Inhalt

HAFTUNGSAUSSCHLUSS

Dieses Dokument bietet eine allgemeine Zusammenfassung einiger bewährter Best Practices für das OSPF/IS-IS- und BGP-Routing. Diese Empfehlungen stellen kein von Cisco validiertes Design dar, und die Bereitstellung in einer

bestimmten Betriebsumgebung erfordert die erforderliche Sorgfalt und Aufmerksamkeit. Sie sollten zusammen mit den Konfigurationsleitfäden und der technischen Dokumentation für die entsprechenden Produkte gelesen werden, in denen detaillierter beschrieben wird, wie diese Best Practice-Empfehlungen implementiert werden können. Verweise in diesem Dokument auf Konfigurationsanleitungen und technische Dokumentation für bestimmte Produkte sind nur als Beispiele gedacht. Weitere Informationen finden Sie in den Konfigurationsanleitungen und der technischen Dokumentation für Ihre jeweiligen Produkte.

Einleitung

In diesem Dokument werden bewährte Verfahren und Empfehlungen für den Aufbau vereinfachter, effizienter und skalierbarer Netzwerke auf Basis von IOS XR-Routing-Plattformen beschrieben. Der Schwerpunkt dieses Dokuments liegt auf spezifischen Implementierungstechniken und den in IOS XR verfügbaren Optionen zur Unterstützung der Anpassung von OSPF/IS-IS- und BGP-Bereitstellungen.

Implementierung von OSPF

Das in RFC 2328 definierte OSPF-Protokoll ist ein IGP, das zur Verteilung von Routing-Informationen innerhalb eines einzelnen autonomen Systems verwendet wird. OSPF bietet im Vergleich zu anderen Protokollen eine Reihe von Vorteilen, jedoch ist ein geeignetes Design erforderlich, um ein skalierbares und fehlertolerantes Netzwerk zu schaffen.

Weitere Informationen zu OSPF finden Sie unter:

- TechNote zu OSPF: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#anc13
- Konfigurationsleitfaden für 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
- Befehlsreferenz: 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

Schlüsselkonzepte

- Hierarchie: Ein hierarchisches Netzwerkmodell ist ein nützliches High-Level-Tool für die Entwicklung einer zuverlässigen Netzwerkinfrastruktur und trägt dazu bei, komplexe Probleme beim Netzwerkdesign in kleinere und besser verwaltbare Bereiche zu zerlegen.
- Modularität: Durch die Aufteilung der verschiedenen Funktionen in einem Netzwerk in Module wird das Netzwerkdesign vereinfacht. Cisco hat mehrere Module identifiziert, darunter den Campus der Enterprise-Klasse, die Services-Bausteine, das Rechenzentrum und das Internet-Edge.
- Ausfallsicherheit: Das Netzwerk ist sowohl unter normalen als auch unter anomalen Bedingungen verfügbar. Zu den normalen Bedingungen gehören erwartete Datenverkehrsflüsse, Muster und geplante Ereignisse wie Wartungsfenster. Zu den ungewöhnlichen Umständen gehören Hardware- oder Softwarefehler, extreme

Datenverkehrslasten, ungewöhnliche Datenverkehrsmuster, Denial-of-Service (DoS)-Ereignisse und andere geplante oder ungeplante Ereignisse.

- Flexibilität: Die Möglichkeit, Teile des Netzwerks zu verändern, neue Services hinzuzufügen oder die Kapazität zu erhöhen, ohne umfangreiche Upgrades (d. h. den Austausch wichtiger Hardware-Geräte) durchzuführen.

Als allgemeine Best Practice sollte bei der Netzwerkbereitstellung die "Spanne" des Netzwerks berücksichtigt werden, um die Routen innerhalb einer bestimmten Grenze sowie die Routen einzuschließen, die für die Weiterleitung durch die Router innerhalb einer Domäne relevant und erforderlich sind. Die effektive Nutzung von OSPF-Bereichen trägt dazu bei, die Anzahl der LSAs (Link-State Advertisements) und des sonstigen Overhead-Datenverkehrs, der über das Netzwerk gesendet wird, zu reduzieren. Einer der Vorteile einer Hierarchie besteht darin, dass mit diesem Ansatz sichergestellt wird, dass die Größe der Topologiedatenbank, die die einzelnen Router verwalten müssen, verwaltbar ist und dem Speicherprofil des Routers entspricht.

OSPF-Domänen- und BGP-Neuverteilung

OSPF ist für die Übertragung von nur wenigen tausend Routen konzipiert. Auf hoher Ebene sind OSPF-"Bereiche" Abschnitte eines Netzwerks, in denen jeder Router die Routing-Funktionen jedes anderen Routers in der Region kennt. Dies ermöglicht eine schnelle Konvergenz bei Geräteproblemen, jedoch auf Kosten einer reduzierten Skalierbarkeit. Daher wird OSPF in einem Service Provider-Core verwendet, um die Basisverbindungen zwischen allen Core-Geräten bereitzustellen, und alle Core-Geräte werden in derselben OSPF-Area konfiguriert. Dies ist ein Standarddesign für "Underlay"-Netzwerk

Im Gegensatz dazu ist BGP für wesentlich mehr Routen ausgelegt als die meisten IGPs, z. B. OSPF. Risiken im Zusammenhang mit der Neuverteilung von BGP-Routen in einem IGP wie OSPF. Wenn ein Service Provider für einen Anwendungsfall die Umverteilung von BGP-Routen in die IGP-Domäne erfordert, muss dies vom Service Provider mit angemessener Filterung bei den autonomen System Boundary Routern (ASBRs) und mit konfiguriertem Überlastungsschutz auf dem empfangenden Router verwaltet werden. Wenn die BGP-Neuverteilung nicht in einen OSPF eingefiltert wird, empfängt jedes OSPF-Gerät im ASBR Routen, die seine Kapazität zur gleichzeitigen Verarbeitung weit übersteigen. Beispielsweise ermöglichen es Cisco IOS XR-Router nur 10.000 BGP-Routen, standardmäßig in OSPF umverteilt zu werden. Wenn BGP-Routen in das IGP umverteilt werden, ist es möglich, dass alle Router in der IGP-Domäne diese Routen empfangen, je nach IGP-Design. Gemäß OSPF-Protokoll RFC muss jede externe Route, die zu OSPF umverteilt wird, auf alle Router im OSPF-Bereich verteilt werden.

Verwaltung der Umverteilung in IGP

Als allgemeine Best Practice sollte die Umverteilung nur dann sorgfältig und geplant erfolgen, wenn es keine anderen Optionen gibt, die von einer Umverteilungsfunktion bereitgestellten Routen für die Erreichbarkeit zu erlernen.

In der Regel sollten Sie:

- Vermeidung von Umverteilung
- Vermeiden von Routen in einer IGP-Domäne
- BGP für externe Erreichbarkeit implementieren

- Verwendung von IGP zur ausschließlichen Übertragung von Next-Hop-Informationen, z. B. Loopback 0

Einschränkungen der OSPF-Routen-Neuverteilung

Die Skalierung der vom BGP in OSPF umverteilten Präfixe wird mit der Konfiguration des Überlastungsschutzes (max-lsa) verwaltet. Dies ist der einzige Schutz vor dem Durchsickern einer großen Anzahl von Routen in die OSPF-Domäne. Bei einer Neuverteilung in einem einzigen OSPF-Bereich sollten Sie mehrere Schutzebenen gegen eine Routen-Neuverteilung implementieren.

Folgende Optionen sind zum Schutz vor Routen-Neuverteilung verfügbar:

- Umverteilungsfilterung mit ACL
- Neuverteilungslimit - globale Einstellung, um zu verhindern, dass mehr als eine bestimmte Anzahl von Routen neu verteilt wird. Wenn der Filter entfernt wird, stellt das globale Neuverteilungslimit die zweite Verteidigungslinie dar und schützt die Kerne.
- Max-LSA-Konfigurationen auf allen Geräten im OSPF-Bereich - Wenn die in den obigen Aufzählungszeichen erwähnten Schutzmaßnahmen fehlschlagen, zwingen Sie die empfangenden Router, die eingehenden übermäßigen LSAs abzulehnen.

Schutz vor Überlastung der OSPF-Link-State-Datenbank

Die OSPF-Funktion zum Schutz vor Link-State-Datenbanküberlastung bietet einen Mechanismus auf OSPF-Ebene, um die Anzahl der nicht selbst generierten LSAs für einen bestimmten OSPF-Prozess zu begrenzen. Wenn andere Router im Netzwerk falsch konfiguriert wurden, können sie eine große Anzahl von LSAs generieren, um beispielsweise eine große Anzahl von Präfixen in OSPF umzuverteilen. Dieser Schutzmechanismus verhindert, dass Router viele LSAs empfangen und somit CPU- und Speicherengpässe auftreten.

Verhalten von Funktionen

So verhält sich die Funktion:

- Wenn diese Funktion aktiviert ist, zählt der Router die Anzahl aller empfangenen (nicht selbst generierten) LSAs.
- Wenn der konfigurierte Schwellenwert erreicht ist, wird eine Fehlermeldung protokolliert.
- Wenn die konfigurierte maximale Anzahl empfangener LSAs überschritten wird, akzeptiert der Router keine neuen LSAs mehr.

```
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>
```

OSPF-Status

Wenn die Anzahl der empfangenen LSAs nach einer Minute die konfigurierte maximale Anzahl übersteigt, werden durch den OSPF-Prozess alle Adjacencies deaktiviert und die OSPF-Datenbank gelöscht. Dieser Zustand wird als

Ignorierzustand bezeichnet. In diesem Zustand werden alle OSPF-Pakete, die auf allen zur OSPF-Instanz gehörenden Schnittstellen empfangen werden, ignoriert, und es werden keine OSPF-Pakete auf den Schnittstellen generiert. Der OSPF-Prozess bleibt für die Dauer der konfigurierten Ignorierzeit im Ignorierstatus (Standardwert: 5 Minuten). Wenn die Ignorierzeit abläuft, kehrt der OSPF-Prozess zum normalen Betrieb zurück und erstellt Adjacencies auf allen zugehörigen Schnittstellen.

Wenn die LSA-Anzahl die maximale Anzahl überschreitet, sobald die OSPF-Instanz aus dem Ignorieren-Zustand zurückkehrt, kann die OSPF-Instanz endlos zwischen ihrem normalen und dem Ignorieren-Zustand hin- und herpendeln. Um diese unendliche Oszillation zu verhindern, zählt die OSPF-Instanz, wie oft sie sich im Ignorierzustand befunden hat. Dieser Leistungsindikator wird als "ignore-count" (Ignoranzähler) bezeichnet. Wenn der Ignoranzähler (der Standardwert für "ignore-count" ist 5) den konfigurierten Wert überschreitet, bleibt die OSPF-Instanz dauerhaft im Ignoranzstatus.

Sie müssen den Befehl clear ospf eingeben, um den normalen Status der OSPF-Instanz wiederherzustellen. Der Ignore-Count wird auf Null zurückgesetzt, wenn der LSA-Count die maximale Anzahl während der durch das Reset-Time-Schlüsselwort konfigurierten Zeit nicht erneut überschreitet.

Wenn Sie das Schlüsselwort warning-only verwenden, wechselt die OSPF-Instanz niemals in den Ignore-Status. Wenn die Anzahl der LSAs die maximale Anzahl überschreitet, protokolliert der OSPF-Prozess eine Fehlermeldung, und die OSPF-Instanz wird im normalen Betrieb fortgesetzt.

Es gibt keinen Standardwert für max-lsa. Der Grenzwert wird nur überprüft, wenn er speziell konfiguriert wurde.

Nach der Konfiguration von max-lsa können andere Parameter Standardwerte aufweisen:

- Standard %-threshold-to-log-warning - 75 %
- default ignore-count-value - 5
- Standard-Ignorierzeit in Minuten: 5 Minuten
- default time-to-reset-ignore-count - 10 Minuten

Das folgende Beispiel zeigt die Implementierung, die die OSPF-Instanz so konfiguriert, dass 12000 nicht selbst generierte LSAs und 1000 nicht selbst generierte LSAs in VRF V1 akzeptiert werden.

```
RP/0/RSP0/CPU0:Router# konfigurieren
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
```

Das folgende Beispiel zeigt, wie der aktuelle Status der OSPF-Instanz angezeigt wird.

```
RP/0/RSP0/CPU0:Router# show ospf 0
    Routing-Prozess "ospf 0" mit ID 10.0.0.2
    NSR (Nonstop Routing) ist deaktiviert.
    Unterstützt nur einzelne TOS(TOS0)-Routen
    Unterstützt opakes LSA
    Er ist ein Area Border Router.
    Maximale Anzahl nicht selbst generierter LSA zulässig: 12000
       Aktuelle Anzahl nicht selbst generierter LSA 1
       Schwellenwert für Warnmeldung 75 %
       Ignorierzeit 5 Minuten, Reset-Zeit 10 Minuten
       Ignore-count allowed 5, current ignore-count 0
```

Implementierung von BGP

BGP-Adressfamilien machen das BGP zu einem "Multiprotokoll"-Routing-Protokoll. Es wird dringend empfohlen, dass Sie wissen, wie die Adressfamilien verwendet werden, um skalierbare Topologien zu erstellen, die einfach zu implementieren und zu verwalten sind. Mithilfe von Adressfamilien kann der Operator verschiedene Topologien für verschiedene Technologien erstellen, z. B. EVPN, Multicast usw.

Weitere Informationen zum BGP finden Sie im BGP-Konfigurationsleitfaden: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html

BGP und BFD

Die BGP-Konvergenz in einem Service Provider-Netzwerk ist wichtig, um die Kundenerwartungen hinsichtlich des Aufbaus ausfallsicherer und fehlertoleranter Netzwerke zu erfüllen. Standardmäßig hat BGP einen Keepalive-Timer von 60 Sekunden und einen Hold-Timer von 180 Sekunden. Dies bedeutet, dass BGP nur sehr langsam konvergiert, wenn es keine Unterstützung durch unterstützende Protokolle gibt. BFD Bi-directional Forwarding (BFD) ist ein Protokoll dieser Art, das die schnellere Konvergenz von Client-Protokollen unterstützt. Mit BFD können Protokolle innerhalb von Sekunden konvergiert werden.

Zusätzliche Informationen

- Dieser Leitfaden enthält Konzeptions- und Konfigurationsinformationen für BFD: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/76x/b-routing-cg-ncs5500-76x/implementing-bfd.html
- Dieses Whitepaper bietet eine anbieterorientierte Ansicht zur schnellen Konvergenz mit BFD auf den Cisco NCS 5500- und Cisco Network Convergence System 500-Routern: https://xrdocs.io/ncs5500/tutorials/bfd-architecture-on-ncs5500-and-ncs500/
- Weitere Informationen zur Verwendung von BFD an Paketschnittstellen und zur Implementierung von Multipath und MultiHop BFD finden Sie im https://xrdocs.io/ Repository.

BGP Langsame Peer-Erkennung

Ein langsamer Peer ist ein Peer, der nicht mit der Geschwindigkeit Schritt halten kann, mit der der Router über einen längeren Zeitraum (in der Größenordnung von Minuten) Update-Nachrichten in einer Update-Gruppe generiert. Wenn in einer Aktualisierungsgruppe ein langsamer Peer vorhanden ist, erhöht sich die Anzahl der formatierten Updates, für die eine Übertragung aussteht. Wenn die Cachegrenze erreicht ist, verfügt die Gruppe nicht über weitere Kontingente zum Formatieren neuer Nachrichten. Damit eine neue Nachricht formatiert werden kann, müssen einige vorhandene Nachrichten über den langsamen Peer übertragen und dann aus dem Cache entfernt werden. Die übrigen Mitglieder der Gruppe, die schneller als der langsame Peer sind und die Übertragung der formatierten Nachrichten abgeschlossen haben, haben nichts Neues zu senden, obwohl es möglicherweise neu modifizierte BGP-Netzwerke gibt, die darauf

warten, angekündigt oder entfernt zu werden. Dieser Effekt des Blockierens der Formatierung aller Peers in einer Gruppe, wenn einer der Peers Updates nur langsam verarbeitet, ist das "Slow-Peer"-Problem.

Ereignisse, die eine erhebliche Schwankung in der BGP-Tabelle verursachen (wie z. B. das Zurücksetzen der Verbindung), können einen kurzen Anstieg der Aktualisierungsgenerierung verursachen. Ein Peer, der bei solchen Ereignissen vorübergehend zurückfällt, sich aber nach dem Ereignis schnell wieder erholt, wird nicht als langsamer Peer betrachtet. Damit ein Peer als langsam gekennzeichnet wird, muss er nicht in der Lage sein, über einen längeren Zeitraum (in der Größenordnung von wenigen Minuten) mit der durchschnittlichen Geschwindigkeit der generierten Updates Schritt zu halten.

Der langsame BGP-Peer kann folgende Ursachen haben:

- Paketverlust oder starker Datenverkehr auf der Verbindung zum Peer.
- Ein BGP-Peer könnte eine hohe CPU-Belastung aufweisen und kann daher die TCP-Verbindung nicht mit der erforderlichen Geschwindigkeit versorgen.
- In diesem Fall müssen die Plattform-Hardware-Fähigkeit und die angebotene Last überprüft werden.
- Durchsatzprobleme mit der BGP-Verbindung
- Weitere Informationen zur BGP Slow Peer-Erkennung finden Sie unter: 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

Nachfolgend finden Sie einige Eindämmungen und Best Practices für das Management langsamer Peers:

- End-to-End-QoS zur Bandbreitenreservierung für BGP-Kontrollebenen-Datenverkehr bei Überlastung.
- Verwendung korrekter und geeigneter MSS-/MTU-Werte mithilfe der BGP PMTUD- und/oder TCP MSS-Einstellungen.
- Verwenden Sie die richtige Hardware und minimieren Sie die Anzahl der Routen in Bezug auf die Hardware.

Slow-Peer-Erkennung ist in Cisco IOS XR ab Version 7.1.2 standardmäßig aktiviert. Langsame Peers sind Peers, die eingehende BGP-Updates nur langsam empfangen und verarbeiten und die Updates dem Absender bestätigen. Wenn der langsame Peer zur gleichen Aktualisierungsgruppe wie andere Peers gehört, kann dies den Aktualisierungsvorgang für alle Peers verlangsamen. Wenn IOS XR in dieser Version einen langsamen Peer erkennt, erstellt es ein Syslog mit den Details zum jeweiligen Peer.

Schnelle Konvergenz durch unabhängige BGP-Präfixkonvergenz

Bei BGP-Präfixen wird eine schnelle Konvergenz mithilfe von BGP Prefix Independent Convergence (PIC) erreicht, bei der BGP einen alternativen besten und primären besten Pfad berechnet und beide Pfade in der Routing-Tabelle als primäre und Backup-Pfade installiert.

Wenn die Remote-Verbindung zum nächsten BGP-Hop nicht mehr erreichbar ist, schaltet das BGP sofort mithilfe von BGP PIC auf den alternativen Pfad um, anstatt den Pfad nach dem Ausfall neu zu berechnen.

Wenn der BGP Next-Hop Remote-PE aktiv ist, aber ein Pfadfehler vorliegt, verarbeitet IGP TI-LFA FRR eine schnelle Rekonvergenz zum alternativen Pfad, und BGP aktualisiert den IGP Next-Hop für den Remote-PE.

BGP PIC wird unter der VRF-Adressfamilie konfiguriert, um die schnelle Konvergenz von VPN-Präfixen zu ermöglichen, wenn ein Remote-PE nicht mehr erreichbar ist.

Weitere Informationen zur unabhängigen BGP-Präfix-Konvergenz finden Sie unter:
https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/bgp-pic.html

BGP-Sicherheit mit BGP Flowspec

BGP Flowspec, kurz gesagt, ist eine Funktion, die es Ihnen ermöglicht, IPv4/IPv6-Spezifikationen für den Datenverkehrsfluss (Quelle X, Ziel Y, Protokoll UDP, Quellport A usw.) und Aktionen zu empfangen, die für diesen Datenverkehr (wie Drop, Policing oder Redirect) über BGP-Updates durchgeführt werden müssen.
Innerhalb des BGP-Updates werden die Kriterien für den Datenverkehrsabgleich durch BGP NLG dargestellt. Die erweiterten Communitys von RI und BGP repräsentieren diese Aktionen.

Diese Funktion basiert auf RFC 5575 und kann zur Eindämmung von DDoS-Angriffen verwendet werden. Wenn ein bestimmter Host innerhalb eines Netzwerks angegriffen wird, können wir ein Flowspec-Update an Edge-Router senden, sodass der Angriffsverkehr kontrolliert oder verworfen oder sogar an einen anderen Standort umgeleitet werden kann, z. B. an eine Appliance, die den Verkehr bereinigen kann (filtern Sie den "schädlichen" Verkehr heraus und leiten Sie nur den "guten" Verkehr an den betroffenen Host weiter).

Sobald die Flussangaben von einem Router empfangen und in die entsprechenden Linecards programmiert wurden, verarbeiten alle aktiven L3-Ports auf diesen Linecards den eingehenden Datenverkehr gemäß den FlowSpec-Regeln.

Weitere Informationen zur Implementierung von BGP FlowSpec finden Sie unter:

- Whitepaper mit Links zum Cisco IOS XR Youtube-Kanal: https://xrdocs.io/ncs5500/tutorials/bgp-flowspec-on-ncs5500/
- BGP-Konfigurationsleitfaden: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html#concept_ugv_bxq_h2b

Best Practices und Empfehlungen

Die folgende Liste bietet einen Überblick über die allgemeinen Best Practices und Empfehlungen, die in keiner bestimmten Reihenfolge aufgeführt sind:

- Netzwerküberprüfung für den allgemeinen Systemzustand. Beginnen Sie mit einem Konfigurations-Audit, und wechseln Sie sequenziell von Schnittstellenkonfigurationen zu Routing und Services.
- eine Überwachungsstrategie verfolgen. SNMP ist zwar gängige Praxis, sollte jedoch die Bereitstellung zuverlässigerer und aussagekräftigerer Techniken mithilfe von Streaming-Telemetrie in Betracht ziehen. Im folgenden Whitepaper finden Sie Empfehlungen zu Best Practices für die Implementierung von Telemetrie auf einem IOS XR-Router: https://xrdocs.io/telemetry/

OSPF

Nachfolgend finden Sie allgemeine Best Practices und Empfehlungen für OSPF:

- Implementierung einer Routenzusammenfassung für Intra-Area-Routen für OSPF.
- Konfigurieren Sie die Router-ID explizit in OSPF als eine der OSPF-aktivierten Loopback-Adressen.
- Entwerfen Sie ein hierarchisches Netzwerk, um die LSAs in einem Bereich für OSPF zu begrenzen. Halten Sie die Anzahl der ABRs für einen Bereich in einem angemessenen Bereich (~3 bis 4).
- Implementieren Sie die OSPF-Konfiguration "max-lsa" für OSPF oder eine entsprechende Konfiguration, um die LSAs in der Datenbank auf eine effektive Nutzung des Systemspeichers zu beschränken.
- Begrenzen Sie die maximale Anzahl von Routen, die vom BGP an OSPF verteilt werden können. In IOS-XR ist der Standardwert 10 KB.
- Verwenden Sie die Routenrichtlinie (RPL), um die Routen in OSPF umzuverteilen.
- Geben Sie ggf. eine Zusammenfassung der Route zwischen den Bereichen und der externen Route vom Typ 5.
- Verwendung der Authentifizierung bei Bedarf.
- Verwenden Sie immer NSF und NSR.
- Konfigurieren Sie die Umverteilungsfilterung an der Quelle statt am Ziel.
- Verwenden Sie ggf. eine passive Schnittstelle.
- OSPF sollte nur Loopback- und Router-Interface-Routen übertragen und somit alle anderen BGP-zu-OSPF-Weiterverteilungen entfernen.
- Ziehen Sie in Betracht, jeden primären Hub in einen eigenen Bereich (NSSA) zu verlagern.
- Schnellere Fehlererkennung im Vergleich zu aggressiven Routing-Protokoll-Timern mit BFD
- Verwenden Sie den Befehl mtu-ignore nicht so oft wie möglich.
- Ziehen Sie eine IGP-LDP-Synchronisierung in einer MPLS-Umgebung in Betracht, um das Senden von Datenverkehr über einen nicht gekennzeichneten Pfad zu vermeiden.
- Berücksichtigen Sie die Skalierbarkeit innerhalb der unterstützten Plattformgrenzen (Anzahl der Präfixe, Anzahl der Labels, ECMP, Anzahl der Bereiche usw.).
- Vermeiden Sie eine gegenseitige Umverteilung an mehreren Stellen.
- Konfigurieren Sie die administrative Distanz so, dass jedes native Präfix für jedes Protokoll oder jeden Prozess über das Protokoll oder den Prozess der entsprechenden Domäne erreicht wird.
- Steuern Sie die Präfixe (mithilfe der Entfernung oder der Kombination aus Präfixliste), sodass dasselbe Präfix nicht an die Ursprungsdomäne zurückgegeben wird.
- Obwohl die OSPF-Prozess-ID für den Router lokal von Bedeutung ist, wird empfohlen, für alle Router in derselben OSPF-Domäne dieselbe Prozess-ID zu verwenden. Dies verbessert die Konsistenz der Konfiguration und vereinfacht automatische Konfigurationsaufgaben.

- Wenn Sie OSPF für Hub-and-Spoke-Umgebungen konfigurieren, sollten Sie die OSPF-Bereiche mit einer geringeren Anzahl an Routern ausstatten.
- Konfigurieren Sie die OSPF-Referenzbandbreite für automatische Kosten in der gesamten OSPF-Domäne für die Verbindung mit der höchsten Bandbreite im Netzwerk.
- Aus Designsicht empfehlen wir die Implementierung von IGP-Peering mit Domänen unter denselben administrativen oder betrieblichen Kontrollen, um zu verhindern, dass sich ungeplante oder unberechtigte IGP-Updates im Netzwerk verbreiten. Dies sollte eine bessere Wartbarkeit und eine einfachere Fehlerbehebung im Falle von Fehlern ermöglichen. Falls eine große IGP-Domäne eine geschäftliche Notwendigkeit darstellt, planen Sie in diesen Fällen die Verwendung von BGP, um die Anzahl der Routen in der IGP-Netzwerkdomäne zu begrenzen.
- Wenn Sie eine End-to-End-MPLS-Konnektivität benötigen, setzen Sie die Hierarchie/Segmentierung fort, und verwenden Sie Optionen wie RFC3107 BGP-LU oder Inter-Domain Path Computation via PCE, oder wählen Sie Umverteilung/Leaking mit der Richtlinie als letztes Mittel.
- Die OSPF Shortest Path First Throttling-Funktion kann verwendet werden, um die SPF-Planung in Millisekundenintervallen zu konfigurieren und die SPF-Berechnungen während einer Netzwerkinstabilität zu verzögern.
- Die Funktion zur Priorisierung von OSPF-SPF-Präfixen ermöglicht es Administratoren, wichtige Präfixe bei der Routeninstallation schneller zu konvergieren.

IS-IS

Hier finden Sie allgemeine Best Practices und Empfehlungen für IS-IS:

- Wenn Sie ein flaches einstufiges Netzwerk betreiben, denken Sie an die Größe. Konfigurieren Sie alle Router nur als L2. Standardmäßig ist der Router L1-L2, und das Versickern von Routing-Informationen von L1 nach L2 ist standardmäßig aktiviert. Dies könnte dazu führen, dass alle Router L1-Routen an L2 weiterleiten und die Link-State-Datenbank aufblähen.
- Wenn Sie ein mehrstufiges Netzwerk (mehrere Bereiche) betreiben, stellen Sie sicher, dass die Layer-3-Topologie der ISIS-Hierarchie folgt. Erstellen Sie keine Backdoor-Verbindungen zwischen L1-Bereichen.
- Wenn Sie ein mehrstufiges Netzwerk (mit mehreren Bereichen) betreiben, stellen Sie sicher, dass die L1- und L2-Router über die L1- und L2-Bereiche verbunden sind. Hierfür sind keine mehrfachen physischen oder virtuellen Verbindungen zwischen den Routern erforderlich. Die Verbindung zwischen den L1- und L2-Routern muss als L1/L2-Schaltung ausgeführt werden.
- Wenn Sie ein mehrstufiges Netzwerk (mehrere Bereiche) betreiben, fassen Sie zusammen, was zusammengefasst werden kann. Im Fall von MPLS muss beispielsweise das Loopback von PE-Routern zwischen den Bereichen verteilt werden, Infrastruktur-Link-Adressen hingegen nicht.
- Erstellen und befolgen Sie nach Möglichkeit den richtigen Adressierungsplan. Dies ermöglicht eine Zusammenfassung und Skalierung.
- Stellen Sie die LSP-Lebensdauer auf maximal 18 Stunden ein.
- Vermeiden Sie jegliche Umverteilung. Die Neuverteilung ist komplex und muss manuell verwaltet werden, um Routingschleifen zu vermeiden. Verwenden Sie wenn möglich ein Mehrbereichs-/Ebenendesign.

- Wenn Sie die Umverteilung verwenden müssen, verwenden Sie während der Umverteilung das Routen-Tagging und die "distribute-list in"-Filterung auf Basis von Tags, um diese zu verwalten. Fassen Sie diese während der Neuverteilung nach Möglichkeit zusammen.
- Konfigurieren Sie die Schnittstellen so weit wie möglich als "Punkt-zu-Punkt". Dies verbessert die Leistung und Skalierbarkeit des Protokolls.
- Verwenden Sie ISIS nicht in stark vernetzter Topologie. Link-State-Protokolle verhalten sich in stark vernetzten Umgebungen schlecht.
- Konfigurieren Sie eine hohe Standardmetrik im ISIS-Untermodus address-family. Dadurch wird verhindert, dass neu hinzugefügte Links Datenverkehr anziehen, wenn sie versehentlich ohne eine Metrik konfiguriert werden.
- Konfigurieren Sie "log adjacency changes" (Adjacency-Protokoll-Änderungen), um die Behebung von Verbindungsproblemen zu unterstützen.
- Verwenden Sie "metric-style wide" im Untermodus "ipv4" der ISIS-Adressfamilie. Enge Metriken sind nicht sehr nützlich und unterstützen keine Funktionen wie Segment-Routing oder Flex-Algo.
- Wenn Sie SR-MPLS TI-LFA verwenden, denken Sie daran, der Konfiguration "ipv4 unnumbered mpls traffic-eng Loopback0" hinzuzufügen, damit ISIS bei Bedarf TE-Tunnel zuweisen kann.
- Lassen Sie die Konfigurationen "lsp-gen-interval" und "spf-interval" als Standardeinstellungen unverändert, es sei denn, Sie sind sich sicher, dass eine schnellere native Konvergenz erforderlich ist. Bei TI-LFA ist native Konvergenz nicht so wichtig, da Fast-Reroute einzelne Topologieänderungen in maximal 50 ms verarbeiten kann.
- Wenn Sie "lsp-gen-interval" oder "spf-interval" ändern, verwenden Sie keine anfängliche Verzögerung, die kürzer als 50 ms ist.
- In den meisten Fällen ist "set-overload-bit" die bessere Wahl als "max-metric", da es sich um eine atomare Änderung handelt, die von Fast-Reroute unterstützt wird.
- Verwenden Sie die kryptografische Authentifizierung für Hellos (hello-password) und LSPs (lsp-password). Schlüsselanhänger bieten die größte Flexibilität und können trefferlose Schlüsselüberläufe unterstützen.
- Konfigurieren Sie "nsf cisco" für die trefferlose Authentifizierung von ISIS-Prozessneustarts und der SMU-Installation. Trotz des Namens bietet diese Lösung eine bessere Interoperabilität mit anderen Anbietern als "nsf ietf".
- Konfigurieren Sie auf einer Plattform mit zwei RPs AUCH "nsr" für RP-Switchovers.
- Verwenden Sie die Vorlagen "group" und "apply-group", um wiederholte Konfigurationsabschnitte zu konfigurieren. Dies ist weniger fehleranfällig und lässt sich bei Bedarf leichter ändern.
- Überlegen Sie sich in einem mehrstufigen Netzwerk sorgfältig, ob Sie "propagieren" müssen, um Präfixe von Stufe 2 auf Stufe 1 durchzulassen. Dies kann die Skalierbarkeit einschränken, und oft reicht die durch das Attached-Bit bereitgestellte Standard-Route der Stufe 1 aus.
- Wenn Sie mehrere ISIS-Instanzen in derselben VRF-Instanz verwenden, sollten Sie für diese eindeutige "Distanzwerte" konfigurieren. Dadurch wird die Routeninstallation in der RIB deterministischer, wenn jede über eine Route mit demselben Präfix verfügt.
- Verwenden Sie BFD für die schnelle Erkennung von Verbindungsausfällen. Wenn BFD diese Funktion bereitstellt, kann das IS-IS-Hello-Intervall sicher vergrößert werden, um die Skalierbarkeit zu verbessern.

BGP

Nachfolgend finden Sie allgemeine Best Practices und Empfehlungen für das BGP:

- Verwenden Sie NSR und NSF/Graceful Restart mit sorgfältig abgestimmten Timern, abhängig von der erwarteten Größe.
- Konfigurieren Sie das BGP mithilfe der stets verfügbaren Loopback-Schnittstelle, nicht der physischen Schnittstelle für IBGP-Peering.
- Verteilen Sie keine BGP-Routen (mit hohem Volumen) ohne ordnungsgemäße RPL in IGP (mit vergleichsweise geringem Volumen) und umgekehrt. So wird die Anzahl der vom BGP neu verteilten Routen auf ein IGP (OSPF/ISIS) beschränkt.
- Eine Umverteilung von BGP zu IGP ohne eine ordnungsgemäße, gründlich getestete Richtlinie (ACL) kann dazu führen, dass die Ressourcen (der Arbeitsspeicher) des Routers erschöpft sind.
- Verwendung von zusammengefassten Routen im BGP, um die Größe der Routing-Tabelle und die Speichernutzung zu verringern. Aggregieren Sie Routen mit rein zusammengefassten Routen, wo immer dies sinnvoll ist.
- Routenfilterung zur effizienten Bereitstellung und Entgegennahme von Routen, insbesondere im BGP
- Wir empfehlen die Verwendung von Route-Reflector (RR) und Confederation, um das Netzwerk zu skalieren.
- Das Design des Routen-Reflektors muss u. a. folgende Aspekte berücksichtigen:
- Die Pfadskalierung wird basierend auf der Anzahl der Clients/Nicht-Clients erhöht.
- Verwenden Sie in hierarchischen RRs dieselbe Cluster-ID auf derselben Ebene (redundante RR), um Schleifen zu verhindern und die Skalierung zu ermöglichen.
- Steuern Sie die MTU im BGP-Pfad, oder verwenden Sie das PMTUD-Protokoll, um die BGP-MSS automatisch anzupassen.
- Schnellere Fehlererkennung durch BFD oder Anpassung von BGP-Timern
- Die BGP-Skalierung richtet sich nach Konfiguration und Anwendungsfall. Es gibt keine Einheitslösung. Sie benötigen eine gute Idee zu folgenden Themen:
- Streckenwaage
  - Pfadskalierung (mit sanfter Neukonfiguration erhöht sich diese)
  - Attributskala
- Wenn der Add-Pfad konfiguriert ist, benötigt er mehr Speicher.
- Sorgfältige Kenntnis der BGP-Nachbarrichtlinien:
  - pass-all (insbesondere bei einem Boundary-Router) kann Chaos verursachen, wenn die Speicherskala ansteigt.
  - Verwenden Sie Richtlinienkonstrukte, die Übereinstimmungen mit regulären Ausdrücken in RPL vermeiden.
- Mit NSR benötigt der Standby-RP ca. 30 % mehr virtuellen Speicher als den aktiven. Beachten Sie dies, wenn ein Standby-RP vorhanden ist.

- Achten Sie bei einer erheblichen Anzahl von Routen (Versionssprünge) auf eine kontinuierliche Abwanderung. Dadurch bleibt der Speicher für die Aktualisierungsgenerierung möglicherweise auf hohem Niveau.
- Schützen Sie Peers mit dem Knopf für das max. Präfix.
- Verwendung von Next-Hop-Trigger-Verzögerungsparametern entsprechend der Skalierungs- und Konvergenzziele
- Vermeiden Sie beim Netzwerkdesign neue Attribute. Eindeutige Attribute führen zu ineffizienten Paketen und damit zu mehr BGP-Updates.
- Die Konfiguration mehrerer Pfade im Netzwerk kann zu Weiterleitungsschleifen führen. Vorsicht bei der Anwendung.
- Verwenden Sie die Tabellenrichtlinie, um die Routing-Installation auf Rib zu vermeiden, wenn RR nicht Inline-RR (kein Next-Hop-Self) ist.

Überwachen des Systemspeichers für Routing-Prozesse

Kein Gerät verfügt über unbegrenzte Ressourcen: Wenn wir eine unbegrenzte Anzahl von Routen an ein Gerät senden, muss das Gerät selbst entscheiden, wie es ausfällt. Die Router versuchen, alle Routen zu bedienen, bis die Speichergrenzen erreicht sind. Dies kann dazu führen, dass alle Routing-Protokolle und -Prozesse fehlschlagen.

Für jeden Prozess im Core-Router ist ein "RLIMIT" definiert. "RLIMIT" bezeichnet den Systemspeicher, den jeder Prozess beanspruchen darf.

In diesem Abschnitt werden einige Standardtechniken zur Überwachung und Überprüfung des vom BGP-Prozess verwendeten Systemspeichers beschrieben.

Prozessspeicher

Zeigt die Speichermenge an, die von einem Prozess belegt wird.

```
RP/0/RP0/CPU0:NCS-5501#show proc memory
JID Text(KB) Daten(KB) Stack(KB) Dynamischer (KB) Prozess
------ ---------- ---------- ---------- ----------- ------------------------------
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
```

Jedem Prozess wird eine maximale Speichermenge zugewiesen, die er verbrauchen darf. Dies wird als Grenzwert definiert.

```
RP/0/RP0/CPU0:NCS-5501#Details zum Prozessspeicher anzeigen
```

```
JID Text Data Stack Dynamic Dyn-Limit Shm-Tot Phy-Tot   Prozess
=============================================================================================
=======
1150 896 KB 359 MB 136 KB 32 MB 1024 MB 18 MB 24 MB  LSP-Server
1084 2 Mio. 2368 Mio. 136.000 30 Mio. 7447 Mio. 43 Mio. 69 Mio.     BGP
1.260 1 Mio. 1.529 Mio. 160.000 30 Mio. 8.192 Mio. 38 Mio. 52 Mio.  IPv4-Rippe
380.316.000 1.833 Mio. 136.000 29 Mio. 2.048 Mio. 25 Mio. 94 Mio.   Parser-Server
1.262 1 Mio. 1.134 Mio. 152.000 28 Mio. 8.192 Mio. 22 Mio. 31 Mio.  IPv6-Rippe
1277 4 Mio. 1445 Mio. 136.000 21 Mio. 1024 Mio. 18 Mio. 41 Mio.     pim6
1.301 80.000 222 Mio. 136.000 20 Mio. 300 Mio. 5 Mio. 33 Mio.   Schema-Server
1276 4 Mio. 1637 Mio. 136.000 20 Mio. 1024 Mio. 19 Mio. 41 Mio.     Pin
250 124 K 676 M 136 K 20 M 1024 M 9 M 31 M   invmgr_proxy
1.294 4 Mio. 2.024 Mio. 136.000 19 Mio. 1.861 Mio. 48 Mio. 66 Mio.  l2vpn_mgr
211 212.000 676 Mio. 136.000 18 Mio. 300 Mio. 9 Mio. 29 Mio.    sdr_invmgr
1.257 4.000 663 Mio. 136.000 17 Mio. 2.048 Mio. 20 Mio. 39 Mio.     Status_Manager_g
288 4.000 534 Mio. 136.000 16 Mio. 2048 Mio. 15 Mio. 33 Mio.    StatusManager_l
...
```

Wichtigste Speicherbenutzer

```
RP/0/RP0/CPU0:NCS-5501#show memory-top-users
##############################
 Hauptspeicher-Verbraucher auf 0/0/CPU0 (bei 2022/Apr/13/15:54:12)
##############################
    PID-Prozess insgesamt (MB) Heap (MB) Gemeinsam genutzt (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 Paket 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
##############################
 Hauptspeicher-Verbraucher auf 0/RP0/CPU0 (bei 2022/Apr/13/15:54:12)
##############################
    PID-Prozess insgesamt (MB) Heap (MB) Gemeinsam genutzt (MB)
   3581 spp 119 9.62 114
   4352 dpa_port_mapper 106 2,75 102
   4494 fib_mgr 99 7,71 90
   3582 Paket 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
```

Gesamter Arbeitsspeicher - verwendet und verfügbar

Systemkomponenten verfügen über einen festen Arbeitsspeicher.

```
RP/0/RP0/CPU0:NCS-5501#Zusammenfassender Speicherspeicherort anzeigen (alle)
Knoten: node0_0_CPU0
----------------------------------------------------------------
 Physischer Speicher: 8192 Mio. insgesamt (6172 Mio. verfügbar)
 Anwendungsspeicher: 8192M (6172M verfügbar)
 Bild: 4M (Bootram: 0M)
 Reserviert: 0M, IOMem: 0M, flashfsys: 0M
 Gesamtes gemeinsam genutztes Fenster: 226 Mio.
Knoten: node0_RP0_CPU0
----------------------------------------------------------------
 Physischer Arbeitsspeicher: 18432 Mio. insgesamt (15344 Mio. verfügbar)
 Anwendungsspeicher: 18432M (15344M verfügbar)
 Bild: 4M (Bootram: 0M)
 Reserviert: 0M, IOMem: 0M, flashfsys: 0M
 Gesamtes gemeinsam genutztes Fenster: 181M
```

Das Fenster "Freigegebener Speicher" enthält Informationen zu den freigegebenen Speicherzuweisungen im System.

```
RP/0/RP0/CPU0:NCS-5501#show memory summary detail location 0/RP0/CPU0
Knoten: node0_RP0_CPU0
----------------------------------------------------------------
 Physischer Arbeitsspeicher: 18432 Mio. insgesamt (15344 Mio. verfügbar)
 Anwendungsspeicher: 18432M (15344M verfügbar)
 Bild: 4M (Bootram: 0M)
 Reserviert: 0M, IOMem: 0M, flashfsys: 0M
 Shared window soasync-app-1: 243.328K
 Shared window soasync-12: 3,328 KB
 ...
 Shared window rewrite-db: 272.164K
 Gemeinsam genutztes Fenster l2fib_brg_shm: 139.758K
 Freigegebenes Fenster im_rules: 384.211K
 Grid_svr_shm im gemeinsamen Fenster: 44,272M
 Gemeinsam genutztes Fenster: 86.387M
 Freigegebenes Fenster im_db: 1.306M
 Gesamtes gemeinsam genutztes Fenster: 180.969M
 Zugewiesener Speicher: 2,337 GB
 Programmtext: 127.993T
 Programmdaten: 64.479G
 Programm-Stack: 2.034G
System-RAM: 18432M ( 19327352832)
Gesamt verwendet: 3088M ( 3238002688)
 Verwendet privat: 0M ( 0)
 Verwendet, gemeinsam genutzt: 3.088 Mio. ( 3238002688)
```

Sie können die Teilnehmerprozesse mit einem gemeinsamen Speicherfenster überprüfen.

```
RP/0/RP0/CPU0:NCS-5501#sh shmwin spp Teilnehmerliste
Daten für Fenster "spp":
----------------------------
Liste der aktuellen Teilnehmer:-
NAME PID JID INDEX
3581 113 0
Paket 3582 345 1
4362 432 2
Netio 4354 234 3
nsr_ping_reply 4371 291 4
aib 4423 296 5
ipv6_io 4497 430 6
ipv4_io 4484 438 7
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:BRU-SPCORE-PE6#sh shmwin soasync-1-Teilnehmerliste
Daten für Fenster "soasync-1":
----------------------------
Liste der aktuellen Teilnehmer:-
NAME PID JID INDEX
TCP 5584 168 0
BGP 8980 1084
```

Ressourcenüberwachung

Die Speichernutzung wird über einen Systemwächter in cXR und mit Resmon in eXR überwacht.

```
RP/0/RP0/CPU0:NCS-5501#Watchdog-Speicherstatus anzeigen
---- node0_RP0_CPU0 ----
Speicherinformationen:
    Physischer Speicher: 18432,0 MB
    Freier Speicher: 15348,0 MB
    Speicherstatus: Normal
RP/0/RP0/CPU0:NCS-5501#
RP/0/RP0/CPU0:NCS-5501#show watchdog threshold memory defaults location 0/RP0/CPU0
---- node0_RP0_CPU0 ----
 Standard-Speicherschwellenwerte:
 Minor: 1.843 MB ß: 10 %
 Schwer: 1.474 MB ß-8 %
 Kritisch: 921,599 MB ß-5 %
Speicherinformationen:
    Physischer Speicher: 18432,0 MB
    Freier Speicher: 15340,0 MB
    Speicherstatus: Normal
RP/0/RP0/CPU0:NCS-5501#
RP/0/RP0/CPU0:NCS-5501(config)#watchdog Schwellenwert-Speicher-Minor ?
  <5-40> Speicherverbrauch in Prozent
```

Bei Überschreitung der Schwellenwerte wird eine Warnung ausgegeben.

```
RP/0/RP0/CPU0:Feb 17 23:30:21.663 UTC: resmon[425]: %HA-HA_WD-4-MEMORY_ALARM : Speicherschwellenwert
überschritten: Minor mit 1840.000MB freiem Speicherplatz. Vorheriger Zustand: Normal
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USERS_INFO : Top 5
Consumer of System Memory (1884160 KB frei):
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 0:
Prozessname: bgp[0], pid: 7861, Heapverwendung: 12207392 KB 1.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 1:
Prozessname: ipv4_rib[0], pid: 4726, Heapverwendung: 708784 KB.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 2:
Prozessname: fib_mgr[0], pid: 3870, Heapverwendung: 584072 KB.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 3:
Prozessname: netconf[0], pid: 9260, Heapverwendung: 553352 KB 1.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 4:
Prozessname: netio[0], pid: 3655, Heapverwendung: 253556 KB 1.
LC/0/3/CPU0:Mar 8 05:48:58.414 PST: resmon[172]: %HA-HA_WD-4-MEMORY_ALARM : Speicherschwellenwert
überschritten: Schwerwiegend mit 600,182 MB freiem Speicherplatz. Vorheriger Zustand: Normal
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USERS_WARNUNG : Top 5
Verbraucher des Systemspeichers (624654 KB frei):
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNUNG : 0:
Prozessname: fib_mgr[0], pid: 5375, Heapnutzung 1014064 KB.
```

```
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNUNG : 1:
Prozessname: ipv4_mfwd_partner[0], pid: 5324, Heap-Nutzung 185596 KB.
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNUNG : 2:
Prozessname: nfsvr[0], pid: 8357, Heapnutzung 183692 KB.
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNUNG : 3:
Prozessname: fia_driver[0], pid: 3542, Heapnutzung 177552 KB.
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNUNG : 4:
Prozessname: npu_driver[0], pid: 3525, Heapnutzung 177156 KB.
```

Einige Prozesse können je nach dem Watchdog-Speicherstatus bestimmte Aktionen ausführen. BGP führt beispielsweise die folgenden Schritte aus:

- Im untergeordneten Status stellt BGP neue Peers nicht mehr bereit.
- Im schwerwiegenden Zustand führt BGP nach und nach zu einem Ausfall einiger Peers.
- in einem kritischen Zustand wird der BGP-Prozess beendet.

Prozesse können so konfiguriert werden, dass sie sich für Speicherzustandsbenachrichtigungen registrieren.

```
Überwachungs- oder Erkennungsprozess anzeigen
```

Benutzer können das automatische Herunterfahren des Prozesses aufgrund eines Watchdog-Zeitlimits deaktivieren.

```
Watchdog-Neustart Speicher-Hog deaktivieren
```

Wo finde ich weitere Informationen?

- Cisco IOS XR-Blogs und Whitepaper-Repository (xrdocs.io)
  - Core Fabric Design: https://xrdocs.io/design/blogs/latest-core-fabric-hld : In diesem Whitepaper werden die neuesten Trends und Entwicklungen im Core-Backbone-Netzwerk erläutert.
  - Peering Fabric Design: https://xrdocs.io/design/blogs/latest-peering-fabric-hld: Dieses Whitepaper bietet einen umfassenden Überblick über die Herausforderungen und Best Practice-Empfehlungen für Peering-Design mit Schwerpunkt auf Netzwerkvereinfachung.
- Konfigurationsleitfaden: Dieser Leitfaden enthält Informationen zum BGP: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html
- Befehlsreferenz: Diese Anleitung beschreibt die Befehle, die zum Konfigurieren und Überwachen von BGP auf Cisco NCS 5500 Routern mit Cisco IOS XR-Software verwendet werden: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/b-ncs5500-bgp-cli-reference.html

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.