Best practice per l'implementazione di Cisco IOS XR per OSPF/IS-IS e routing BGP

Sommario

[UPDATE THE TABLE] 3
[UPDATE THE TABLE][UPDATE THE TABLE] 3
[UPDATE THE TABLE][UPDATE THE TABLE] 3
[UPDATE THE TABLE] 3
[UPDATE THE TABLE] 4
[UPDATE THE TABLE][UPDATE THE TABLE] 4
[UPDATE THE TABLE][UPDATE THE TABLE] 5
[UPDATE THE TABLE][UPDATE THE TABLE] 5
[UPDATE THE TABLE] 5
[UPDATE THE TABLE][UPDATE THE TABLE] 6
[UPDATE THE TABLE][UPDATE THE TABLE] 7
[UPDATE THE TABLE][UPDATE THE TABLE] 7
[UPDATE THE TABLE][UPDATE THE TABLE] 8
[UPDATE THE TABLE][UPDATE THE TABLE] 8
[UPDATE THE TABLE] 9
[UPDATE THE TABLE] 11
[UPDATE THE TABLE][UPDATE THE TABLE] 11
[UPDATE THE TABLE][UPDATE THE TABLE] 13
[UPDATE THE TABLE][UPDATE THE TABLE] 14
[UPDATE THE TABLE] 15
[UPDATE THE TABLE][UPDATE THE TABLE] 15
[UPDATE THE TABLE][UPDATE THE TABLE] 16
[UPDATE THE TABLE][UPDATE THE TABLE] 17
[UPDATE THE TABLE][UPDATE THE TABLE] 19
[UPDATE THE TABLE][UPDATE THE TABLE] 21
[UPDATE THE TABLE] 22

AVVERTENZA

Questo documento fornisce un riepilogo di alto livello di alcune best practice consigliate per il routing OSPF/IS-IS e BGP. Queste raccomandazioni non rappresentano una progettazione convalidata da Cisco e per l'installazione in qualsiasi ambiente operativo specifico è necessario prestare la dovuta attenzione e attenzione. Devono essere letti insieme alle guide alla configurazione e alla documentazione tecnica dei prodotti pertinenti che descrivono in modo più dettagliato come queste raccomandazioni sulle migliori pratiche possono essere implementate. I riferimenti alle guide alla configurazione e alla documentazione tecnica per particolari prodotti contenuti in questo documento sono da intendersi come semplici esempi. Fare riferimento alle guide alla configurazione e alla documentazione tecnica per i prodotti specifici.

Introduzione

In questo documento vengono descritte alcune best practice consolidate e vengono forniti suggerimenti per la creazione di reti semplificate, efficienti e scalabili basate su piattaforme di routing IOS XR. In questo documento vengono illustrate le tecniche di implementazione specifiche e le opzioni di supporto delle funzionalità disponibili in IOS XR per la personalizzazione delle implementazioni OSPF/IS-IS e BGP.

Implementazione di OSPF

Il protocollo OSPF, definito nella RFC 2328, è un protocollo IGP utilizzato per distribuire le informazioni di routing all'interno di un singolo sistema autonomo. OSPF offre numerosi vantaggi rispetto ad altri protocolli, ma è necessaria una progettazione adeguata per creare una rete scalabile e a tolleranza di errore.
Per ulteriori informazioni su OSPF, consultare:

- Nota tecnica su OSPF: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#anc13
- Guida alla configurazione di OSPF: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-6/routing/configuration/guide/b-routing-cg-asr9000-76x/implementing-ospf.html
- Informazioni di riferimento sui comandi: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/routing/command/reference/b-routing-cr-asr9000-75x/ospf-commands.html#wp2421918195

Concetti fondamentali

- Gerarchia: Un modello di rete gerarchico è un utile strumento di alto livello per la progettazione di infrastrutture di rete affidabili e consente di suddividere i problemi di progettazione di reti complesse in aree più piccole e più gestibili.
- Modularità: Dividendo varie funzioni di una rete in moduli, la rete è molto più facile da progettare. Cisco ha identificato diversi moduli, tra cui il campus aziendale, il blocco di servizi, il centro dati e il perimetro di Internet.
- Resilienza: La rete è disponibile sia in condizioni normali che anomale. Le condizioni normali includono i flussi di traffico previsti, gli schemi e gli eventi pianificati, ad esempio le finestre di manutenzione. Le condizioni anormali includono guasti hardware o software, carichi di traffico

estremi, modelli di traffico insoliti, eventi DoS (Denial-of-Service) e altri eventi pianificati o non pianificati.

■ Flessibilità: la possibilità di modificare parti della rete, aggiungere nuovi servizi o aumentare la capacità senza dover affrontare un upgrade radicale (ad esempio, la sostituzione dei principali dispositivi hardware).

Come buona norma, l'implementazione della rete deve tenere conto del fatto che lo "span" della rete contiene le route all'interno di un limite specifico e le route rilevanti e richieste dai router di un dominio per l'inoltro. L'uso efficace delle aree OSPF consente di ridurre il numero di annunci allo stato del collegamento (LSA) e di altro traffico di sovraccarico inviati attraverso la rete. Uno dei vantaggi della creazione di una gerarchia consiste nel fatto che questo approccio contribuisce a garantire che le dimensioni del database della topologia che ogni router dovrà mantenere siano gestibili e conformi al profilo di memoria del router.

Ridistribuzione del dominio OSPF e BGP

OSPF è progettato per trasportare solo alcune migliaia di route. Ad alto livello, le "aree" OSPF sono sezioni di una rete in cui qualsiasi router è a conoscenza della capacità di routing di ogni altro router dell'area. Ciò consente una rapida convergenza quando un dispositivo presenta un problema, ma a costo di una scalabilità ridotta. Pertanto, OSPF viene utilizzato in un core Service Provider per fornire la connettività di livello base tra tutti i dispositivi core e tutti i dispositivi core vengono configurati all'interno della stessa area OSPF. Si tratta di una struttura standard di una rete "underlay".

Per contro, BGP è progettato per trasportare un numero di route significativamente maggiore rispetto alla maggior parte degli IGP, come OSPF. Rischi associati alla ridistribuzione delle route BGP in un IGP come OSPF. Se un provider di servizi richiede la ridistribuzione delle route BGP nel dominio IGP per qualsiasi scenario, la gestione deve essere eseguita dal provider di servizi con il filtro appropriato nei router ASBR (Autonomous System Boundary Router) e con la protezione dall'overload configurata sul router ricevente. Se la ridistribuzione BGP non è filtrata in un OSPF, ogni dispositivo OSPF nell'ASBR inizierà a ricevere route di gran lunga superiori alla sua capacità di gestire contemporaneamente. I router Cisco IOS XR, ad esempio, consentono la ridistribuzione in OSPF di solo 10.000 route BGP per impostazione predefinita. Quando le route BGP vengono ridistribuite nell'IGP, è possibile che tutti i router del dominio IGP ricevano queste route, a seconda della progettazione IGP. In base al protocollo RFC dell'OSPF, qualsiasi route esterna ridistribuita nell'OSPF deve essere distribuita a tutti i router dell'area OSPF.

Gestione della ridistribuzione in IGP

Come buona norma generale, la ridistribuzione dovrebbe essere effettuata solo in modo attento e pianificato quando non vi sono altre opzioni per apprendere le vie di raggiungibilità che una funzione di ridistribuzione fornirà.

In generale, è consigliabile:

■ Evitare la ridistribuzione
■ Evitare di trasportare i percorsi in un dominio IGP
■ Implementazione di BGP per la raggiungibilità esterna
■ Usare IGP per trasportare solo le informazioni sull'hop successivo; ad esempio, Loopback 0

Limitazioni di ridistribuzione della route OSPF

La scala dei prefissi ridistribuiti da BGP in OSPF viene gestita con la configurazione di protezione dall'overload (max-lsa). Si tratta dell'unica protezione contro la perdita di un numero elevato di route nel dominio OSPF. In caso di ridistribuzione in una singola area OSPF, è necessario implementare più livelli di protezione contro la ridistribuzione della route.

Di seguito sono elencate alcune delle opzioni disponibili per la protezione dalla ridistribuzione delle route:

- Filtraggio di ridistribuzione con ACL
- Limite di ridistribuzione - impostazione globale per impedire la ridistribuzione di più di un numero specifico di route. Se il filtro viene rimosso, il limite di ridistribuzione globale è la seconda linea di difesa e protegge i core.
- Configurazioni Max-LSA su tutti i dispositivi nell'area OSPF - se le protezioni indicate nei punti precedenti hanno esito negativo, forzare i router riceventi a rifiutare le LSA eccessive in entrata.

Protezione dall'overload del database allo stato del collegamento OSPF

La funzione OSPF Link-State Database Overload Protection fornisce un meccanismo a livello OSPF per limitare il numero di LSA non autogenerate per un determinato processo OSPF. Se altri router della rete sono stati configurati in modo errato, potrebbero generare un volume elevato di LSA, ad esempio per ridistribuire un numero elevato di prefissi in OSPF. Questo meccanismo di protezione aiuta a evitare che i router ricevano molte LSA e si verifichino quindi carenze di CPU e memoria.

Funzionamento delle feature

Di seguito viene illustrato il comportamento della funzionalità:

- Quando questa funzione è abilitata, il router tiene un conteggio del numero di tutte le LSA ricevute (non generate automaticamente).
- Quando viene raggiunto il valore soglia configurato, viene registrato un messaggio di errore.
- Quando viene superato il numero massimo configurato di LSA ricevute, il router non accetta più nuove LSA.

```
max-lsa <max-lsa-count> <%-threshold-to-log-warning> ignore-count <ignore-count-value> ignore-time <ignore-time-in-minutes> reset-time <time-to-reset-ignore-count-in-minutes>
```

Stati OSPF

Se il numero di LSA ricevuti è superiore al numero massimo configurato dopo un minuto, il processo OSPF elimina tutte le adiacenze e cancella il database OSPF. Questo stato è denominato stato ignore. In questo stato, tutti i pacchetti OSPF ricevuti su tutte le interfacce appartenenti all'istanza OSPF vengono ignorati e sulle interfacce non vengono generati pacchetti OSPF. Il processo OSPF rimane nello stato ignore per la durata del tempo di ignoramento configurato (il valore predefinito è 5 minuti). Alla scadenza del tempo di ignora, il processo OSPF torna al funzionamento normale e crea adiacenze su tutte le relative interfacce.

Se il conteggio LSA supera il numero max non appena l'istanza OSPF ritorna dallo stato ignore, l'istanza OSPF può oscillare all'infinito tra il suo stato normale e lo stato ignore. Per evitare questa oscillazione infinita, l'istanza OSPF conta quante volte è stata ignorata. Questo contatore

è denominato ignore-count. Se ignore-count (il valore predefinito ignore-count è 5) supera il valore configurato, l'istanza OSPF rimane in modo permanente nello stato ignore.
Per ripristinare lo stato normale dell'istanza OSPF, è necessario eseguire il comando clear ospf.
Il valore ignore-count viene reimpostato su zero se il conteggio LSA non supera di nuovo il numero massimo durante il tempo configurato dalla parola chiave reset-time.
Se si utilizza la parola chiave warning-only, l'istanza OSPF non entra mai nello stato ignore. Quando il conteggio LSA supera il numero massimo, il processo OSPF registra un messaggio di errore e l'istanza OSPF continua il suo normale funzionamento.
Non è disponibile un valore predefinito per max-lsa. Il limite viene controllato solo se è configurato in modo specifico.

Dopo aver configurato max-lsa, gli altri parametri possono avere valori predefiniti:

- avviso predefinito %-soglia-log - 75%
- valore-conteggio-ignora-predefinito - 5
- ignorare il tempo-in-minuti predefinito - 5 minuti
- tempo predefinito di ripristino-conteggio-ignora-conteggio - 10 minuti

Di seguito è riportato un esempio di implementazione che mostra come configurare l'istanza OSPF in modo che accetti 12000 LSA non generate automaticamente e 1000 LSA non generate automaticamente nel VRF V1.

```
RP/0/RSP0/CPU0:router# configurazione
RP/0/RSP0/CPU0:router(config)# router ospf 0
RP/0/RSP0/CPU0:router(config-ospf)# max-lsa 12000
RP/0/RSP0/CPU0:router(config-ospf)# vrf V1
RP/0/RSP0/CPU0:router(config-ospf)# max-lsa 1000
```

Nell'esempio seguente viene illustrato come visualizzare lo stato corrente dell'istanza OSPF.

```
RP/0/RSP0/CPU0:router# show ospf 0
    Processo di routing "ospf 0" con ID 10.0.0.2
    L'NSR (Non-Stop Routing) è disabilitato
    Supporta solo route TOS(TOS0) singole
    Supporta LSA opaco
    È un router di confine area
    Numero massimo di LSA non autogenerate consentite 12000
       Numero corrente di LSA 1 non autogenerato
       Soglia per il messaggio di avviso 75%
       Ignora-tempo 5 minuti, reimposta-tempo 10 minuti
       Ignore-count consentito 5, current ignore-count 0
```

Implementazione di BGP

Le famiglie di indirizzi BGP rendono il BGP un protocollo di routing "multiprotocollo". Si consiglia di comprendere in che modo le famiglie di indirizzi vengono utilizzate per creare

topologie scalabili facili da implementare e gestire. Utilizzando le famiglie di indirizzi, l'operatore può creare topologie diverse per tecnologie diverse, ad esempio EVPN, Multicast e così via.

Per ulteriori informazioni su BGP, vedere la guida alla configurazione di BGP: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html

BGP e BFD

La convergenza BGP in una rete di provider di servizi è importante per soddisfare le aspettative dei clienti nella creazione di reti resilienti e fault-tolerant. Per impostazione predefinita, il BGP dispone di un timer Keepalive di 60 secondi e di un timer Hold di 180 secondi. Ciò significa che la convergenza di BGP sarà molto lenta, a meno che non sia disponibile una guida dai protocolli di supporto. BFD (Bi-directional Forwarding) è un protocollo di questo tipo progettato per accelerare la convergenza dei protocolli client. Con BFD, i protocolli possono convergere in pochi secondi.

Ulteriori informazioni

■ Questa guida fornisce informazioni concettuali e di configurazione per il BFD: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/76x/b-routing-cg-ncs5500-76x/implementing-bfd.html

■ Questo white paper presenta una vista incentrata sui provider di servizi sulla convergenza rapida utilizzando il BFD sui router Cisco NCS 5500 e Cisco Network Convergence System serie 500: https://xrdocs.io/ncs5500/tutorials/bfd-architecture-on-ncs5500-and-ncs500/

■ Per ulteriori informazioni sull'uso di BFD sulle interfacce Bundle e sull'implementazione di BFD Multipath e MultiHop, consultare il repository https://xrdocs.io/.

Rilevamento peer lento BGP

Un peer lento è un peer che non riesce a mantenere la velocità con cui il router genera messaggi di aggiornamento per un periodo di tempo prolungato (in ordine di minuti) in un gruppo di aggiornamento. Quando in un gruppo di aggiornamento è presente un peer lento, viene generato il numero di aggiornamenti formattati in attesa di trasmissione. Quando viene raggiunto il limite della cache, il gruppo non dispone di altre quote per formattare i nuovi messaggi. Per formattare un nuovo messaggio, alcuni messaggi esistenti devono essere trasmessi utilizzando il peer lento e quindi rimossi dalla cache. Gli altri membri del gruppo che sono più veloci del peer lento e hanno completato la trasmissione dei messaggi formattati non avranno niente di nuovo da inviare, anche se ci possono essere reti BGP modificate di recente in attesa di essere pubblicizzate o ritirate. Questo effetto del blocco della formattazione di tutti i peer di un gruppo quando uno dei peer è lento nel consumo degli aggiornamenti è il problema del "peer lento".

Gli eventi che causano un cambiamento significativo nella tabella BGP (ad esempio le reimpostazioni di connessione) possono causare un breve picco nella frequenza di generazione degli aggiornamenti. Un peer che rimane temporaneamente indietro durante tali eventi ma si riprende rapidamente dopo l'evento non è considerato un peer lento. Affinché un peer venga contrassegnato come lento, deve essere incapace di tenere il passo con la velocità media degli aggiornamenti generati in un periodo più esteso (nell'ordine di alcuni minuti).

Il peer BGP lento può essere causato da:

■ Perdita di pacchetti o traffico elevato sul collegamento al peer.
■ Un peer BGP potrebbe essere sovraccarico in termini di CPU e quindi non è in grado di servire la connessione TCP alla velocità richiesta.
■ In questo caso, controllare la capacità hardware della piattaforma e il carico offerto.
■ Problemi di velocità effettiva con la connessione BGP
■ Per ulteriori informazioni sul rilevamento peer BGP Slow, vedere: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html#concept_ir5_j4w_p4b
Di seguito sono riportate alcune limitazioni e best practice per la gestione dei peer lenti:

■ QoS end-to-end, che riserva la larghezza di banda per il traffico dei control plane BGP durante la congestione.
■ Uso di valori MSS/MTU corretti e appropriati usando le impostazioni PMTUD BGP e/o MSS TCP.
■ Utilizzare l'hardware corretto e ridurre il numero di percorsi rispetto all'hardware.
Il rilevamento dei peer lenti è abilitato per impostazione predefinita in Cisco IOS XR a partire dalla versione 7.1.2. I peer lenti sono peer lenti a ricevere ed elaborare gli aggiornamenti BGP in entrata e a confermare gli aggiornamenti al mittente. Se il peer lento partecipa allo stesso gruppo di aggiornamento degli altri peer, il processo di aggiornamento di tutti i peer potrebbe risultare rallentato. In questa versione, quando IOS XR rileva un peer lento, crea un syslog contenente i dettagli sul peer specifico.

Convergenza rapida tramite convergenza indipendente con prefisso BGP

Per i prefissi BGP, la convergenza rapida viene ottenuta utilizzando BGP Prefix Independent Convergence (PIC), in cui BGP calcola un percorso migliore alternativo e un percorso migliore primario e installa entrambi i percorsi nella tabella di routing come percorsi primari e di backup.

Se il telecomando dell'hop successivo BGP diventa irraggiungibile, BGP passa immediatamente al percorso alternativo utilizzando BGP PIC anziché ricalcolare il percorso dopo l'errore.

Se il file PE remoto dell'hop successivo BGP è attivo, ma si verifica un errore di percorso, IGP TI-LFA FRR gestisce la riconversione rapida al percorso alternativo e BGP aggiorna l'hop successivo IGP per il file PE remoto.

BGP PIC è configurato nella famiglia di indirizzi VRF per una rapida convergenza dei prefissi VPN se un PE remoto diventa irraggiungibile.

Per ulteriori informazioni su BGP Prefix Independent Convergence, visitare il sito Web all'indirizzo https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/bgp-pic.html

Sicurezza BGP con BGP Flowspec

In breve, Flowspec BGP è una funzionalità che consente di ricevere le specifiche del flusso di traffico IPv4/IPv6 (origine X, destinazione Y, protocollo UDP, porta di origine A e così via) e le azioni da intraprendere sul traffico (come drop, polizia o reindirizzamento) tramite l'aggiornamento BGP.

All'interno dell'aggiornamento BGP, i criteri di corrispondenza Flowspec sono rappresentati da BGP NLRI e le community estese BGP rappresentano le azioni.

Questa funzionalità è basata sulla RFC 5575 e può essere utilizzata per ridurre gli attacchi DDoS. Quando un host specifico all'interno di una rete viene attaccato, è possibile inviare un aggiornamento Flowspec ai router perimetrali in modo che il traffico di attacco possa essere monitorato o interrotto, o addirittura reindirizzato altrove, magari a un'appliance in grado di pulire il traffico (filtrare il traffico "danneggiato" e inoltrare solo il traffico "buono" verso l'host interessato).

Una volta che le specifiche di flusso vengono ricevute da un router e programmate nelle schede di linea applicabili, qualsiasi porta L3 attiva su tali schede di linea inizierà l'elaborazione del traffico in entrata secondo le regole di Flowspec.

Per ulteriori informazioni sull'implementazione di BGP FlowSpec, vedere:

■ White paper BGP FlowSpec: https://xrdocs.io/ncs5500/tutorials/bgp-flowspec-on-ncs5500/
■ Guida alla configurazione BGP: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html#concept_uqv_bxq_h2b

Funzione BGP Maximum Prefix

La funzionalità Maximum-Prefix è utile quando, in seguito a una modifica dei criteri in uscita nel sito di peering remoto, un router inizia a ricevere un numero di prefissi superiore a quello che le risorse del router di peering possono gestire, ma anche per proteggere le risorse o i peer BGP interni in cui verranno inoltrati questi prefissi esterni. Tale sovraccarico di risorse potrebbe causare interruzioni.

La funzionalità BGP maximum-prefix impone un limite massimo al numero di prefissi ricevuti da un router adiacente per una determinata famiglia di indirizzi. Per impostazione predefinita, quando il numero di prefissi ricevuti supera il numero massimo configurato, la sessione BGP invia una notifica di interruzione al router adiacente e la sessione viene terminata. Una famiglia di indirizzi che supera il prefisso massimo interrompe l'intera sessione BGP, con un impatto su tutte le altre famiglie di indirizzi abilitate in quella sessione BGP.

Questa funzionalità viene in genere utilizzata per i peer BGP esterni per proteggere l'infrastruttura interna di un provider di servizi. Funge da guardrail per impedire l'esaurimento delle risorse del router che potrebbe essere causato da una configurazione errata, localmente o sul router adiacente remoto. Si consiglia di configurare maximum-prefix per proteggere il sistema da errori di configurazione locali o remoti che potrebbero causare il flooding della tabella di routing. In questo modo si protegge anche dagli attacchi di disaggregazione dei prefissi.

La configurazione del prefisso massimo BGP deve essere abilitata in modo esplicito su tutti i router eBGP per limitare il numero di prefissi che deve ricevere da un particolare router adiacente, sia cliente che peer AS. Si consiglia all'operatore di configurare un margine accettabile di prefissi aggiuntivi che il sistema potrebbe essere in grado di sostenere dopo un'attenta valutazione della memoria di sistema disponibile. Si noti che non esiste una

configurazione adatta a tutte le configurazioni che può essere applicata a tutti i router e la soglia deve essere regolata attentamente in base al ruolo del dispositivo nella rete. Ad esempio, se il prefisso massimo BGP deve essere configurato sui router adiacenti IBGP, il valore del prefisso massimo deve essere inferiore sui router adiacenti configurati sul router-reflector rispetto a quello dei router adiacenti configurati sui router-reflector-client. Il reflector di routing aggrega i prefissi ricevuti da più router peer e quindi annuncia nuovamente l'intera tabella ai client del reflector di routing. Pertanto, il riflettore di routing annuncerà ai propri client un numero di prefissi maggiore di quello che riceve da ogni singolo peer. Analogamente, un router peer può anche reannunciare più prefissi verso il riflettore di routing di quanti ne riceva da ogni singolo peer esterno.

Per riassumere, si consiglia di esaminare e configurare attentamente l'azione appropriata da intraprendere quando viene raggiunta la soglia del prefisso massimo su un dispositivo di produzione. Di seguito sono descritti alcuni attributi delle opzioni del comando maximum-prefix:

- Quando una sessione BGP è configurata in modo esplicito con la funzione maximum-prefix senza parole chiave aggiuntive (ad esempio, warning-only o potenziale restart), la sessione viene disattivata come comportamento predefinito. L'azione predefinita di una sessione peer interrotta senza ripristino automatico potrebbe causare un'interruzione prolungata all'interno del core.

```
%ROUTING-BGP-5-ADJCHANGE_DETAIL : router adiacente 10.10.10.10 Inattivo
- Ricevuta notifica BGP, raggiunto numero massimo di prefissi (VRF:
predefinito; AFI/SAFI: 1/1, 1/128, 2/4, 2/128, 1/133, 2/133) (AS:
65000) "
%ROUTING-BGP-5-NBR_NSR_DISABLED_STANDBY: NSR disabilitato sul router
adiacente 10.10.10.10 sulla porta RP in standby a causa del superamento
del limite massimo di prefissi da parte del peer (VRF: impostazione
predefinita)
```

- Configurando l'opzione Elimina percorsi aggiuntivi, tutti i prefissi in eccesso ricevuti dal router adiacente superano la soglia di valore massimo configurata. Questa perdita non causa il flap della sessione. I vantaggi di questa opzione includono la limitazione dell'utilizzo della memoria di processo BGP e l'arresto del flapping dei peer all'interno della rete principale. Tuttavia, ciò potrebbe causare l'eliminazione dei loop di inoltro per i prefissi, in quanto le voci di inoltro potrebbero diventare incoerenti tra i router della rete.
- Quando si utilizza add-path, il valore di prefisso massimo configurato si applica ai percorsi anziché ai prefissi, in quanto l'NLRI è costituito dagli attributi prefisso e percorso. Per ulteriori informazioni, consultare la seguente guida di riferimento ai comandi:

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/b-ncs5500-bgp-cli-reference/b-ncs5500-bgp-cli-reference_chapter_01.html

Consiglio: valutare attentamente le seguenti opzioni durante la configurazione del comando maximum-prefix:

- Nessuna azione esplicita definita: il router interrompe la sessione e mantiene inattiva la relazione con il router adiacente BGP fino a quando l'operatore non cancella manualmente la sessione BGP. [comando clear bgp]
- Restart [time-interval]: consente di interrompere la sessione e di tentare un riavvio automatico della sessione BGP periodicamente dopo un timer configurato. Questa operazione avrà esito positivo se il peer remoto interrompe l'annuncio dei prefissi in eccesso, altrimenti la sessione BGP si interromperà di nuovo (causando instabilità periodica).
- Discard-extra-path: con l'opzione discard-extra-path, la sessione BGP rimane attiva ma i prefissi oltre il limite massimo di prefissi vengono eliminati. Questa opzione non influisce su altre famiglie di indirizzi in cui il prefisso massimo non è stato raggiunto e garantisce che le risorse locali non siano esaurite, ma ciò potrebbe comportare l'eliminazione dei loop di inoltro per i prefissi. L'opzione elimina percorsi aggiuntivi non può coesistere con la manopola soft reconfig.
- Solo avvertenza: registra un'avvertenza solo quando viene raggiunta la soglia in modo che l'operatore possa eseguire azioni manuali per cancellare la condizione.

Per ulteriori informazioni, consultare la Guida alla configurazione del routing come indicato di seguito:

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-3/routing/configuration/guide/b-routing-cg-asr9000-73x/implementing-BGP.html#concept_5AF38064B1D044B7B5F439C10BCF9808

Procedure ottimali e suggerimenti

L'elenco seguente fornisce una panoramica delle procedure consigliate e dei consigli generali, elencati senza un ordine specifico:

■ Controllo della rete per lo stato generale del sistema. Iniziare con un controllo della configurazione e passare in sequenza dalle configurazioni dell'interfaccia al routing e ai servizi.
■ Attuare una strategia di monitoraggio. Sebbene l'SNMP sia una pratica standard, è consigliabile implementare tecniche più robuste e descrittive utilizzando la telemetria di streaming. Per raccomandazioni sulle best practice da adottare per l'implementazione della telemetria su un router IOS XR, consultare il seguente white paper:
https://xrdocs.io/telemetry/

OSPF

Di seguito sono riportate le procedure ottimali e le raccomandazioni generali per OSPF:

■ Implementare il riepilogo delle route per le route intra-area per OSPF.
■ Configurare esplicitamente l'ID router all'interno di OSPF come uno degli indirizzi di loopback abilitati per OSPF.

■ Progettare una rete gerarchica per limitare le LSA all'interno di un'area per OSPF. Mantenere il numero di ABR per un'area entro un intervallo ragionevole (~3-4).
■ Implementare la configurazione "max-lsa" OSPF per OSPF, o equivalente, per limitare le LSA nel database in modo da utilizzare efficacemente la memoria del sistema.
■ Limitare il numero massimo di route che possono essere distribuite da BGP a OSPF. In IOS-XR, il limite predefinito è 10K.
■ Utilizzare RPL (Route Policy) per ridistribuire le route in OSPF.
■ Riepilogare le route tra aree e le route esterne di tipo 5, ove applicabile.
■ Uso dell'autenticazione quando necessario.
■ Usare sempre NSF e NSR.
■ Configurare il filtro di ridistribuzione all'origine anziché alla destinazione.
■ Utilizzare l'interfaccia passiva, se applicabile.
■ OSPF deve avere solo route loopback e router-interface - rimuovere qualsiasi altra ridistribuzione da BGP a OSPF.
■ Considerare la possibilità di spostare ogni hub principale nella propria area (NSSA).
■ Utilizzare il BFD per rilevare rapidamente gli errori rispetto ai timer del protocollo di routing aggressivo.
■ Non usare il comando mtu-ignore per quanto possibile.
■ Prendere in considerazione l'uso della sincronizzazione IGP-LDP in un ambiente MPLS per evitare l'invio del traffico su un percorso senza etichetta.
■ Considerare la scala entro i limiti della piattaforma supportata (numero di prefissi, numero di etichette, ECMP, numero di aree e così via).
■ Evitare la ridistribuzione reciproca in più punti.
■ Configurare la distanza amministrativa in modo che ogni prefisso nativo di ciascun protocollo o processo venga raggiunto tramite il protocollo o processo del dominio corrispondente.
■ Controllare i prefissi (utilizzando la distanza o la combinazione di prefissi e elenchi) in modo che lo stesso prefisso non venga annunciato di nuovo al dominio di origine.
■ Sebbene l'ID di processo OSPF abbia un significato locale per il router, si consiglia di avere lo stesso ID di processo per tutti i router dello stesso dominio OSPF. Ciò migliora la coerenza della configurazione e semplifica le attività di configurazione automatica.
■ Quando si configura OSPF per ambienti hub e spoke, progettare le aree OSPF con un numero inferiore di router.
■ Configurare la larghezza di banda di riferimento del costo automatico dell'OSPF in tutto il dominio OSPF sul collegamento con la larghezza di banda più elevata della rete.
■ Dal punto di vista della progettazione, si consiglia di implementare il peering IGP con i domini sottoposti agli stessi controlli amministrativi o operativi per evitare la propagazione di aggiornamenti IGP non pianificati o non autorizzati attraverso la rete. In questo modo è possibile garantire una maggiore facilità di manutenzione e di risoluzione dei problemi in caso di errori. Nel caso in cui un dominio IGP di grandi dimensioni sia una necessità aziendale, pianificare l'uso di BGP in questi casi per limitare il numero di route nel dominio di rete IGP.
■ Se è necessaria la connettività MPLS end-to-end, continuare a utilizzare la gerarchia/segmentazione e le opzioni come la RFC3107 BGP-LU o il calcolo del percorso tra domini tramite PCE, oppure selezionare come ultima risorsa la ridistribuzione/perdita di dati con le policy.

■ La funzione OSPF Shortest Path First Throttling può essere utilizzata per configurare la pianificazione SPF in intervalli di millisecondi e per ritardare potenzialmente i calcoli SPF durante l'instabilità della rete.
■ La funzione di definizione delle priorità dei prefissi SPF OSPF consente agli amministratori di far convergere più rapidamente i prefissi importanti durante l'installazione della route.

IS-IS

Di seguito sono riportate le best practice e le raccomandazioni generali per IS-IS:

■ Se si esegue una rete piatta a livello singolo, pensare alla scala. Configurare tutti i router solo come L2. Per impostazione predefinita, il router è L1-L2 e la perdita di informazioni di routing da L1 a L2 è abilitata per impostazione predefinita. Ciò potrebbe causare la perdita di tutte le route L1 da parte di tutti i router a L2, con conseguente aumento del livello del database dello stato del collegamento.
■ Se si esegue una rete a più livelli (aree multiple), verificare che la topologia di layer 3 segua la gerarchia ISIS. Non creare collegamenti tra aree L1.
■ Se si esegue una rete multilivello (aree multiple), verificare che i router L1 e L2 siano collegati tramite entrambe le aree L1 e L2. Ciò non richiede più connessioni fisiche o virtuali tra di esse; eseguire il collegamento tra i router L1 e L2 come un circuito L1/L2.
■ Se si esegue una rete a più livelli (aree multiple), riepilogare i dati che possono essere riepilogati. Ad esempio, nel caso di MPLS, il loopback dei router PE deve essere propagato tra le aree, a differenza degli indirizzi dei collegamenti dell'infrastruttura.
■ Creare e seguire il piano di indirizzamento appropriato, se possibile. Ciò consente il riassunto e agevola la scalabilità.
■ Impostare la durata massima dell'LSP su 18 ore.
■ Evitare la ridistribuzione con qualsiasi mezzo. La ridistribuzione è complessa e deve essere gestita manualmente per evitare loop di routing. Se possibile, utilizzate la progettazione a più aree/livelli.
■ Se è necessario utilizzare la ridistribuzione, utilizzare l'assegnazione di tag di route durante la ridistribuzione e il filtro "distribuisci-lista in" basato sui tag per gestirla. Se possibile, eseguire il riepilogo durante la ridistribuzione.
■ Configurare le interfacce come "point-to-point" quando possibile. Ciò migliora le prestazioni e la scalabilità del protocollo.
■ Non utilizzare l'ISIS in topologie a mesh elevata. I protocolli dello stato del collegamento non funzionano correttamente in ambienti con mesh elevata.
■ Configurare una metrica predefinita alta nella modalità secondaria della famiglia di indirizzi ISIS. In questo modo si evita che i nuovi collegamenti aggiunti attirino traffico se vengono configurati inavvertitamente senza una metrica.
■ Configurare "log adiacency changes" per facilitare la risoluzione dei problemi di connessione.
■ Usare "metrica-wide" nella modalità secondaria ipv4 della famiglia di indirizzi ISIS. Le metriche restrittive non sono molto utili e non supportano funzioni come il routing dei segmenti o il flex-algo.
■ Se si sta utilizzando SR-MPLS TI-LFA ricordare di aggiungere "ipv4 mpls traffico-eng Loopback0" alla configurazione per consentire all'ISIS di allocare i tunnel TE quando necessario.

■ Lasciare le configurazioni "lsp-gen-interval" e "spf-interval" predefinite, a meno che non si sia certi che sia necessaria una convergenza nativa più rapida. Con TI-LFA la convergenza nativa non è così critica, poiché fast-reroute gestisce le singole modifiche di topologia in 50 ms o meno.
■ Se si modifica "lsp-gen-interval" o "spf-interval" non utilizzare un ritardo iniziale inferiore a 50 ms.
■ Nella maggior parte dei casi, "set-overload-bit" è una scelta migliore di "max-metric" in quanto è una modifica atomica supportata dalla funzione di fast-reute.
■ Utilizzare l'autenticazione crittografica per Hellos (hello-password) e LSP (lsp-password). Le catene di tasti offrono la massima flessibilità e possono
contenere rollover di tasti hitless.
■ Configurare "nsf cisco" per l'autenticazione hitless dei riavvii del processo ISIS e dell'installazione SMU. Nonostante il nome, questo fornisce una migliore interoperabilità con altri fornitori rispetto a "nsf ietf".
■ Su una piattaforma con due RP, configurare ANCHE "nsr" per gestire gli switchover RP.
■ Usare i modelli "gruppo" e "applica-gruppo" per configurare le sezioni di configurazione ripetute. Ciò consente di ridurre la probabilità di errore e di apportare modifiche più semplici se necessario.
■ In una rete multilivello, valutare attentamente se è necessario utilizzare la "propagazione" per perdere i prefissi dal livello 2 al livello 1. Ciò può limitare la scalabilità e spesso è sufficiente il percorso predefinito di livello 1 fornito dal bit allegato.
■ Se si utilizzano più istanze ISIS nello stesso VRF, considerare la configurazione di valori univoci per la "distanza". In questo modo, l'installazione del percorso nel RIB risulterà più deterministica se per ognuno è disponibile un percorso con lo stesso prefisso.
■ Utilizzare il BFD per il rilevamento rapido di link-down. Con la funzione BFD, l'intervallo di attesa ISIS può essere aumentato per migliorare la scalabilità.

BGP

Di seguito sono riportate le best practice e le raccomandazioni generali per BGP:

■ Utilizzare l'NSR e l'NSF / riavvio graduale con timer regolati attentamente a seconda della scala prevista.
■ Configurare BGP usando l'interfaccia di loopback "always UP" (sempre attivo), non l'interfaccia fisica per il peering IBGP.
■ Non ridistribuire le route BGP (alti volumi) in IGP (relativamente bassi volumi) e viceversa senza un'adeguata RPL, limitando il numero di route ridistribuite da BGP a un IGP (OSPF/ISIS).
■ Se si esegue la ridistribuzione da BGP a IGP senza un corretto e ben testato criterio (ACL), si potrebbe verificare l'esaurimento della memoria delle risorse sul router.
■ Uso delle route di riepilogo in BGP per ridurre le dimensioni della tabella di routing e l'uso della memoria. Aggregare le route con solo riepilogo ovunque sia necessario
■ Utilizzare il filtro delle route per pubblicizzare e ricevere le route in modo efficiente, in particolare in BGP.
■ Si consiglia di utilizzare il router-riflettore (RR) e la confederazione per ampliare la rete.
■ Di seguito sono riportate alcune considerazioni relative al progetto del riflettore di percorso:
■ La scalabilità dei percorsi aumenta in base al numero di client/non client.

■ Nei record di risorse gerarchici, utilizzare lo stesso ID cluster allo stesso livello (record di risorse ridondante) per la prevenzione dei loop e la scalabilità.
■ Controllare l'MTU nel percorso BGP o usare il protocollo PMTUD per regolare automaticamente il valore BGP MSS.
■ Usare i timer BFD o sintonizzati BGP per rilevare più rapidamente gli errori.
■ La scala BGP segue la configurazione e l'utilizzo degli scenari, e non esiste un'unica soluzione per tutte le esigenze. Devi avere una buona idea su:
■ scala del percorso
— scala del percorso (con una riconfigurazione soft, aumenta)
— scala attributo
■ Se il percorso aggiuntivo è configurato, consuma più memoria.
■ Comprensione delle politiche dei vicini BGP:
— pass-all (in particolare su un router di confine) può causare problemi in quanto la scala della memoria salta.
— Utilizzare costrutti di criteri che evitino corrispondenze di espressioni regolari in RPL.
■ Con l'NSR, l'RP in standby utilizza circa il 30% di memoria virtuale in più rispetto alla memoria attiva. Tenere presente questa considerazione in caso di standby.
■ Prestare attenzione alla continua variabilità in un numero significativo di percorsi (versioni di protuberanza). In questo modo la memoria per la generazione degli aggiornamenti rimane a un livello massimo.
■ Proteggere i peer con la manopola del prefisso max.
■ Usare i parametri di ritardo dell'hop successivo in base agli obiettivi di scala e convergenza.
■ Nel progetto di rete, cercare di evitare nuovi attributi. Gli attributi univoci determinano un imballaggio inefficiente e un numero maggiore di aggiornamenti BGP.
■ La configurazione dei percorsi multipli sulla rete può portare a loop di inoltro. Utilizzare con cautela.
■ Usare le policy delle tabelle per evitare l'installazione dei percorsi alla nervatura se RR non è inline-RR (no next-hop-self)

Monitoraggio della memoria di sistema per i processi di routing

Nessun dispositivo dispone di risorse infinite. Se a un dispositivo viene inviato un numero infinito di percorsi, il dispositivo deve scegliere la modalità di errore. I router tenteranno di servire tutte le route finché i limiti di memoria non saranno esauriti. Ciò potrebbe causare errori in tutti i protocolli e i processi di routing.

Per ogni processo nel router principale è definito un "RLIMIT". Il "RLIMIT" è la quantità di memoria di sistema che ogni processo può utilizzare.

In questa sezione vengono descritte alcune tecniche standard per monitorare e controllare la memoria di sistema utilizzata dal processo BGP.

Memoria di processo

Mostra la quantità di memoria utilizzata da un processo.

```
RP/0/RP0/CPU0:NCS-5501#show proc memory

Testo JID(KB) Dati(KB) Stack(KB) Processo dinamico(KB)

– – – –
```

```
1150 896 368300 136 33462 lspv_server
380 316 1877872 136 32775 parser_server
1084 2092 2425220 136 31703 bgp
1260 1056 1566272 160 31691 ipv4_rib
1262 1304 1161960 152 28962 ipv6_rib
1277 4276 1479984 136 21555 pim6
1301 80 227388 136 21372 schema_server
1276 4272 1677244 136 20743 pim
250 124 692436 136 20647 invmgr_proxy
1294 4540 2072976 136 20133 l2vpn_mgr
211 212 692476 136 19408 sdr_invmgr
1257 4 679752 136 17454 statsd_manager_g
```

A ogni processo viene allocata una quantità massima di memoria che può utilizzare. Questo è definito come il limite.

```
RP/0/RP0/CPU0:NCS-5501#show proc memory detail
Processo Shm-Tot Dynamic Dyn-Limit Stack di dati di testo JID
================================================================================
=====
1150 896K 359M 136K 32M 1024M 18M 24M lspv_server
1084 2M 2368M 136K 30M 7447M 43M 69M bgp
1260 1M 1529M 160K 30M 8192M 38M 52M ipv4_rib
380 316K 1833M 136K 29M 2048M 25M 94M parser_server
1262 1M 1134M 152K 28M 8192M 22M 31M ipv6_rib
1277 4M 1445M 136K 21M 1024M 18M 41M pim6
1301 80K 222M 136K 20M 300M 5M 33M schema_server
1276 4M 1637M 136K 20M 1024M 19M 41M pim
250 124K 676M 136K 20M 1024M 9M 31M invmgr_proxy
1294 4M 2024M 136K 19M 1861M 48M 66M l2vpn_mgr
211 212K 676M 136K 18M 300M 9M 29M sdr_invmgr
1257 4K 663M 136K 17M 2048M 20M 39M statsd_manager_g
288 4K 534M 136K 16M 2048M 15M 33M statsd_manager_l
...
```

Primi consumer di memoria

```
RP/0/RP0/CPU0:NCS-5501#show memory-top-consumer
################################################################################
############################################################
```

```
 Primi consumer di memoria su 0/0/CPU0 (a 2022/Apr/13/15:54:12)
##################################################################################
##################################################################
    Totale processi PID (MB) Heap (MB) Condiviso (MB)
   3469 fia_driver 826 492,82 321
   4091 fib_mgr 175 1094,43 155
   3456 spp 130 9,68 124
   4063 dpa_port_mapper 108 1,12 105
   3457 pacchetto 104 1,36 101
   5097 l2fib_mgr 86 52.01 71
   4147 bfd_agent 78 6,66 66
   4958 eth_intf_ea 66 4,76 61
   4131 optics_driver 62 141,23 22
   4090 ipv6_nd 55 4,13 49
##################################################################################
##################################################################
 Primi consumer di memoria su 0/RP0/CPU0 (a 20xx/MMM/HH:MM:SS)
##################################################################################
##################################################################
    Totale processi PID (MB) Heap (MB) Condiviso (MB)
   3581 spp 119 9,62 114
   4352 dpa_port_mapper 106 2,75 102
   4494 fib_mgr 99 7,71 90
   3582 pacchetto 96 1,48 94
   3684 parser_server 95 64.27 25
   8144 te_control 71 15,06 55
   8980 bgp 70 27,61 44
   7674 l2vpn_mgr 67 23,64 48
   8376 mibd_interface 65 35,28 28
   3608 gsp 65 15,75 48
```

Memoria totale - Utilizzata e disponibile

I componenti di sistema dispongono di una quantità fissa di memoria disponibile.

```
RP/0/RP0/CPU0:NCS-5501#show memory summary
nodo: node0_0_CPU0
—
 Memoria fisica: 8.192 M in totale (6.172 M disponibili)
```

```
 Memoria applicazione: 8192M (6172M disponibili)
 Immagine: 4 M (bootram: 0 M)
 Riservato: 0M, IOMem: 0M, flashfsys: 0M
 Totale finestre condivise: 226M
nodo: node0_RP0_CPU0
—
 Memoria fisica: 18.432 M totali (15.344 M disponibili)
 Memoria applicazione: 18432M (15344M disponibili)
 Immagine: 4 M (bootram: 0 M)
 Riservato: 0M, IOMem: 0M, flashfsys: 0M
 Totale finestre condivise: 181M
```

La finestra della memoria condivisa fornisce informazioni sulle allocazioni di memoria condivisa del sistema.

```
RP/0/RP0/CPU0:NCS-5501#show memory summary detail location 0/RP0/CPU0
nodo: node0_RP0_CPU0
—
 Memoria fisica: 18.432 M totali (15.344 M disponibili)
 Memoria applicazione: 18432M (15344M disponibili)
 Immagine: 4 M (bootram: 0 M)
 Riservato: 0M, IOMem: 0M, flashfsys: 0M
 Finestra condivisa soasync-app-1: 243.328K
 Finestra condivisa soasync-12: 3.328K
 ...
 Finestra condivisa rewrite-db: 272.164K
 Finestra condivisa l2fib_brg_shm: 139,758K
 Finestra condivisa im_rules: 384.211K
 Finestra condivisa grid_svr_shm: 44,272M
 Sponde condivise: 86,387 M
 Finestra condivisa im_db: 1,306 M
 Totale finestra condivisa: 180.969M
 Memoria allocata: 2,337 G
 Testo del programma: 127.993T
 Dati programma: 64.479G
 Stack di programmi: 2,034 G
RAM di sistema: 18432M ( 19327352832)
```

```
Totale utilizzato: 3088 M ( 3238002688)
 Utilizzato privato: 0M ( 0)
 Usato condiviso: 3088M ( 3238002688)
```

È possibile controllare i processi dei partecipanti con una finestra di memoria condivisa.

```
RP/0/RP0/CPU0:NCS-5501#sh shmwin spp elenco partecipanti
Dati per Window "spp":
—
Elenco dei partecipanti attuali:-
NOME INDICE JID PID
spp 3581 113 0
pacchetto 3582 345 1
ncd 4362 432 2
netio 4354 234  3
nsr_ping_reply 4371 291 4
aib 423 296 5
ipv6_io 4497 430 6
ipv4_io 4484 438
fib_mgr 4494 293 8
...
snmpd 8171 1002 44
ospf 8417 1030 45
mpls_ldp 7678 1292 46
bgp 8980 1084 47
cdp 9295 337 48
RP/0/RP0/CPU0:NCS-5501#sh shmwin soasync-1 elenco partecipanti
Dati per Window "soasync-1":
—
Elenco dei partecipanti attuali:-
NOME INDICE JID PID
tcp 5584 168 0
bgp 8980 1084
```

Monitoraggio delle risorse e watchdog

L'utilizzo della memoria viene monitorato tramite un watchdog di sistema in cXR e con Resmon in eXR.

```
RP/0/RP0/CPU0:NCS-5501#show watchdog memory-state
```

```
— node0_RP0_CPU0 —
Informazioni sulla memoria:
    Memoria fisica: 18432 MB
    Memoria libera: 1.5348 MB
    Stato memoria : Normale
RP/0/RP0/CPU0:NCS-5501#
RP/0/RP0/CPU0:NCS-5501#show watchdog threshold memory defaults location
0/RP0/CPU0
— node0_RP0_CPU0 —
 Soglie di memoria predefinite:
 Secondario: 1843 MB ß—10%
 Grave: 1474 MB ß—8%
 Critico: 921,599 MB ß—5%
Informazioni sulla memoria:
    Memoria fisica: 18432 MB
    Memoria libera: 15.340 MB
    Stato memoria : Normale
RP/0/RP0/CPU0:NCS-5501#
RP/0/RP0/CPU0:NCS-5501(config)#watchdog threshold memory minor ?
  <5-40> consumo di memoria in percentuale
```

Se le soglie vengono superate, viene visualizzato un avviso.

```
RP/0/RP0/CPU0:Feb 17 23:30:21.663 UTC: resmon[425]: %HA-HA_WD-4-MEMORY_ALARM :
Soglia di memoria superata: secondaria con 1840.000 MB di spazio libero. Stato
precedente: Normale
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USERS_INFO : I 5 principali consumer di memoria di sistema (1884160
Kbyte liberi):
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 0: Nome processo: bgp[0], pid: 7861, Utilizzo heap:
12207392 kbyte.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 1: Nome processo: ipv4_rib[0], pid: 4726, Utilizzo heap:
708784 kbyte.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 2: Nome processo: fib_mgr[0], pid: 3870, Utilizzo heap:
584072 kbyte.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 3: Nome processo: netconf[0], pid: 9260, Utilizzo heap:
553352 kbyte.
```

```
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 4: Nome processo: netio[0], pid: 3655, Uso heap: 253556
kbyte.

LC/0/3/CPU0:Mar 8 05:48:58.414 PST: resmon[172]: %HA-HA_WD-4-MEMORY_ALARM :
Soglia di memoria superata: grave con 600,182 MB disponibili. Stato precedente:
Normale

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USERS_WARNING : Primi 5 consumer di memoria di sistema (624654 Kbyte
liberi):

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 0: Nome processo: fib_mgr[0], pid: 5375, utilizzo heap
1014064 Kbyte.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 1: Nome processo: ipv4_mfwd_partner[0], pid: 5324,
utilizzo heap 185596 Kbyte.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 2: nome processo: nfsvr[0], pid: 8357, utilizzo heap
183692 Kbyte.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 3: Nome processo: fia_driver[0], pid: 3542, utilizzo
heap 177552 Kbyte.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 4: Nome processo: npu_driver[0], pid: 3525, utilizzo
heap 177156 Kbyte.
```

Alcuni processi possono eseguire azioni specifiche in base allo stato della memoria del watchdog. Ad esempio, BGP esegue le operazioni seguenti:

- in stato minore, BGP smette di far apparire nuovi peer
- in uno stato grave, BGP abbassa gradualmente alcuni peer.
- in uno stato critico, il processo BGP si arresta.

È possibile configurare i processi per la registrazione per le notifiche sullo stato della memoria.

Mostra processo di watchdog o consapevole

Gli utenti possono disattivare l'arresto automatico del processo a causa del timeout di watchdog.

watchdog restart memory-hog disable

Dove trovare ulteriori informazioni?

- Repository dei blog e dei white paper di Cisco IOS XR (xrdocs.io)
    - Core Fabric Design: https://xrdocs.io/design/blogs/latest-core-fabric-hld : In questo white paper vengono descritte le tendenze recenti e l'evoluzione delle reti backbone principali.
    - Peering Fabric Design: https://xrdocs.io/design/blogs/latest-peering-fabric-hld: questo white paper fornisce una panoramica completa delle sfide e consigli sulle

best practice per la progettazione peer con particolare attenzione alla semplificazione della rete.

■ Guida di riferimento alla configurazione: implementazione di BGP
https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/710x/b-bgp-cg-ncs5500-710x/implementing-bgp.html

Miglioramenti alle funzionalità

Isolamento dei limiti del sistema autonomo e controllo dell'adiacenza del router per gli overflow LSA	Introdotto nella versione 7.10.1 sui router a porta fissa NCS 5500: NCS 5700 fixed port router In una rete in cui si utilizza un ASBR (Autonomous System Boundary Router) e altri router, il flusso del traffico non viene interrotto anche se l'ASBR genera VLAN che superano il limite configurato. Ciò è possibile in quanto è possibile isolare le ASBR e controllare la durata dell'adiacenza nella fase EXCHANGE o LOADING. Isolando l'ASBR dai router adiacenti, la topologia di rete rimanente può continuare a funzionare senza interruzioni, evitando impatti negativi sul flusso del traffico. Questo approccio semplifica anche il processo di ripristino, in quanto l'intervento manuale è necessario solo per i router adiacenti ai router ASBR. Questa funzionalità introduce le seguenti modifiche: CLI: • max-external-lsa • exchange-timer Modello dati YANG: • Cisco-IOS-XR-ipv4-ospf-cfg.yang • Cisco-IOS-XR-ipv4-ospf-oper.yang • Cisco-IOS-XR-um-router-ospf-cfg.yang (vedere GitHub, YANG Data Models Navigator)
Ristabilire automaticamente una sessione BGP adiacente	Introdotto in questa release su: router a porta fissa NCS 5500; router a porta fissa NCS 5700; router modulari NCS 5500 (schede di linea NCS 5500; schede di linea NCS 5700 [Modalità: Compatibilità; Nativa]) È ora possibile configurare il router in modo che ristabilisca automaticamente una sessione BGP adiacente disabilitata a causa del superamento del limite del prefisso massimo. La funzione introduce queste modifiche: CLI • maximum-prefix-restart-time Modello dati YANG: • Nuovi XPath per openconfig-bgp-neighbor.yang(vedere GitHub, YANG Data Models Navigator)
BGP Flowspec su interfacce virtuali bridge-group	Introdotto nella release 7.10.1 su: NCS 5500 modular router (schede di linea NCS 5700 [Modalità: Nativa]) È ora possibile utilizzare BGP Flowspec su BVI (Bridge-Group Virtual

	Interface) per connettersi ai domini di broadcast che ospitano dispositivi host, come nel caso delle reti aziendali. Questo supporto consente ai clienti di proteggere le reti da minacce di rete quali attacchi Distributed Denial of Service (DDoS) in entrata tramite BVI.
Ignora messaggio di aggiornamento BGP in arrivo	Introdotto nella release 7.10.1 in data: NCS 5500 fixed port router; NCS 5700 fixed port router; NCS 5500 modular router (schede di linea NCS 5500; schede di linea NCS 5700 [Modalità: Compatibilità; Nativa]) È ora possibile evitare la reimpostazione della sessione quando una sessione BGP rileva degli errori durante l'analisi del messaggio di aggiornamento ricevuto. Questa operazione è possibile perché la funzione consente di scartare il messaggio di aggiornamento in arrivo come messaggio di ritiro. CLI: • aggiornamento nella gestione degli errori da considerare come ritirato Modello dati YANG: • Nuovi XPath per openconfig-bgp-neighbors.yang (vedere GitHub, YANG Data Models Navigator)
Esclusione dell'allocazione di etichette per route non annunciate	Introdotto nella release 7.10.1 in data: NCS 5500 fixed port router; NCS 5700 fixed port router; NCS 5500 modular router (schede di linea NCS 5500; schede di linea NCS 5700 [Modalità: Compatibilità; Nativa]) È stata migliorata la gestione dello spazio per le etichette e l'utilizzo delle risorse hardware rendendo più flessibile l'allocazione delle etichette MPLS. Questa flessibilità consente di assegnare queste etichette solo alle route annunciate alle relative route peer, garantendo una migliore gestione dello spazio delle etichette e un migliore utilizzo delle risorse hardware. Prima di questa release, l'allocazione delle etichette veniva eseguita indipendentemente dal fatto che le route fossero o meno pubblicizzate. Ne è conseguito un utilizzo inefficiente dello spazio delle etichette.
Protezione dei vicini EBGP con connessione diretta tramite identificatore LPTS basato sull'interfaccia	Introdotto nella release 7.10.1 in data: NCS 5500 fixed port router Abbiamo migliorato la sicurezza di rete per i vicini eBGP connessi direttamente garantendo che solo i pacchetti provenienti dai vicini eBGP designati possano attraversare una singola interfaccia, impedendo così lo spoofing IP. Ciò è possibile perché è stato aggiunto un identificatore di interfaccia per i servizi di trasporto pacchetti locali (LPTS, Local Packet Transport Services). LPTS filtra e regola i pacchetti in base al tipo di velocità di flusso configurato. La funzione introduce quanto segue: CLI: • bgp lpts-secure-binding Modello dati YANG:

	• Cisco-IOS-XR-um-router-bgp-cfg (vedere GitHub, YANG Data Models Navigator)
Riduzione delle ricorsioni per il peering eBGP sull'indirizzo di loopback sull'interfaccia virtuale Bridge-Group	Introdotto nella release 7.10.1 su: NCS 5500 modular router (schede di linea NCS 5700 [Modalità: Nativa]) È ora possibile ottenere il peering eBGP sulle interfacce loopback su BVI (Bridge-Group Virtual Interface) e ridurre il livello di ricorsione da tre a due. Questa riduzione del livello di ricorsione, ottenuta eliminando la necessità di utilizzare il nome BVI nella configurazione delle route statiche, consente l'inoltro dei pacchetti più rapido e un migliore utilizzo delle risorse di rete.
BGP Policy Accounting	Introdotto nella release 7.9.1: il protocollo BGP (Border Gateway Protocol) misura la contabilità e classifica il traffico IP ricevuto da diversi peer. È possibile identificare e contabilizzare tutto il traffico per cliente e fatturare di conseguenza. L'accounting dei criteri viene abilitato in base all'interfaccia di input individuale. Utilizzando l'accounting dei criteri BGP, è ora possibile registrare il traffico in base alla route attraversata. Questa funzione è ora supportata sui router che hanno schede di linea Cisco NC57 con eTCAM (External TCAM) e funzionano in modalità nativa. Questa funzionalità introduce le seguenti modifiche: • CLI: la funzione introduce il modalità stati bgppa fib hw-module • YANG Data Model: nuovi XPath per Cisco-IOS-XR-um-hw-module-profile-cfg.yang (vedere GitHub, YANG Data Models Navigator)
Rileva peer lento in un gruppo BGP	Introdotti nella release 7.9.1: i peer BGP elaborano i messaggi di aggiornamento BGP in arrivo a velocità diverse. Un peer lento è un peer che elabora i messaggi di aggiornamento BGP in arrivo molto lentamente per un lungo periodo di tempo rispetto ad altri peer nel sottogruppo di aggiornamento. La gestione lenta dei peer è importante quando le route cambiano costantemente in un lungo periodo di tempo. È importante eliminare le informazioni non aggiornate nella coda e inviare solo lo stato più recente. È utile sapere se esiste un peer lento, il che indica un problema di rete, ad esempio una congestione di rete prolungata o un ricevitore che non elabora gli aggiornamenti in tempo, che l'amministratore di rete può risolvere.
Limitazione dei numeri LSA in un database allo stato di	Introdotto nella release 7.9.1: gli annunci allo stato del collegamento (LSA) non generati automaticamente per un determinato processo OSPF (Open Shortest Path First) sono limitati a 500000. Questo

collegamento OSPF	meccanismo di protezione impedisce ai router di ricevere molte LSA, impedendo errori della CPU e carenze di memoria, ed è abilitato per impostazione predefinita da questa versione in poi. Se la rete contiene più di 500000 LSA, configurare il comando max-lsa con la scala LSA prevista prima di eseguire l'aggiornamento a questa versione o a una versione successiva. Questa funzione modifica i seguenti comandi: • show ospf per visualizzare il numero massimo di prefissi ridistribuiti. • show ospf database-summary detail per visualizzare il numero di conteggi LSA per router. • show ospf database-summary adv-routerrouter ID per visualizzare le informazioni sul router e le LSA ricevute da un particolare router.
Limitazione del numero massimo di prefissi LSA di tipo 3 ridistribuiti in OSPF	Introdotto nella release 7.9.1: per impostazione predefinita, il numero massimo di prefissi LSA Type-3 ridistribuiti per un determinato processo OSPF è ora limitato a 100000. Questo meccanismo impedisce che OSPF ridistribuisca un gran numero di prefissi come LSA di tipo 3 e quindi previene un elevato utilizzo della CPU e carenze di memoria. Quando il numero di prefissi ridistribuiti viene raggiunto o supera il valore di soglia, viene generato il messaggio di registro del sistema e non vengono ridistribuiti altri prefissi.

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).