllo dell'integrità della PDU MKA MACSec sugli switch Nexus 9000

Sommario

Problema

La configurazione di MACSec (Media Access Control Security) tra switch Nexus 9000 consente di visualizzare la sessione MACsec Key Agreement (MKA) come "protetta", ma genera messaggi di errore ripetuti circa ogni due secondi. Il seguente modello sovraccarica i log di 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
```

Questi messaggi alternati di esito positivo e negativo creano un numero eccessivo di voci di registro che devono essere corrette mantenendo la funzionalità MACSec.

Ambiente

- Prodotto: switch Cisco Nexus
- Tecnologia: MACSec (Link Encryption)

Risoluzione

Per risolvere il problema, modificare la configurazione del portachiavi di fallback in modo da utilizzare ID di chiave diversi da quelli configurati nel portachiavi primario:

1. Esaminare le configurazioni dei portachiavi MACSec esistenti per identificare gli ID di chiave corrispondenti tra le catene di chiavi primaria e di fallback con questo 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. Modificare la catena di chiavi di fallback in modo da utilizzare un ID chiave diverso con questi comandi. Ad esempio, se la catena di chiavi primaria utilizza l'ID chiave 01, configurare la catena di chiavi di fallback in modo che utilizzi invece l'ID chiave 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. Controllare i registri di sistema per verificare che i messaggi CTS_MKPDU_ICV_SUCCESS e CTS_MKPDU_ICV_FAILURE alternati non siano più visualizzati.

Causa

La causa principale è un conflitto di configurazione in cui il portachiavi di fallback utilizza lo stesso ID di chiave del portachiavi primario. Ciò crea ambiguità nel protocollo MKA, causando l'esito negativo del controllo di integrità e la conseguente commutazione del sistema tra la valutazione delle chiavi primarie e di fallback. Per evitare questo conflitto, nella guida alla configurazione di Nexus MACSec viene indicato che "l'ID della chiave di fallback non deve corrispondere ad alcun ID di chiave proveniente da una catena di chiavi primaria".

Contenuto correlato

- Guida alla configurazione di Nexus MACSec
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).