Risoluzione dei problemi relativi alla creazione del cluster di bilanciamento del carico VPN dopo l'aggiornamento di ASA o FTD alla protezione avanzata, settembre 2026

Sommario

- Problema
- Ambiente
- Risoluzione
  - Opzione 1: Completa aggiornamento (scelta consigliata)
  - Opzione 2: Metodo di aggiornamento hitless (solo ASA)
  - Fasi di verifica
- Causa
- Contenuto correlato

Problema

Dopo aver aggiornato i dispositivi Cisco ASA o FTD a una delle versioni pubblicate come parte della release di protezione avanzata di settembre 2026, i cluster di bilanciamento del carico VPN (VPN Load Balancing) non possono formarsi. Si sono verificati ripetuti errori di connessione nei dispositivi, come mostrato nell'output del comando debug:

```
device# debug vpnlb 125
debug vpnlb enabled at level 125
device# 5718045: Created peer[198.51.100.1]
5718012: Sent HELLO request to [198.51.100.1]
```

```
5718061: Inbound socket read fail: context=0.
7718036: Process timeout for req-type[13], exid[304], peer[198.51.100.1]
6718038: Slave processed 1 timeouts
5718028: Send OOS indicator failure to [198.51.100.1]
5718056: Deleted Master peer, IP 198.51.100.1
5718044: Deleted peer[198.51.100.1]
7718017: Got timeout for unknown peer[198.51.100.1] msg type[25]
```

Quando la crittografia del cluster è disabilitata, il cluster di bilanciamento del carico VPN viene creato correttamente. Tuttavia, la riattivazione della crittografia causa l'errore della formazione del cluster e, nonostante la configurazione sia stata completata, non vengono visualizzati messaggi di debug IKEv1.

Questo problema riguarda solo il coordinamento tra i membri all'interno del cluster; le sessioni client VPN ad accesso remoto non vengono eliminate. Il membro del cluster interessato non partecipa al bilanciamento del carico VPN finché non viene aggiornato.

Ambiente

- Cisco Secure Firewall ASA o FTD
- Versione del software ASA o FTD contenente la correzione per la release di protezione avanzata: Settembre 2026
- Configurazione del bilanciamento del carico VPN con crittografia del cluster abilitata
- Criteri IKEv1 configurati per la comunicazione cluster

Risoluzione

Per risolvere il problema sono disponibili due opzioni convalidate:

Opzione 1: Completa aggiornamento (scelta consigliata)

Aggiornare tutti i membri del cluster alla stessa versione software ASA o FTD. Il cluster viene riformato automaticamente quando tutti i membri eseguono la stessa release.

Finché tutti i membri del cluster non vengono aggiornati, i membri che eseguono versioni precedenti non sono sincronizzati con quelli che eseguono versioni più recenti.

Passaggio 1: Verificare le versioni software correnti in tutti i membri del cluster:

```
device# show version
```

Passaggio 2: Aggiornare i membri cluster rimanenti alla stessa versione software ASA o FTD.

Passaggio 3: Verificare la formazione del cluster dopo il completamento di tutti gli aggiornamenti:

```
device# show vpn load-balancing
```

Opzione 2: Metodo di aggiornamento hitless (solo ASA)

Rimuovere temporaneamente la chiave del cluster in tutti i membri durante il processo di aggiornamento, quindi riapplicarla dopo l'aggiornamento di tutti i dispositivi.

Passaggio 1: Rimuovere la chiave del cluster da tutti i membri del cluster:

```
device(config)# vpn load-balancing
device(config-load-balancing)# no cluster key
```

Passaggio 2: Aggiornare tutti i membri del cluster alla stessa versione del software ASA.

Passaggio 3: Riapplica la chiave del cluster a tutti i membri al termine dell'aggiornamento:

```
device(config)# vpn load-balancing
device(config-load-balancing)# cluster key your-cluster-key
```

Importante: La semplice rimozione della sola crittografia del cluster non è sufficiente. La chiave del cluster deve essere completamente rimossa durante il processo di aggiornamento.

Questa soluzione non si applica ai dispositivi FTD perché la crittografia è obbligatoria per i dispositivi FTD gestiti da FMC.

Fasi di verifica

Dopo aver implementato una delle due opzioni, verificare il corretto funzionamento del cluster.

Passaggio 1: Verificare le versioni software correnti in tutti i membri del cluster:

```
device# show version
```

Passaggio 2: Verificare che il cluster si sia formato dopo il completamento di tutti gli aggiornamenti:

```
device# show vpn load-balancing
```

Passaggio 3: Verificare la connettività peer:

```
device# debug vpnlb 125
```

Passaggio 4: Confermare che le associazioni di protezione IKEv1 siano state stabilite, se la crittografia è abilitata:

```
device# show crypto ikev1 sa
```

Prendere nota dell'ID bug Cisco CSCww64385. Questo problema influisce sulla visibilità della topologia e sui tempi di riconvergenza, ma non sulle connessioni VPN attive o sull'inoltro del traffico sui dispositivi aggiornati.

Causa

Questo problema è causato da un miglioramento della protezione avanzata che aggiunge l'autenticazione alla comunicazione tra i membri del cluster di bilanciamento del carico VPN. Il protocollo di sicurezza avanzato non è compatibile con le versioni ASA o FTD precedenti, impedendo la formazione di cluster in distribuzioni con versioni miste. Ne consegue un'incompatibilità di protocollo in cui:

- I nodi aggiornati applicano il protocollo v5 autenticato
- I nodi di pre-aggiornamento utilizzano il protocollo v4 non autenticato
- I membri aggiornati richiedono il protocollo con protezione avanzata con cui i membri meno recenti non possono comunicare
- La formazione del cluster non riesce finché tutti i membri non utilizzano la stessa versione del protocollo

Contenuto correlato

- 'ID bug Cisco CSCww64385'
- 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).