Meilleures pratiques de déploiement de Cisco IOS XR pour le routage OSPF/IS-IS et BGP

Table des matières

AVERTISSEMENT

Ce document fournit un résumé de haut niveau de quelques recommandations établies de meilleures pratiques pour le routage OSPF/IS-IS et BGP. Ces recommandations ne représentent pas une conception validée par Cisco, et le déploiement dans un environnement d'exploitation spécifique requiert toute l'attention et toute l'attention requises. Ils doivent être lus conjointement avec les guides de configuration et la documentation technique des produits concernés, qui décrivent plus en détail la manière dont ces recommandations de meilleures pratiques peuvent être mises en oeuvre. Les références dans ce document aux guides de configuration et à la documentation technique pour des produits particuliers sont fournies à titre d'exemple uniquement. Reportez-vous aux guides de configuration et à la documentation technique de vos produits spécifiques.

Introduction

Ce document présente certaines des meilleures pratiques établies et des recommandations pour créer des réseaux simplifiés, efficaces et évolutifs alimentés par des plates-formes de routage IOS XR. Ce document se concentre sur des techniques d'implémentation spécifiques et sur les options de prise en charge des fonctionnalités disponibles dans IOS XR pour aider à personnaliser les déploiements OSPF/IS-IS et BGP.

Implémentation OSPF

Le protocole OSPF, défini dans la RFC 2328, est un protocole IGP utilisé pour distribuer des informations de routage dans un système autonome unique. Le protocole OSPF offre plusieurs avantages par rapport aux autres protocoles, mais une conception appropriée est nécessaire pour créer un réseau évolutif et à tolérance de panne.
Pour plus d'informations sur le protocole OSPF, reportez-vous à :

- TechNote sur OSPF : https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#anc13
- Guide de configuration pour 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
- Référence des commandes : 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

Concepts clés

- Hiérarchie : un modèle de réseau hiérarchique est un outil de haut niveau utile pour la conception d'une infrastructure réseau fiable et permet de diviser des problèmes de conception réseau complexes en zones plus petites et plus faciles à gérer.
- Modularité : en divisant les différentes fonctions d'un réseau en modules, le réseau est beaucoup plus facile à concevoir. Cisco a identifié plusieurs modules, notamment le campus d'entreprise, le bloc de services, le data center et la périphérie Internet.
- Résilience : le réseau est disponible dans des conditions normales et anormales. Les conditions normales incluent les flux de trafic attendus, les modèles et les événements planifiés tels que les fenêtres de maintenance. Les conditions anormales incluent les pannes matérielles

ou logicielles, les charges de trafic extrêmes, les modèles de trafic inhabituels, les événements de déni de service (DoS) et d'autres événements planifiés ou non planifiés.
■ Flexibilité : possibilité de modifier des parties du réseau, d'ajouter de nouveaux services ou d'augmenter la capacité sans passer par une mise à niveau massive (c'est-à-dire en remplaçant les principaux périphériques matériels).
En règle générale, le déploiement du réseau doit tenir compte de la « portée » du réseau pour contenir les routes dans une limite spécifique et les routes qui sont pertinentes et requises par les routeurs dans un domaine pour le transfert. L'utilisation efficace des zones OSPF permet de réduire le nombre d'annonces d'état des liaisons (LSA) et d'autres trafics aériens envoyés sur le réseau. L'un des avantages de la création d'une hiérarchie est que cette approche permet de s'assurer que la taille de la base de données topologique que chaque routeur devra gérer est gérable et conforme au profil de mémoire du routeur.

Redistribution du domaine OSPF et BGP

Le protocole OSPF est conçu pour transporter seulement quelques milliers de routes. À un niveau élevé, les « zones » OSPF sont des sections d'un réseau où n'importe quel routeur connaît la capacité de routage de tous les autres routeurs de la zone. Cela permet une convergence rapide lorsqu'un périphérique rencontre un problème, mais au prix d'une évolutivité réduite. Ainsi, OSPF est utilisé dans un coeur de fournisseur de services pour fournir la connectivité de niveau de base entre tous les périphériques principaux, et tous les périphériques principaux sont configurés dans la même zone OSPF. Il s'agit d'une conception standard d'un réseau « sous-jacent ».

En revanche, le protocole BGP est conçu pour transporter beaucoup plus de routes que la plupart des protocoles IGP, comme le protocole OSPF. Risques associés à la redistribution des routes BGP dans un IGP comme OSPF. Si un fournisseur de services exige que les routes BGP soient redistribuées dans le domaine IGP pour n'importe quel cas d'utilisation, alors cela doit être géré par le fournisseur de services avec un filtrage approprié au niveau des routeurs ASBR (Autonomous System Boundary Routers) et avec la protection de surcharge configurée sur le routeur récepteur. Si la redistribution BGP n'est pas filtrée dans un OSPF, chaque périphérique OSPF dans l'ASBR commencera à recevoir des routes bien au-delà de sa capacité de traitement en même temps. Les routeurs Cisco IOS XR, par exemple, n'autoriseront que 10 000 routes BGP à être redistribuées dans OSPF par défaut. Lorsque des routes BGP sont redistribuées dans le protocole IGP, il est possible que tous les routeurs du domaine IGP reçoivent ces routes, selon la conception IGP. Conformément au protocole OSPF RFC, toute route externe redistribuée dans OSPF doit être distribuée à tous les routeurs de la zone OSPF.

Gestion de la redistribution dans IGP

En règle générale, la redistribution ne doit être effectuée que de manière prudente et planifiée lorsqu'il n'existe aucune autre option pour apprendre les routes d'accessibilité fournies par une fonction de redistribution.

En règle générale, vous devez :

■ Éviter la redistribution
■ Éviter de transporter des routes dans un domaine IGP
■ Implémenter BGP pour l'accessibilité externe

■ Utilisez le protocole IGP pour transporter uniquement les informations de tronçon suivant ; par exemple, Loopback 0

Limites de redistribution de route OSPF

L'échelle des préfixes redistribués de BGP dans OSPF est gérée avec la configuration de protection de surcharge (max-lsa). C'est la seule protection contre la fuite d'un grand nombre de routes dans le domaine OSPF. En cas de redistribution dans une zone OSPF unique, vous devez implémenter plusieurs couches de protection contre la redistribution de route.

Voici quelques-unes des options disponibles pour la protection contre la redistribution de route :

■ Filtrage de redistribution avec ACL
■ Limite de redistribution - paramètre global pour empêcher la redistribution de plus d'un nombre spécifique de routes. Si le filtre est supprimé, la limite de redistribution globale est la deuxième ligne de défense et protégera les coeurs.
■ Configurations Max-LSA sur tous les périphériques de la zone OSPF : si les protections mentionnées dans les puces ci-dessus échouent, forcez les routeurs récepteurs à refuser les LSA excessives entrantes.

Protection contre la surcharge de la base de données à état de liens OSPF

La fonction de protection contre la surcharge de la base de données d'état des liaisons OSPF fournit un mécanisme au niveau OSPF pour limiter le nombre de LSA non générées automatiquement pour un processus OSPF donné. Si d'autres routeurs du réseau ont été mal configurés, ils peuvent générer un grand nombre de LSA, par exemple, pour redistribuer un grand nombre de préfixes dans OSPF. Ce mécanisme de protection permet d'empêcher les routeurs de recevoir de nombreuses LSA et, par conséquent, de connaître des pénuries de CPU et de mémoire.

Comportement des fonctionnalités

Voici comment la fonction se comporte :

■ Lorsque cette fonctionnalité est activée, le routeur conserve le nombre de toutes les LSA reçues (non générées automatiquement).
■ Lorsque la valeur de seuil configurée est atteinte, un message d'erreur est consigné.
■ Lorsque le nombre maximal configuré de LSA reçues est dépassé, le routeur cesse d'accepter de nouvelles 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>
```

États OSPF

Si le nombre de LSA reçues est supérieur au nombre max configuré après une minute, le processus OSPF met fin à toutes les contiguïtés et efface la base de données OSPF. Cet état est appelé l'état ignore. Dans cet état, tous les paquets OSPF reçus sur toutes les interfaces appartenant à l'instance OSPF sont ignorés et aucun paquet OSPF n'est généré sur les interfaces. Le processus OSPF reste à l'état ignore pendant la durée de la durée d'exclusion configurée (la valeur par défaut est 5 minutes). Lorsque le délai d'inactivité expire, le processus OSPF revient au fonctionnement normal et établit des contiguïtés sur toutes ses interfaces.

Si le nombre de LSA dépasse le nombre max dès que l'instance OSPF revient de l'état d'ignorance, l'instance OSPF peut osciller sans fin entre son état normal et l'état d'ignorance. Pour empêcher cette oscillation infinie, l'instance OSPF compte le nombre de fois qu'elle a été dans l'état ignore. Ce compteur est appelé ignore-count. Si la valeur ignore-count (la valeur par défaut ignore-count est 5) dépasse sa valeur configurée, l'instance OSPF reste définitivement à l'état ignore.
Vous devez émettre la commande clear ospf pour rétablir l'instance OSPF à son état normal. Le nombre ignore-count est remis à zéro si le nombre de LSA ne dépasse pas à nouveau le nombre maximal pendant la durée configurée par le mot clé reset-time.
Si vous utilisez le mot clé warning-only, l'instance OSPF n'entre jamais l'état ignore. Lorsque le nombre de LSA dépasse le nombre maximal, le processus OSPF consigne un message d'erreur et l'instance OSPF continue à fonctionner dans son état normal.
Il n'existe pas de valeur par défaut pour max-lsa. La limite n'est vérifiée que si elle est spécifiquement configurée.

Une fois que max-lsa est configuré, d'autres paramètres peuvent avoir des valeurs par défaut :

- %-threshold-to-log-warning par défaut - 75 %
- default ignore-count-value - 5
- ignore-time-in-minutes par défaut - 5 minutes
- délai par défaut de réinitialisation-ignore-count - 10 minutes

Voici un exemple d'implémentation qui montre comment configurer l'instance OSPF pour accepter 12000 LSA non auto-générées et 1000 LSA non auto-générées dans VRF V1.

```
RP/0/RSP0/CPU0:router# configure
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
```

L'exemple suivant montre comment afficher l'état actuel de l'instance OSPF.

```
RP/0/RSP0/CPU0:router# show ospf 0
    Processus de routage « ospf 0 » avec l'ID 10.0.0.2
    NSR (Non-stop routing) est désactivé
    Prend en charge uniquement les routes TOS(TOS0) uniques
    Prend en charge LSA opaque
    Il s’agit d’un routeur périphérique
    Nombre maximal de LSA non auto-générées autorisé 12000
       Nombre actuel de LSA 1 non autogénérées
       Seuil pour les messages d'avertissement 75 %
       Ignore-time 5 minutes, reset-time 10 minutes
       Ignore-count allowed 5, ignore-count 0 actuel
```

Implémentation de BGP

Les familles d'adresses BGP font du protocole BGP un protocole de routage « multiprotocole ». Il est vivement recommandé de comprendre comment les familles d'adresses sont utilisées pour créer des topologies évolutives faciles à mettre en oeuvre et à gérer. Grâce aux familles d'adresses, l'opérateur peut créer différentes topologies pour différentes technologies, par exemple, EVPN, multidiffusion, etc.

Pour plus d'informations sur BGP, consultez le guide de configuration BGP : https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html

BGP et BFD

La convergence BGP dans un réseau de fournisseur de services est importante pour répondre aux attentes des clients en matière de création de réseaux résilients et tolérants aux pannes. Par défaut, le BGP a un compteur de maintien de la connexion de 60 secondes et un compteur d'attente de 180 secondes. Tout cela signifie que le protocole BGP sera très lent à converger à moins qu'une aide soit disponible à partir des protocoles de prise en charge. BFD Bi-directional Forwarding (BFD) est un protocole conçu pour aider les protocoles clients à converger plus rapidement. Avec BFD, les protocoles peuvent converger en quelques secondes.

Additional Information

■ Ce guide fournit des informations conceptuelles et de configuration pour BFD : https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/76x/b-routing-cg-ncs5500-76x/implementing-bfd.html

■ Ce livre blanc présente une vue axée sur les fournisseurs de services sur la convergence rapide à l'aide de BFD sur les routeurs Cisco NCS 5500 et Cisco Network Convergence System 500 : https://xrdocs.io/ncs5500/tutorials/bfd-architecture-on-ncs5500-and-ncs500/

■ Pour plus d'informations sur l'utilisation de BFD sur les interfaces de bundle et la mise en oeuvre de Multipath et MultiHop BFD, reportez-vous au référentiel https://xrdocs.io/.

Détection d'homologue lente BGP

Un homologue lent est un homologue qui ne peut pas suivre le rythme auquel le routeur génère des messages de mise à jour sur une période prolongée (de l'ordre des minutes) dans un groupe de mise à jour. Lorsqu'un homologue lent est présent dans un groupe de mises à jour, le nombre de mises à jour formatées en attente de transmission augmente. Lorsque la limite de cache est atteinte, le groupe ne dispose plus de quotas pour formater les nouveaux messages. Pour qu'un nouveau message soit formaté, certains messages existants doivent être transmis à l'aide de l'homologue lent, puis supprimés du cache. Les autres membres du groupe qui sont plus rapides que l'homologue lent et ont terminé la transmission des messages formatés n'auront rien de nouveau à envoyer, même s'il peut y avoir des réseaux BGP nouvellement modifiés en attente d'annonce ou de retrait. Cet effet de blocage de la mise en forme de tous les homologues d'un groupe lorsque l'un des homologues est lent à consommer des mises à jour est le problème de « l'homologue lent ».

Les événements qui provoquent un taux de désactivation significatif dans la table BGP (tels que les réinitialisations de connexion) peuvent provoquer un bref pic dans le taux de génération des mises à jour. Un homologue qui prend temporairement du retard lors de tels événements, mais qui se rétablit rapidement après l'événement n'est pas considéré comme un homologue lent.

Pour qu'un homologue soit marqué comme lent, il doit être incapable de suivre le taux moyen de mises à jour générées sur une période plus longue (de l'ordre de quelques minutes).

L'homologue lent BGP peut être causé par :

■ Perte de paquets ou trafic élevé sur la liaison vers l'homologue.
■ Un homologue BGP peut être lourdement chargé en termes de CPU et ne peut donc pas servir la connexion TCP à la vitesse requise.
■ Dans ce cas, la capacité matérielle de la plate-forme et la charge offerte doivent être vérifiées.
■ Problèmes de débit avec la connexion BGP
■ Pour plus d'informations sur la détection d'homologue lent BGP, voir : 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

Voici quelques mesures d'atténuation et les meilleures pratiques pour gérer les homologues lents :

■ QoS de bout en bout, qui réserve de la bande passante pour le trafic du plan de contrôle BGP pendant l'encombrement.
■ Utilisation de valeurs MSS / MTU correctes et appropriées à l'aide des paramètres BGP PMTUD et/ou TCP MSS.
■ Utilisez le matériel approprié et minimisez le nombre de routes par rapport au matériel.

La détection des homologues lents est activée par défaut dans Cisco IOS XR à partir de la version 7.1.2. Les homologues lents sont des homologues qui sont lents à recevoir et à traiter les mises à jour BGP entrantes et à accuser réception des mises à jour à l'expéditeur. Si l'homologue lent participe au même groupe de mise à jour que les autres homologues, cela peut ralentir le processus de mise à jour pour tous les homologues. Dans cette version, lorsque IOS XR détecte un homologue lent, il crée un syslog contenant les détails de l'homologue spécifique.

Convergence rapide utilisant la convergence indépendante du préfixe BGP

Pour les préfixes BGP, une convergence rapide est obtenue à l'aide de la convergence indépendante des préfixes BGP (PIC), dans laquelle BGP calcule un meilleur chemin alternatif et un meilleur chemin principal et installe les deux chemins dans la table de routage en tant que chemins principaux et de secours.

Si la distance de tronçon suivant BGP devient inaccessible, BGP bascule immédiatement vers le chemin alternatif à l'aide du PIC BGP au lieu de recalculer le chemin après l'échec.

Si le PE distant de tronçon suivant BGP est actif, mais qu'il y a une défaillance de chemin, IGP TI-LFA FRR gère la convergence rapide vers le chemin alternatif, et BGP met à jour le tronçon suivant IGP pour le PE distant.

Le PIC BGP est configuré sous VRF address-family pour une convergence rapide des préfixes VPN si un PE distant devient inaccessible.

Pour plus d'informations sur la convergence indépendante du préfixe BGP, consultez la page : https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/bgp-pic.html

Sécurité BGP avec BGP Flowspec

BGP Flowspec, en bref, est une fonctionnalité qui vous permet de recevoir les spécifications de flux de trafic IPv4/IPv6 (source X, destination Y, protocole UDP, port source A, etc.) et les actions qui doivent être prises sur ce trafic (telles que la suppression, la police ou la redirection) via la mise à jour BGP.

Dans la mise à jour BGP, les critères de correspondance Flowspec sont représentés par BGP NLRI, et les communautés étendues BGP représentent les actions.

Cette fonctionnalité est basée sur la norme RFC 5575 et peut être utilisée pour limiter les attaques DDoS. Lorsqu'un hôte donné à l'intérieur d'un réseau est attaqué, nous pouvons envoyer une mise à jour Flowspec aux routeurs de périphérie afin que le trafic d'attaque puisse être régulé ou abandonné, ou même redirigé ailleurs, peut-être vers une appliance capable de nettoyer le trafic (filtrer le « mauvais » trafic et transférer uniquement le « bon » trafic vers l'hôte affecté).

Une fois que les spécifications de flux sont reçues par un routeur et programmées dans les cartes de ligne applicables, tous les ports L3 actifs sur ces cartes de ligne commencent à traiter le trafic entrant conformément aux règles Flowspec.

Pour plus d'informations sur l'implémentation de BGP FlowSpec, consultez :

■ Livre blanc BGP FlowSpec : https://xrdocs.io/ncs5500/tutorials/bgp-flowspec-on-ncs5500/
■ Guide de configuration 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

Fonction de préfixe maximal BGP

La fonctionnalité Maximum-Prefix est utile lorsque, lors d'une modification de la stratégie sortante sur le site d'appairage distant, un routeur commence à recevoir plus de préfixes que les ressources du routeur d'appairage ne peuvent en gérer, mais également pour protéger les ressources ou les homologues BGP internes où ces préfixes externes seront transférés. Une telle surcharge de ressources pourrait être gênante.

La fonctionnalité BGP maximum-prefix impose une limite maximale au nombre de préfixes qui sont reçus d'un voisin pour une famille d'adresses donnée. Par défaut, chaque fois que le nombre de préfixes reçus dépasse le nombre maximal configuré, la session BGP envoie une notification d'arrêt au voisin et la session se termine. Une seule famille d'adresses traversant le préfixe maximum entraînera l'arrêt de toute la session BGP, ce qui aura un impact sur toutes les autres familles d'adresses activées dans cette session BGP.

Cette fonctionnalité est couramment utilisée pour les homologues BGP externes afin de protéger l'infrastructure interne d'un fournisseur de services. Il sert de garde-corps pour empêcher l'épuisement des ressources du routeur qui pourrait être causé par une mauvaise configuration, soit localement, soit sur le voisin distant. La configuration de maximum-prefix est fortement recommandée pour se protéger contre les erreurs de configuration locales ou distantes qui pourraient déclencher la diffusion de la table de routage. Cela protège également contre les attaques de désagrégation de préfixe.

La configuration BGP maximum-prefix doit être explicitement activée sur tous les routeurs eBGP pour limiter le nombre de préfixes qu'il doit recevoir d'un voisin particulier, qu'il soit client ou homologue AS. Il est recommandé que l'opérateur configure une marge acceptable de préfixes supplémentaires que le système peut être en mesure de supporter après une évaluation minutieuse de la mémoire système disponible. Il convient de noter qu'il n'existe pas de configuration unique applicable à tous les routeurs et que le seuil doit être soigneusement ajusté en fonction du rôle du périphérique dans le réseau. Par exemple, si le préfixe maximal BGP doit être configuré sur les voisins IBGP, alors la valeur du préfixe maximal doit être inférieure sur les voisins configurés sur le route-reflector par rapport à celle des voisins configurés sur le route-reflector-clients. Le réflecteur de route agrège les préfixes reçus de plusieurs routeurs d'appairage, puis annonce de nouveau la table complète aux clients du réflecteur de route. Par conséquent, le réflecteur de route annoncera plus de préfixes à ses clients que ce qu'il reçoit de chaque homologue individuel. De même, un routeur d'appairage peut également annoncer à nouveau plus de préfixes vers le réflecteur de route que ce qu'il reçoit de chaque homologue externe individuel.

En résumé, il est recommandé d'examiner attentivement et de configurer l'action appropriée à entreprendre lorsque le seuil de préfixe maximal est atteint sur un périphérique de production. Certains attributs des options de commande maximum-prefix sont décrits comme suit :

- Lorsqu'une session BGP est explicitement configurée avec la fonctionnalité maximum-prefix sans aucun mot clé supplémentaire (tel qu'avertissement-only ou redémarrage potentiel), la session sera démantelée comme comportement par défaut. L'action par défaut consistant à arrêter une session homologue sans récupération automatique peut entraîner une interruption prolongée au niveau du coeur.

```
%ROUTING-BGP-5-ADJCHANGE_DETAIL : neighbor 10.10.10.10 Down -
Notification BGP reçue, nombre maximal de préfixes atteint (VRF : par
défaut ; AFI/SAFI : 1/1, 1/128, 2/4, 2/128, 1/133, 2/133) (AS : 65000)
"
%ROUTING-BGP-5-NBR_NSR_DISABLED_STANDBY : NSR désactivé sur le voisin
10.10.10.10 sur le RP en veille en raison d'un homologue dépassant la
limite de préfixe maximale (VRF : par défaut)
```

- La configuration de l'option de suppression des chemins supplémentaires supprime tous les préfixes excédentaires reçus du voisin au-dessus du seuil de valeur maximale configuré. Cette suppression n'entraîne pas d'instabilité de session. Les avantages de cette option incluent la limitation de l'utilisation de la mémoire du processus BGP et l'arrêt du battement des homologues au sein du réseau principal. Cependant, cela peut entraîner l'abandon des boucles de transfert pour les préfixes, car les entrées de transfert peuvent devenir incohérentes entre les routeurs du réseau.
- Lors de l'utilisation de add-path, la valeur maximum-prefix configurée s'applique aux chemins au lieu des préfixes car le NLRI est constitué du préfixe et des attributs de chemin. Référez-vous à la référence de commande suivante pour plus d'informations :

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

Recommandation : évaluez soigneusement les options suivantes lors de la configuration de la commande maximum-prefix :

- Aucune action explicite définie : le routeur arrête la session et maintient la relation de voisinage BGP inactive jusqu'à ce que l'opérateur efface manuellement la session BGP. [commande clear bgp]
- Restart [time-interval] : arrête la session et tente un redémarrage automatique de la session BGP périodiquement après une minuterie configurée. Cela réussira si l'homologue distant arrête d'annoncer les préfixes en excès sinon la session BGP sera de nouveau interrompue (provoquant ainsi une instabilité périodique).
- Discard-extra-paths : avec l'option discard-extra-paths, la session BGP reste active mais les préfixes au-dessus de la limite de préfixe maximum sont ignorés. Cette option n'a pas d'impact sur les autres familles d'adresses où le préfixe maximum n'a pas été atteint et garantit que les ressources locales ne sont pas épuisées, mais cela peut conduire à des boucles de transfert pour les préfixes qui sont rejetés. Notez que l'option discard extra paths ne peut pas coexister avec le bouton de reconfiguration logicielle.
- Warning-only : consigne un avertissement uniquement lorsque le seuil est atteint, afin que l'opérateur puisse prendre des mesures manuelles pour effacer la condition.

Pour plus d'informations, reportez-vous au Guide de configuration du routage comme suit :
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

Meilleures pratiques et recommandations

La liste suivante fournit un aperçu des meilleures pratiques générales et des recommandations, répertoriées dans un ordre non spécifique :

■ Audit du réseau pour l'état général du système. Commencez par un audit de configuration et passez séquentiellement des configurations d'interface au routage et aux services.
■ Avoir une stratégie de surveillance en place. Bien que le protocole SNMP soit une pratique standard, envisagez de déployer des techniques plus robustes et descriptives à l'aide de la télémétrie en continu. Reportez-vous au livre blanc suivant pour obtenir des recommandations sur les meilleures pratiques de mise en oeuvre de la télémétrie sur un routeur IOS XR : https://xrdocs.io/telemetry/

OSPF

Voici les meilleures pratiques générales et les recommandations relatives au protocole OSPF :

■ Implémenter le résumé de routage pour les routes intra-zone pour OSPF.
■ Configurez explicitement l'ID de routeur à l'intérieur du protocole OSPF comme l'une des adresses de bouclage compatibles OSPF.
■ Concevez un réseau hiérarchique pour limiter les LSA dans une zone pour OSPF. Conservez le nombre d'ABR dans une plage raisonnable (~3 à 4).
■ Implémentez la configuration « max-lsa » OSPF pour OSPF, ou l'équivalent, afin de limiter les LSA dans la base de données pour utiliser efficacement la mémoire du système.

■ Limitez le nombre maximal de routes qui peuvent être distribuées de BGP à OSPF. Dans IOS-XR, la limite par défaut est 10K.
■ Utilisez la politique de routage (RPL) pour redistribuer les routes dans OSPF.
■ Résumez la route inter-zone et les routes externes de type 5, le cas échéant.
■ Utilisation de l'authentification si nécessaire.
■ Utilisez toujours NSF et NSR.
■ Configurez le filtrage de redistribution à la source plutôt qu'à la destination.
■ Utiliser une interface passive, le cas échéant.
■ OSPF ne doit transporter que des routes de bouclage et d'interface de routeur - supprimez toute autre redistribution BGP vers OSPF.
■ Envisagez de déplacer chaque concentrateur principal dans sa propre zone (NSSA).
■ Utilisez BFD pour une détection rapide des défaillances par rapport aux compteurs de protocole de routage agressifs.
■ N'utilisez pas la commande mtu-ignore autant que possible.
■ Pensez à utiliser la synchronisation IGP-LDP dans un environnement MPLS pour éviter d'envoyer du trafic sur un chemin non étiqueté.
■ Tenez compte de l'évolutivité dans les limites de la plate-forme prise en charge (nombre de préfixes, nombre d'étiquettes, ECMP, nombre de zones, etc.).
■ Éviter la redistribution mutuelle en plusieurs points.
■ Configurez la distance administrative de sorte que chaque préfixe natif de chaque protocole ou processus soit atteint via le protocole ou processus du domaine correspondant.
■ Contrôlez les préfixes (en utilisant la distance ou la combinaison préfixe-liste) de sorte que le même préfixe ne soit pas annoncé au domaine d'origine.
■ Bien que l'ID de processus OSPF ait une signification locale pour le routeur, il est recommandé d'avoir le même ID de processus pour tous les routeurs du même domaine OSPF. Cela améliore la cohérence de la configuration et facilite les tâches de configuration automatiques.
■ Lors de la configuration du protocole OSPF pour les environnements Hub and Spoke, concevez les zones OSPF avec un nombre de routeurs plus réduit.
■ Configurez la bande passante de référence de coût automatique OSPF dans tout le domaine OSPF sur la liaison de bande passante la plus élevée du réseau.
■ Du point de vue de la conception, nous vous recommandons d'implémenter l'appairage IGP avec des domaines sous les mêmes contrôles administratifs ou opérationnels afin d'éviter la propagation d'une mise à jour IGP non planifiée ou indésirable sur le réseau. Cela devrait permettre une meilleure facilité de maintenance et de dépannage en cas d'erreurs. Dans le cas où un grand domaine IGP est une nécessité commerciale, prévoyez d'utiliser BGP dans ces cas pour limiter le nombre de routes dans le domaine de réseau IGP.
■ Si vous avez besoin d'une connectivité MPLS de bout en bout, continuez à utiliser la hiérarchie/segmentation et utilisez des options telles que RFC3107 BGP-LU ou le calcul de chemin entre domaines via PCE, ou sélectionnez redistribution/fuite avec la politique en dernier recours.
■ La fonction de limitation du plus court chemin OSPF peut être utilisée pour configurer la planification SPF à intervalles de quelques millisecondes et pour retarder potentiellement les calculs SPF pendant l'instabilité du réseau.

■ La fonctionnalité de hiérarchisation des préfixes SPF OSPF permet à un administrateur de faire converger les préfixes importants plus rapidement pendant l'installation de la route.

IS-IS

Voici les meilleures pratiques générales et les recommandations pour IS-IS :

■ Si vous utilisez un réseau plat à un niveau, pensez à l'échelle. Configurez tous les routeurs en tant que L2 uniquement. Par défaut, le routeur est L1-L2 et les fuites d'informations de routage de L1 vers L2 sont activées par défaut. Cela peut entraîner la fuite de toutes les routes L1 vers L2 par tous les routeurs, ce qui peut gonfler la base de données d'état des liaisons.
■ Si vous exécutez un réseau à plusieurs niveaux (plusieurs zones), assurez-vous que la topologie de couche 3 suit la hiérarchie ISIS. Ne créez pas de liens de porte dérobée entre les zones L1.
■ Si vous utilisez un réseau à plusieurs niveaux (plusieurs zones), assurez-vous que les routeurs L1 et L2 sont connectés via les zones L1 et L2. Cela ne nécessite pas de connexions physiques ou virtuelles multiples entre eux ; exécutez la liaison entre les routeurs L1 et L2 en tant que circuit L1/L2.
■ Si vous exécutez un réseau à plusieurs niveaux (plusieurs zones), résumez ce qui peut être résumé : par exemple, dans le cas de MPLS, le bouclage des routeurs PE doit être propagé entre les zones, mais pas les adresses de liaison d'infrastructure.
■ Créez et suivez le plan d'adressage approprié si possible. Cela permet la récapitulation et facilite l'évolutivité.
■ Réglez la durée de vie du LSP sur 18 heures maximum.
■ Évitez la redistribution par tous les moyens. La redistribution est complexe et doit être gérée manuellement pour éviter les boucles de routage. Si possible, utilisez une conception à zones/niveaux multiples.
■ Si vous devez utiliser la redistribution, utilisez le balisage de route pendant la redistribution et le filtrage « distribute-list in » basé sur les balises pour la gérer. Résumer lors de la redistribution si possible.
■ Configurez les interfaces en tant que « point à point » chaque fois que possible. Cela améliore les performances et l'évolutivité du protocole.
■ N'utilisez pas ISIS dans une topologie à maillage élevé. Les protocoles à état de liens se comportent mal dans les environnements à maillage élevé.
■ Configurez une métrique haute par défaut dans le sous-mode de la famille d'adresses ISIS. Cela empêche les liaisons nouvellement ajoutées d'attirer le trafic si elles sont configurées par inadvertance sans métrique.
■ Configurez « log adjacency changes » pour faciliter le dépannage des connexions.
■ Utilisez « metric-style wide » sous le sous-mode ipv4 de la famille d'adresses ISIS. Les métriques étroites ne sont pas très utiles et ne prennent pas en charge des fonctionnalités telles que le routage de segment ou flex-algo.
■ Si vous utilisez SR-MPLS TI-LFA, n'oubliez pas d'ajouter "ipv4 unnumbered mpls traffic-eng Loopback0" à la configuration pour permettre à ISIS d'allouer des tunnels TE si nécessaire.
■ Laissez les configurations "lsp-gen-interval" et "spf-interval" par défaut, sauf si vous êtes sûr que la convergence native plus rapide est requise. Avec la convergence native TI-LFA, ce n'est pas aussi important, car le réacheminement rapide gère les changements de topologie uniques en 50 ms ou moins.

■ Si vous modifiez « lsp-gen-interval » ou « spf-interval », n'utilisez pas un délai initial inférieur à 50 ms.
■ Dans la plupart des cas, "set-overload-bit" est un meilleur choix que "max-metric" car c'est un changement atomique qui est pris en charge par fast-reroute.
■ Utiliser l'authentification cryptographique pour les paquets Hello (hello-password) et LSP (lsp-password). Les porte-clés offrent la plus grande flexibilité et peuvent accueillir des inversions de clés.
■ Configurez « nsf cisco » pour une authentification transparente des redémarrages de processus ISIS et de l'installation SMU. Malgré son nom, il offre une meilleure interopérabilité avec les autres fournisseurs que « nsf ietf ».
■ Sur une plate-forme avec deux RP, configurez ÉGALEMENT « nsr » pour gérer les commutations RP.
■ Utilisez les modèles « group » et « apply-group » pour configurer des sections de configuration répétées. Cela est moins sujet aux erreurs et plus facile à modifier si nécessaire.
■ Dans un réseau à plusieurs niveaux, réfléchissez soigneusement si vous devez utiliser la « propagation » pour faire passer les préfixes du niveau 2 au niveau 1. Cela peut limiter l'évolutivité et, souvent, la route par défaut de niveau 1 fournie par le bit attaché est suffisante.
■ Si vous utilisez plusieurs instances ISIS dans le même VRF, envisagez de configurer des valeurs de « distance » uniques pour ces instances. L'installation de route dans le RIB sera ainsi plus déterministe si chacun d'eux a une route vers le même préfixe.
■ Utilisez BFD pour une détection rapide de liaison inactive. Avec BFD fournissant cette fonction, l'intervalle Hello ISIS peut être augmenté en toute sécurité pour améliorer l'évolutivité.

BGP

Voici les meilleures pratiques générales et les recommandations pour BGP :

■ Utilisez NSR et NSF / redémarrage en douceur avec des minuteurs soigneusement réglés en fonction de l'échelle prévue.
■ Configurez BGP en utilisant l'interface de bouclage « toujours actif », et non l'interface physique pour l'appairage IBGP.
■ Ne redistribuez pas les routes BGP (grand volume) dans IGP (volume relativement faible) et vice-versa sans RPL approprié, limitant le nombre de routes redistribuées de BGP à un IGP (OSPF/ISIS).
■ La redistribution BGP vers IGP sans une stratégie (ACL) correcte et bien testée peut entraîner une épuisement des ressources (mémoire) sur le routeur.
■ Utilisation de résumés de routage dans BGP pour diminuer la taille de la table de routage et l'utilisation de la mémoire. Agrégez les routes avec résumé uniquement là où cela est logique
■ Utiliser le filtrage de route pour annoncer et recevoir des routes efficacement, en particulier dans BGP.
■ Nous vous recommandons d'utiliser le réflecteur de route (RR) et la confédération pour faire évoluer le réseau.
■ Voici quelques-unes des considérations relatives à la conception du réflecteur de route :
■ L'échelle des chemins augmente en fonction du nombre de clients/non-clients.

■ Dans les RR hiérarchiques, utilisez le même ID de cluster au même niveau (RR redondant) pour la prévention des boucles et l'évolutivité.
■ Contrôlez MTU dans le chemin BGP ou utilisez le protocole PMTUD pour ajuster automatiquement BGP MSS.
■ Utilisez BFD ou réglez les compteurs BGP pour accélérer les détections de panne.
■ L'échelle BGP est conforme à la configuration et au cas d'utilisation, et aucune taille unique ne convient à tous. Vous devez avoir une bonne idée des éléments suivants :
■ échelle de routage
— échelle du chemin (avec une reconfiguration logicielle, elle augmentera)
— échelle des attributs
■ Si le chemin d'accès supplémentaire est configuré, il consomme plus de mémoire.
■ Compréhension attentive des politiques de voisinage BGP :
— la passe-tout (en particulier au niveau d'un routeur de périphérie) peut provoquer des dégâts, car l'échelle de la mémoire augmentera.
— Utiliser des constructions de stratégie qui éviteront les correspondances d'expressions régulières dans RPL.
■ Avec NSR, le RP de secours utilisera environ 30 % de mémoire virtuelle en plus que la mémoire active. Gardez ceci à l'esprit s'il y a un RP de secours.
■ Recherchez des désabonnements continus dans un nombre significatif de routes (bosses de version). Cela peut maintenir la mémoire de génération de mise à jour dans un filigrane élevé.
■ Protéger les homologues avec le bouton préfixe max.
■ Utiliser les paramètres de délai de déclenchement du saut suivant en fonction des objectifs d'échelle et de convergence.
■ Dans la conception du réseau, essayez d'éviter de nouveaux attributs. Des attributs uniques conduisent à un emballage inefficace et entraînent plus de mises à jour BGP.
■ La configuration de plusieurs chemins sur le réseau peut entraîner des boucles de transfert. À utiliser avec précaution.
■ Utilisez la stratégie de table pour éviter l'installation de route vers rib si RR n'est pas inline-RR (no next-hop-self)

Surveiller la mémoire système pour les processus de routage

Aucun périphérique ne dispose de ressources infinies : si nous envoyons un nombre infini de routes à un périphérique, ce dernier doit choisir la manière dont il tombe en panne. Les routeurs tentent de desservir toutes les routes jusqu'à ce que les limites de mémoire soient épuisées, ce qui peut entraîner l'échec de tous les protocoles et processus de routage.

Un « RLIMIT » est défini pour chaque processus du routeur principal. Le « RLIMIT » est la quantité de mémoire système que chaque processus est autorisé à consommer.

Cette section décrit quelques techniques standard pour surveiller et vérifier votre mémoire système utilisée par le processus BGP.

Mémoire de traitement

Affiche la quantité de mémoire consommée par un processus.

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

JID Text(KB) Data(KB) Stack(KB) Dynamic(KB) Process
```

```
------ ---------- ---------- ---------- ----------- ----------------------------
-
1150 896 368300 136 33462 serveur_lspv
380 316 1877872 136 32775 parser_server
1 084 2 092 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 serveur_schéma
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
```

Une quantité maximale de mémoire pouvant être consommée par chaque processus est allouée. Il s'agit de la limite.

```
RP/0/RP0/CPU0:NCS-5501#show proc memory detail
JID Text Data Stack Dynamic Dyn-Limit Shm-Tot Phy-Tot Process
================================================================================
============================
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
211 212 000 676 M 136 000 18 300 M 9 M 29 M sdr_invmgr
1257 4K 663M 136K 17M 2048M 20M 39M statsd_manager_g
288 4K 534M 136K 16M 2048M 15M 33M statsd_manager_l
...
```

Principaux consommateurs de mémoire

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

```
##############################################################################
##############################################################################
##############################################################################
##############################################################################
 Principaux consommateurs de mémoire sur 0/0/CPU0 (à 2022/13/15:54:12)
##############################################################################
##############################################################################
##############################################################################
##############################################################################
    Total du processus PID (Mo) Segment (Mo) Partagé (Mo)
   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 paquet 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 pilote_optique 62 141,23 22
   4090 ipv6_nd 55 4,13 49
##############################################################################
##############################################################################
##############################################################################
##############################################################################
 Principaux consommateurs de mémoire sur 0/RP0/CPU0 (à 20xx/MMM/HH:MM:SS)
##############################################################################
##############################################################################
##############################################################################
##############################################################################
    Total du processus PID (Mo) Segment (Mo) Partagé (Mo)
   3581 spp 119 9,62 114
   4352 dpa_port_mapper 106 2,75 102
   4494 fib_mgr 99 7,71 90
   3582 paquet 96 1,48 94
   3684 parser_server 95 64,27 25
   8144 te_control 71 15,06 55
   8 980 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
```

Mémoire totale - Utilisée et disponible

Les composants du système disposent d'une quantité fixe de mémoire.

```
RP/0/RP0/CPU0:NCS-5501#show memory summary location all
noeud : node0_0_CPU0
------------------------------------------------------------------
 Mémoire physique : 8 192 M au total (6 172 M disponibles)
 Mémoire d'application : 8192M (6172M disponible)
 Image : 4M (bootram : 0M)
 Réservé : 0M, IOMem : 0M, flashfsys : 0M
 Fenêtre partagée totale : 226 millions
noeud : node0_RP0_CPU0
------------------------------------------------------------------
 Mémoire physique : 18432M au total (15344M disponibles)
 Mémoire d'application : 18432M (15344M disponible)
 Image : 4M (bootram : 0M)
 Réservé : 0M, IOMem : 0M, flashfsys : 0M
 Fenêtre partagée totale : 181 millions
```

La fenêtre Mémoire partagée fournit des informations sur les allocations de mémoire partagée sur le système.

```
RP/0/RP0/CPU0:NCS-5501#show memory summary detail location 0/RP0/CPU0
noeud : node0_RP0_CPU0
------------------------------------------------------------------
 Mémoire physique : 18432M au total (15344M disponibles)
 Mémoire d'application : 18432M (15344M disponible)
 Image : 4M (bootram : 0M)
 Réservé : 0M, IOMem : 0M, flashfsys : 0M
 Fenêtre partagée soasync-app-1 : 243 328 Ko
 Fenêtre partagée soasync-12 : 3 328 Ko
 ...
 Rewrite-db de fenêtre partagée : 272,164 Ko
 Fenêtre partagée l2fib_brg_shm : 139 758 Ko
 Fenêtre partagée im_rules : 384,211 Ko
 Fenêtre partagée grid_svr_shm : 44,272 Mo
 Fenêtre partagée spp : 86,387 M
```

```
 Fenêtre partagée im_db : 1,306 M
 Fenêtre partagée totale : 180,969 millions
 Mémoire allouée : 2,337G
 Texte du programme : 127.993T
 Données du programme : 64.479G
 Pile de programmes : 2,034G
Mémoire vive du système : 18432M ( 19327352832)
Total utilisé : 3 088 millions ( 3238002688)
 Privé utilisé : 0M ( 0)
 Partagé utilisé : 3 088 M ( 3238002688)
```

Vous pouvez vérifier les processus des participants avec une fenêtre de mémoire partagée.

```
RP/0/RP0/CPU0:NCS-5501#sh liste des participants shmwin spp
Données pour la fenêtre "spp" :
----------------------------
Liste des participants actuels : -
NOM PID JID INDEX
espèces 3581 113 0
paquet 3582 345 1
ncd 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:NCS-5501#sh shmwin soasync-1 liste des participants
Données pour la fenêtre "soasync-1" :
----------------------------
Liste des participants actuels : -
```

```
NOM PID JID INDEX
tcp 5584 168 0
bgp 8980 1084
```

Surveillance des ressources et chiens de garde

L'utilisation de la mémoire est surveillée par un contrôleur système dans cXR et avec Resmon dans eXR.

```
RP/0/RP0/CPU0:NCS-5501#show watchdog memory-state
---- node0_RP0_CPU0 ----
Informations sur la mémoire :
    Mémoire physique : 18432,0 Mo
    Mémoire libre : 15348,0 Mo
    État de la mémoire : 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 ----
 Seuils de mémoire par défaut :
 Mineur : 1 843 Mo ß - 10 %
 Grave : 1 474 Mo ß - 8 %
 Critique : 921,599 Mo ß - 5 %
Informations sur la mémoire :
    Mémoire physique : 18432,0 Mo
    Mémoire libre : 15340,0 Mo
    État de la mémoire : Normal
RP/0/RP0/CPU0:NCS-5501#
RP/0/RP0/CPU0:NCS-5501(config)#watchdog threshold memory minor ?
  <5-40> consommation de mémoire en pourcentage
```

Un avertissement est imprimé si les seuils sont dépassés.

```
RP/0/RP0/CPU0:Feb 17 23:30:21.663 UTC: resmon[425]: %HA-HA_WD-4-MEMORY_ALARM :
Seuil de mémoire dépassé : Mineur avec 1840.000 Mo de mémoire libre. État
précédent : Normal
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USERS_INFO : 5 principaux consommateurs de mémoire système (1884160 Ko
libres) :
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC : resmon[425] : %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 0: Nom du processus : bgp[0], pid : 7861, Utilisation du
segment de mémoire : 12207392 ko.
```

```
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC : resmon[425] : %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 1 : Nom du processus : ipv4_rib[0], pid : 4726,
Utilisation du segment de mémoire : 708784 ko.

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC : resmon[425] : %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 2 : Nom du processus : fib_mgr[0], pid : 3870, Utilisation
du segment de mémoire : 584072 ko.

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC : resmon[425] : %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 3 : Nom du processus : netconf[0], pid : 9260, Utilisation
du segment de mémoire : 553352 ko.

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC : resmon[425] : %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 4 : Nom du processus : netio[0], pid : 3655, Utilisation
du segment de mémoire : 253556 ko.

LC/0/3/CPU0:Mar 8 05:48:58.414 PST: resmon[172]: %HA-HA_WD-4-MEMORY_ALARM : Seuil
de mémoire dépassé : Sévère avec 600,182 Mo de mémoire libre. État précédent :
Normal

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USERS_WARNING : 5 principaux consommateurs de mémoire système (624654
Ko libres) :

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 0: Nom du processus : fib_mgr[0], pid: 5375,
Utilisation du segment de mémoire 1014064 Ko.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 1: Nom du processus : ipv4_mfwd_partner[0], pid: 5324,
Utilisation du segment de mémoire 185596 Ko.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 2: Nom du processus : nfsvr[0], pid: 8357, Utilisation
du segment de mémoire 183692 Ko.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 3: Nom du processus : fia_driver[0], pid: 3542,
Utilisation du segment de mémoire 177552 Ko.

LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 4: Nom du processus : npu_driver[0], pid: 3525,
Utilisation du segment de mémoire 177156 Ko.
```

Certains processus peuvent effectuer des actions spécifiques en fonction de l'état de la mémoire du chien de garde. Par exemple, BGP effectue les opérations suivantes :

- dans l'état mineur, BGP arrête d'amener de nouveaux homologues
- dans l'état sévère, BGP fait tomber progressivement certains homologues.
- dans un état critique, le processus BGP s'arrête.

Les processus peuvent être configurés pour s'inscrire aux notifications d'état de la mémoire.

Show watchdog ou-aware-process

Les utilisateurs peuvent désactiver l'arrêt automatique des processus en raison du délai de surveillance.

watchdog restart memory-hog disable

Où trouver plus d'informations ?

- Référentiel de blogs et de livres blancs Cisco IOS XR (xrdocs.io)
  - Core Fabric Design : https://xrdocs.io/design/blogs/latest-core-fabric-hld : ce livre blanc traite des tendances et de l'évolution récentes des réseaux fédérateurs.
  - Peering Fabric Design : https://xrdocs.io/design/blogs/latest-peering-fabric-hld : ce livre blanc présente de manière exhaustive les défis et les meilleures pratiques en matière de conception d'appairage, en mettant l'accent sur la simplification du réseau.
- Référence du guide de configuration : Implementing BGP https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/710x/b-bgp-cg-ncs5500-710x/implementing-bgp.html

Améliorations des fonctionnalités

Isolation du routeur de périphérie du système autonome et contrôle de contiguïté pour les dépassements de LSA	Introduit dans la version 7.10.1 sur les routeurs à port fixe NCS 5500 : routeurs à port fixe NCS 5700 Dans un réseau utilisant un routeur ASBR (Autonomous System Boundary Router) et d'autres routeurs, vous êtes désormais assuré d'un flux de trafic ininterrompu même si l'ASBR génère des LSA qui dépassent la limite que vous avez configurée. Ceci est rendu possible puisque vous pouvez maintenant isoler les ASBR et contrôler également la durée de contiguïté dans la phase EXCHANGE ou LOADING. En isolant le routeur ASBR de ses voisins immédiats, la topologie de réseau restante peut continuer à fonctionner sans interruption, évitant ainsi tout impact négatif sur le flux de trafic. Cette approche simplifie également le processus de récupération, car une intervention manuelle n'est nécessaire que pour les voisins immédiats des routeurs ASBR. Cette fonctionnalité introduit les modifications suivantes : CLI : • max-external-lsa • exchange-timer Modèle de données YANG : • Cisco-IOS-XR-ipv4-ospf-cfg.yang • Cisco-IOS-XR-ipv4-ospf-oper.yang • Cisco-IOS-XR-um-router-ospf-cfg.yang (voir GitHub, Navigateur de modèles de données YANG)
Rétablir automatiquement une session de voisinage BGP	Introduit dans cette version sur : les routeurs à port fixe NCS 5500 ; les routeurs à port fixe NCS 5700 ; les routeurs modulaires NCS 5500 (cartes de ligne NCS 5500 ; cartes de ligne NCS 5700 [Mode : Compatibilité ; Natif]) Vous pouvez maintenant configurer le routeur pour rétablir automatiquement une session de voisinage BGP qui a été désactivée parce que la limite de préfixe maximal a été dépassée. La fonctionnalité introduit les modifications suivantes :

	CLI • maximum-prefix-restart-time Modèle de données YANG : • Nouveaux XPaths pour openconfig-bgp-neighbor.yang(voir GitHub, Navigateur de modèles de données YANG)
BGP Flowspec sur les interfaces virtuelles du groupe de ponts	Introduit dans la version 7.10.1 sur : Routeurs modulaires NCS 5500 (cartes de ligne NCS 5700 [Mode : natif]) Vous pouvez maintenant utiliser BGP Flowspec sur l'interface virtuelle de groupe de ponts (BVI) pour vous connecter à des domaines de diffusion qui hébergent des périphériques hôtes, comme dans le cas des réseaux d'entreprise. Grâce à cette prise en charge, vos clients peuvent protéger leurs réseaux contre les menaces réseau telles que les attaques par déni de service distribué (DDoS) provenant de l'interface BVI.
Ignorer le message de mise à jour BGP entrant	Introduit dans la version 7.10.1 sur : les routeurs à port fixe NCS 5500 ; les routeurs à port fixe NCS 5700 ; les routeurs modulaires NCS 5500 (cartes de ligne NCS 5500 ; cartes de ligne NCS 5700 [Mode : Compatibilité ; Natif]) Vous pouvez maintenant éviter la réinitialisation de session lorsqu'une session BGP rencontre des erreurs lors de l'analyse du message de mise à jour reçu. Ceci est rendu possible parce que la fonctionnalité permet de rejeter le message de mise à jour entrant comme un message de retrait. CLI : • mise à jour dans la gestion des erreurs de traitement de traitement de retrait Modèle de données YANG : • Nouveaux XPaths pour openconfig-bgp-neighbor.yang (voir GitHub, Navigateur de modèles de données YANG)
Exclusion de l'allocation d'étiquettes pour les routes non annoncées	Introduit dans la version 7.10.1 sur : les routeurs à port fixe NCS 5500 ; les routeurs à port fixe NCS 5700 ; les routeurs modulaires NCS 5500 (cartes de ligne NCS 5500 ; cartes de ligne NCS 5700 [Mode : Compatibilité ; Natif]) Nous avons amélioré la gestion de l'espace d'étiquetage et l'utilisation des ressources matérielles en assouplissant l'allocation d'étiquettes MPLS. Cette flexibilité signifie que vous pouvez désormais attribuer ces étiquettes uniquement aux routes annoncées à leurs homologues, ce qui garantit une meilleure gestion de l'espace d'étiquetage et une meilleure utilisation des ressources matérielles. Avant cette version, l'attribution d'étiquettes était effectuée indépendamment du fait que les routes soient annoncées ou non. Cela a entraîné une utilisation inefficace de l'espace réservé aux étiquettes.

Protection des voisins EBGP connectés directement via l'identificateur LPTS basé sur l'interface	Introduit dans la version 7.10.1 sur : routeurs à port fixe NCS 5500 Nous avons amélioré la sécurité du réseau pour les voisins eBGP connectés directement en nous assurant que seuls les paquets provenant de voisins eBGP désignés peuvent traverser une interface unique, empêchant ainsi l'usurpation d'adresse IP. Ceci est rendu possible parce que nous avons maintenant ajouté un identificateur d'interface pour les services de transport de paquets locaux (LPTS). LPTS filtre et gère les paquets en fonction du type de débit que vous configurez. Cette fonctionnalité introduit les éléments suivants : CLI : • bgp lpts-secure-binding Modèle de données YANG : • Cisco-IOS-XR-um-router-bgp-cfg (voir GitHub, Navigateur de modèles de données YANG)
Réduire les récursions pour l'appairage eBGP sur l'adresse de bouclage sur l'interface virtuelle du groupe de ponts	Introduit dans la version 7.10.1 sur : Routeurs modulaires NCS 5500 (cartes de ligne NCS 5700 [Mode : natif]) Vous pouvez maintenant obtenir l'appairage eBGP sur les interfaces de bouclage sur l'interface virtuelle de groupe de pont (BVI) et réduire le niveau de récursivité de trois à deux. Cette réduction du niveau de récursivité, obtenue en supprimant la nécessité d'utiliser le nom BVI dans la configuration des routes statiques, permet un transfert de paquets plus rapide et une meilleure utilisation des ressources réseau.
Comptabilité de stratégie BGP	Introduit dans la version 7.9.1 : la comptabilité des politiques BGP (Border Gateway Protocol) mesure et classe le trafic IP reçu de différents homologues. Vous pouvez identifier et comptabiliser tout le trafic par client et facturer en conséquence. La comptabilité des stratégies est activée sur une base d'interface d'entrée individuelle. En utilisant la comptabilité de stratégie BGP, vous pouvez maintenant rendre compte du trafic en fonction de la route qu'il traverse. Cette fonctionnalité est désormais prise en charge sur les routeurs équipés de cartes de ligne Cisco NC57 avec TCAM externe (eTCAM) et fonctionnant en mode natif. Cette fonctionnalité introduit les modifications suivantes : • CLI : cette fonctionnalité présente la hw-module fib bgppa stats-mode erasecat4000_flash:. • Modèle de données YANG : nouveaux chemins d'accès pour Cisco-IOS-XR-um-hw-module-profile-cfg.yang (voir GitHub, Navigateur de modèles de données YANG)
Détecter un homologue lent dans	Introduit dans la version 7.9.1 : les homologues BGP traitent les messages de mise à jour BGP entrants à des débits différents. Un

un groupe BGP	homologue lent est un homologue qui traite les messages de mise à jour BGP entrants très lentement sur une longue période par rapport aux autres homologues dans le sous-groupe de mise à jour. La lenteur de la gestion des homologues est importante lorsque les routes changent constamment sur une longue période. Il est important de nettoyer les informations obsolètes dans la file d'attente et d'envoyer uniquement l'état le plus récent. Il est utile de savoir s'il existe un homologue lent, ce qui indique qu'il existe un problème réseau, tel qu'une congestion permanente du réseau ou un récepteur ne traitant pas les mises à jour à temps, que l'administrateur réseau peut résoudre.
Limitation des numéros LSA dans une base de données d'états de liens OSPF	Introduit dans la version 7.9.1 : les LSA (Link-State Advertisements) non auto-générées pour un processus OSPF (Open Shortest Path First) donné sont limitées à 500000. Ce mécanisme de protection empêche les routeurs de recevoir de nombreuses LSA, ce qui empêche les pannes de CPU et les pénuries de mémoire, et est activé par défaut à partir de cette version. Si vous avez plus de 500000 LSA dans votre réseau, configurez la commande max-lsa avec l'échelle de LSA attendue avant de mettre à niveau vers cette version ou ultérieure. Cette fonction modifie les commandes suivantes : • show ospf pour afficher le nombre maximal de préfixes redistribués. • show ospf database database-summary detail pour afficher le nombre de LSA par routeur. • show ospf database-summary adv-routerrouter ID pour afficher les informations du routeur et les LSA reçues d'un routeur particulier.
Limitation du nombre maximal de préfixes LSA de type 3 redistribués dans OSPF	Introduit dans la version 7.9.1 : par défaut, le nombre maximal de préfixes LSA de type 3 redistribués pour un processus OSPF donné est désormais limité à 100000. Ce mécanisme empêche le protocole OSPF de redistribuer un grand nombre de préfixes en tant que LSA de type 3 et empêche ainsi une utilisation élevée du CPU et des pénuries de mémoire. Une fois que le nombre de préfixes redistribués est atteint ou dépasse la valeur seuil, le message du journal système est généré et aucun autre préfixe n'est redistribué.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.