أفضل ممارسات نشر Cisco IOS XR لتوجيه IS-OSPF/IS و BGP

المحتويات

إخلاء المسؤولية

توفر هذه الوثيقة ملخصا رفيع المستوى لبعض التوصيات المعتمدة بشأن أفضل الممارسات لتوجيه IS-OSPF/IS و BGP. لا تمثل هذه التوصيات تصميم تم التحقق من صحة Cisco، كما يلزم توفر العناية والانتباه اللازمين للنشر في أي بيئة تشغيل معينة. يجب قراءتها بالاقتران مع أدلة التكوين والمستندات التقنية للمنتجات ذات الصلة التي تصف بمزيد من التفصيل كيفية تنفيذ توصيات أفضل الممارسات هذه. الغرض من المراجع الواردة في هذا المستند إلى أدلة التكوين والمستندات التقنية لمنتجات معينة هو كأمثلة فقط. ارجع إلى أدلة التكوين والمستندات التقنية الخاصة بالمنتجات الخاصة بك.

المقدمة

يوضح هذا المستند بعض أفضل الممارسات والتوصيات الراسخة لإنشاء شبكات مبسطة وفعالة وقابلة للتطوير تعمل بمنصات توجيه IOS XR. يركز هذا المستند على تقنيات تنفيذ محددة وخيارات دعم الميزات المتوفرة في IOS XR للمساعدة في تخصيص عمليات نشر IS-OSPF/IS و BGP.

تنفيذ OSPF

يعد بروتوكول OSPF، المحدد في RFC 2328، بروتوكول العبارة الداخلية (IGP) المستخدم لتوزيع معلومات التوجيه داخل نظام مستقل واحد. يوفر OSPF العديد من الفوائد مقارنة بالبروتوكولات الأخرى، ولكن يلزم توفر تصميم مناسب لإنشاء شبكة قابلة للتطوير وقابلة لمواجهة الأعطال.

لمزيد من المعلومات حول OSPF، ارجع إلى:

- TechNote على OSPF:
  -9ospf/703-first-path-shortest-https://www.cisco.com/c/en/us/support/docs/ip/open
  html#anc13.1
- دليل التكوين ل OSPF: 00https://www.cisco.com/c/en/us/td/docs/routers/asr90 -r7-software/asr9k/
  ospf.html-x/implementing76-asr9000-cg-routing-routing/configuration/guide/b/6
- مرجع الأوامر:
  -https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/711x/routing/configuration/guide/b
  ospf.html?dtid=osscdc000283-x/implementing711-asr9000-cg-routing

المفاهيم الرئيسية

- التدرج الهرمي: يعد نموذج الشبكة الهرمي أداة مفيدة عالية المستوى لتصميم بنية أساسية موثوقة للشبكة، ويساعد على تقسيم مشاكل تصميم الشبكة المعقدة إلى مناطق أصغر حجما وأكثر قابلية للإدارة.
- قابلية إضافة وحدات أخرى: من خلال تقسيم وظائف متعددة على شبكة إلى وحدات، يكون تصميم الشبكة أسهل بكثير. قامت Cisco بتحديد العديد من الوحدات النمطية، بما في ذلك مجمع المؤسسة، وكتلة الخدمات، ومركز البيانات، وحافة الإنترنت.
- المرونة: تتوفر الشبكة في كل من الظروف العادية وغير العادية. تتضمن الظروف العادية تدفقات حركة المرور المتوقعة والأنماط والأحداث المجدولة مثل نوافذ الصيانة. تتضمن الظروف غير العادية حالات تعطل الأجهزة أو البرامج وحمولات حركة المرور الشديدة والأنماط غير العادية لحركة المرور وأحداث رفض الخدمة (DoS) والأحداث الأخرى المخطط لها أو غير المخطط لها.
- المرونة: القدرة على تعديل أجزاء من الشبكة أو إضافة خدمات جديدة أو زيادة السعة دون الحاجة إلى إجراء ترقية كبيرة للرافع الشوكية (أي إستبدال الأجهزة الرئيسية).

كأفضل ممارسة عامة، يجب أن يراعي نشر الشبكة "فسحة بين دعامتين" الشبكة لاحتواء المسارات داخل حدود ومسارات محددة ذات صلة ومتطلبة بواسطة الموجهات داخل مجال لإعادة التوجيه. يساعد الاستخدام الفعال لمساحات OSPF على تقليل عدد إعلانات حالة الارتباط (LSAs) وحركة مرور البيانات العامة الأخرى التي يتم إرسالها عبر الشبكة. إحدى ميزات إنشاء تسلسل هيكلي هي أن هذا النهج يساعد على التأكد من أن حجم قاعدة بيانات المخطط التي سيحتاج كل موجه إلى صيانتها قابل للإدارة ويتطابق مع ملف تعريف الذاكرة للموجه.

مجال OSPF وإعادة توزيع BGP

لقد صمم OSPF لحمل بضعة آلاف من الطرق فقط. على مستوى عال، "مناطق" OSPF هي أقسام من شبكة يعرف فيها أي موجه إمكانية التوجيه لكل موجه آخر في المنطقة. وهذا يسمح بالتقارب السريع عندما يكون هناك أي جهاز به مشكلة، ولكن على حساب انخفاض قابلية التطوير. على هذا النحو، يتم إستخدام OSPF في مركز مزود خدمة لتوفير الاتصال على المستوى الأساسي بين جميع الأجهزة الأساسية، ويتم تكوين جميع الأجهزة الأساسية داخل نفس منطقة OSPF. هذا تصميم قياسي لشبكة "أساسية".

وعلى النقيض من ذلك، تم تصميم بروتوكول بوابة الحدود (BGP) لحمل مسارات أكبر كثيرا من معظم بروتوكولات العبارة الداخلية، مثل بروتوكول فتح أقصر مسار أولا (OSPF). المخاطر المرتبطة بإعادة توزيع مسارات BGP إلى بروتوكول العبارة الداخلية مثل OSPF. إذا تطلب موفر الخدمة إعادة توزيع مسارات BGP إلى مجال IGP لأي حالة إستخدام، فيجب إدارة هذا بواسطة موفر الخدمة مع التصفية المناسبة في موجهات حدود النظام الذاتي (ASBR) ومع حماية الحمل الزائد التي تم تكوينها على الموجه المستقبل. إذا تم إلغاء تصفية إعادة توزيع BGP في إطار OSPF، فسوف يبدأ كل جهاز من أجهزة OSPF في بروتوكول ASBR في تلقي مسارات تتجاوز قدرته على المعالجة في نفس الوقت. على سبيل المثال، ستسمح موجهات Cisco IOS XR بإعادة توزيع مسارات BGP 10000 فقط إلى OSPF بشكل افتراضي.

عند إعادة توزيع مسارات BGP إلى بروتوكول العبارة الداخلية، من الممكن أن تستلم جميع الموجهات داخل مجال بروتوكول العبارة الداخلية هذه المسارات، حسب تصميم بروتوكول العبارة الداخلية. وفقا لبروتوكول OSPF RFC، يجب توزيع أي مسار خارجي تتم إعادة توزيعه على OSPF على جميع الموجهات في منطقة OSPF.

إدارة إعادة التوزيع إلى بروتوكول العبارة الداخلية

وكأفضل ممارسة عامة، لا ينبغي إعادة التوزيع إلا بطريقة متأنية ومخطط لها عندما لا تكون هناك خيارات أخرى لتعلم الطرق التي يمكن الوصول إليها والتي ستوفرها وظيفة إعادة التوزيع.

كممارسة عامة، يجب عليك:

- تجنب إعادة التوزيع
- تجنب نقل المسارات في مجال IGP
- تنفيذ بروتوكول بوابة الحدود (BGP) لتوفير إمكانية الوصول الخارجية
- أستخدم بروتوكول العبارة الداخلية لحمل معلومات الخطوة التالية فقط، على سبيل المثال، الاسترجاع 0

قيود إعادة توزيع مسار OSPF

تتم إدارة نطاق البادئات التي تتم إعادة توزيعها من BGP إلى PFOS باستخدام تكوين حماية الحمل الزائد (lsa-max). هذه هي الحماية الوحيدة ضد تسريب عدد كبير من المسارات إلى مجال OSPF. في حالة إعادة التوزيع في منطقة OSPF واحدة، يجب عليك تنفيذ طبقات متعددة من الحماية ضد إعادة توزيع المسار.

فيما يلي بعض الخيارات المتاحة للحماية من إعادة توزيع الطرق:

- تصفية إعادة التوزيع باستخدام قائمة التحكم في الوصول (ACL)
- حد إعادة التوزيع - إعداد عمومي لمنع إعادة توزيع أكثر من عدد محدد من المسارات. في حالة إزالة عامل التصفية، يكون حد إعادة التوزيع العام هو خط الدفاع الثاني وسيحمي المراكز.
- تكوينات LSA-Max على جميع الأجهزة في منطقة OSPF - في حالة فشل أوجه الحماية المذكورة في الطلقات الواردة أعلاه، فإنها تفرض على الموجهات المتلقية رفض فئات LSA الزائدة الواردة.

حماية الحمل الزائد لقاعدة بيانات حالة إرتباط OSPF

توفر ميزة "حماية الحمل الزائد لقاعدة بيانات حالة إرتباط OSPF" آلية على مستوى OSPF لتحديد عدد إعلانات حالة الارتباط غير المنشأة ذاتيا لعملية OSPF معينة. إذا تم تكوين الموجهات الأخرى في الشبكة بشكل غير صحيح، فقد تقوم بإنشاء حجم كبير من LSAs، على سبيل المثال، لإعادة توزيع أعداد كبيرة من البادئات في OSPF. تساعد آلية الحماية هذه في منع الموجهات من تلقي العديد من LSAs وبالتالي تواجه نقصا في وحدة المعالجة المركزية (CPU) والذاكرة.

سلوك الميزة

فيما يلي كيفية تصرف الميزة:

- عند تمكين هذه الميزة، يحتفظ الموجه بعدد من جميع إعلانات LSA التي تم تلقيها (غير المنشأة ذاتيا).
- عند الوصول إلى قيمة الحد الذي تم تكوينه، يتم تسجيل رسالة خطأ.
- عند تجاوز الحد الأقصى للعدد المستلم من LSAs، يتوقف الموجه عن قبول LSAs الجديدة.

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

دول الاتحاد الأوروبي

إذا كان عدد إعلانات LSA المستلمة أعلى من الحد الأقصى للعدد الذي تم تكوينه بعد دقيقة، فإن عملية OSPF تقوم بإسقاط جميع التجاور وتمسح قاعدة بيانات OSPF. تسمى هذه الحالة **حالة التجاهل**". في هذه الحالة، يتم تجاهل جميع حزم OSPF المستلمة على جميع الواجهات التي تنتمي إلى مثيل OSPF، ولا يتم إنشاء حزم OSPF على الواجهات. تظل عملية OSPF في حالة التجاهل لمدة وقت التجاهل الذي تم تكوينه (الافتراضي هو 5 دقائق). عند انتهاء صلاحية وقت التجاهل، ترجع عملية OSPF إلى العملية العادية وتبني التجاور على جميع الواجهات الخاصة بها.

إذا تجاوز عدد ملفات LSA الحد الأقصى للرقم بمجرد إرجاع مثيل OSPF من حالة التجاهل، فيمكن لمثيل OSPF أن يتأرجح إلى ما لا نهاية بين حالته العادية وحالة التجاهل. لمنع هذا الاهتزاز اللامتناهي، يحسب مثيل OSPF عدد المرات التي كان فيها في حالة التجاهل. يسمى هذا العداد **count-ignore**. إذا تجاوز igno-ignore (default count 5-recount) القيمة التي تم تكوينها، يبقى مثيل OSPF بشكل دائم في حالة التجاهل.

يجب عليك إصدار الأمر **ospf clear** لإرجاع مثيل OSPF إلى حالته العادية. تتم إعادة تعيين **عدد التجاهل** إلى صفر إذا لم يتجاوز عدد LSA الحد الأقصى للرقم مرة أخرى أثناء الوقت الذي تم تكوينه بواسطة الكلمة الأساسية time-reset.

إذا كنت تستخدم الكلمة الأساسية **only-warning** ، فإن مثيل OSPF لا يدخل أبدا في حالة التجاهل. عندما يتجاوز عدد LSA الحد الأقصى للرقم، تسجل عملية OSPF رسالة خطأ، ويستمر مثيل OSPF في عملية الحالة العادية الخاصة به.

لا توجد قيمة افتراضية ل lsa-max. يتم التحقق من الحد فقط إذا تم تكوينه بشكل محدد.

بمجرد تكوين lsa-max، يمكن أن تحتوي المعلمات الأخرى على قيم افتراضية:

- تحذير ٪-log-to-threshold الافتراضي - 75٪
- قيمة count-ignore الافتراضية - 5
- مدة التجاهل الافتراضية في الدقائق - 5 دقائق
- الوقت الافتراضي لإعادة ضبط عدد التجاهل - 10 دقائق

هنا مثال على التنفيذ الذي يوضح كيفية تكوين مثيل OSPF لقبول 12000 LSAs غير المنشأة ذاتيا و 1000 LSAs غير المنشأة ذاتيا في VRF V1.

```
تكوين #RP/0/RSP0/CPU0:Router
RP/0/RSP0/CPU0:Router(config)# Router ospf 0
lsa 12000-ospf)# max-RP/0/RSP0/CPU0:router(config
ospf)# vrf v1-rp/0/RSP0/cpu0:router(config
lsa 1000-ospf)# max-RP/0/RSP0/CPU0:router(config
```

يوضح المثال التالي كيفية عرض الحالة الحالية لمثيل OSPF.

```
يعرض #RP/0/RSP0/CPU0:Router الأمر ospf 0
    عملية التوجيه "ospf 0" بالمعرف 10.0.0.2
    تم تعطيل NSR (التوجيه المستمر)
    يدعم مسارات TOS(TOS0) الأحادية فقط
    يدعم LSA المعتم
    هو موجه حدود المنطقة
    الحد الأقصى لعدد LSA غير المنشأة ذاتيا المسموح به 12000
        الرقم الحالي ل LSA 1 غير المنشأة ذاتيا
        حد رسالة التحذير 75٪
        وقت التجاهل 5 دقائق، وقت إعادة الضبط 10 دقائق
        عدد التجاهل المسموح به 5، عدد التجاهل الحالي 0
```

تنفيذ BGP

تجعل عائلات عناوين BGP بروتوكول توجيه BGP بروتوكول توجيه "متعدد البروتوكولات". يوصى بشدة بفهم كيفية إستخدام عائلات العناوين لإنشاء مخططات قابلة للتطوير تتسم بسهولة التطبيق والإدارة. باستخدام عائلات العناوين، يمكن أن يقوم المشغل بإنشاء طوبولوجيا مختلفة لتقنيات مختلفة، على سبيل المثال، EVPN والبث المتعدد وما إلى ذلك.

لمزيد من المعلومات حول BGP، راجع دليل تكوين BGP:
bgp.html-x/implementing76-ncs5500-cg-bgp-om/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/bhttps://www.cisco.c

BGP و BFD

يعتبر تقارب BGP في شبكة مزود الخدمة أمرا مهما لتلبية توقعات العملاء لبناء شبكات مرنة وقادرة على مواجهة الأعطال. بشكل افتراضي، يحتوي BGP على مؤقت Keepalive من 60 ثانية وموقت إحتجاز من 180 ثانية. وكل هذا يعني أن بروتوكول BGP سيكون بطيئا للغاية في التقارب ما لم تكن هناك مساعدة متوفرة من بروتوكولات الدعم. إعادة توجيه BFD ثنائي الإتجاه (BFD) هو أحد هذه البروتوكولات التي تم تصميمها لمساعدة بروتوكولات العميل على التقارب بشكل أسرع. باستخدام BFD، يمكن للبروتوكولات التقارب في ثوان.

معلومات إضافية

■ يوفر هذا الدليل معلومات عن التصورات والتكوين الخاصة ب BFD:
-x/implementing76-ncs5500-cg-routing-https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/76x/b
bfd.html
■ يقدم هذا التقرير الرسمي طريقة عرض مرتكزة على مزود الخدمة حول التجميع السريع باستخدام BFD على موجهات سلسلة NCS 5500
من Cisco ونظام تقارب الشبكات من Cisco: -and-ncs5500-on-architecture-utorials/bfdhttps://xrdocs.io/ncs5500/t
/ncs500
■ لمزيد من التعمق في إستخدام BFD على واجهات الحزمة وتنفيذ Multipath و BFD MultiHop، ارجع إلى https://xrdocs.io/
المستودع.

اكتشاف النظير البطيء ل BGP

النظير البطيء هو نظير لا يمكنه مجاراة معدل إنشاء الموجه لرسائل التحديث على مدى فترة طويلة (حسب ترتيب الدقائق) في مجموعة تحديث. عند وجود نظير بطيء في مجموعة تحديث، يتم إنشاء عدد من التحديثات المنسقة المعلقة. عند الوصول إلى حد ذاكرة التخزين المؤقت، لا توجد لدى المجموعة أية حصص نسبية أخرى لتنسيق رسائل جديدة. لكي يتم تنسيق رسالة جديدة، يجب إرسال بعض الرسائل الموجودة باستخدام النظير البطيء ثم إزالتها من ذاكرة التخزين المؤقت. لن يكون لدى باقي أعضاء المجموعة التي تكون أسرع من النظير البطيء وأكملت إرسال الرسائل المنسقة أي شيء جديد لإرساله، على الرغم من احتمال وجود شبكات BGP معدلة حديثا في انتظار الإعلان عنها أو سحبها. هذا التأثير لحظر تنسيق كافة النظراء في مجموعة عندما يكون أحد النظراء بطيئا في إستهلاك التحديثات هو مشكلة "النظير البطيء".

الأحداث التي تتسبب في حدوث طفرة كبيرة في جدول BGP (مثل برامج إعادة التوجيه الخاصة بالاتصال) يمكن أن تتسبب في إرتفاع معدل إنشاء التحديث بشكل موجز. ولا يعتبر النظير الذي يتخلف مؤقتا خلال هذه الأحداث ولكنه يتعافى بسرعة بعد وقوع الحدث نظيرا بطيئا. ولكي يتم تمييز النظير على أنه بطيء، يجب أن يكون غير قادر على مواكبة متوسط معدل التحديثات التي تم إنشاؤها خلال فترة أطول (في غضون دقائق قليلة).

قد يكون نظير BGP البطيء بسبب:

■ فقدان الحزمة أو حركة مرور البيانات العالية على الارتباط بالنظير.
■ يمكن تحميل نظير BGP بشدة فيما يتعلق بوحدة المعالجة المركزية، وبالتالي لا يمكن خدمة اتصال TCP بالسرعة المطلوبة.
■ في هذه الحالة، يجب التحقق من إمكانية أجهزة النظام الأساسي والحمولة المعروضة.
■ مشاكل الإنتاجية مع اتصال BGP
■ لمزيد من المعلومات حول اكتشاف النظير البطيء ل BGP، راجع:
-plementingx/im76-ncs5500-cg-bgp-https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b
bgp.html#concept_ir5_j4w_p4b

فيما يلي بعض التخفيفات وأفضل الممارسات لإدارة عمليات النظير البطيء:

■ جودة الخدمة الشاملة، والتي تحجز النطاق الترددي لحركة مرور مستوى التحكم في BGP أثناء الازدحام.
■ إستخدام قيم MTU / MSS الصحيحة والمناسبة باستخدام إعدادات PMTUD BGP و/أو MSS TCP.
■ أستخدم الأجهزة الصحيحة وقلل عدد المسارات فيما يتعلق بالأجهزة.

يتم تمكين اكتشاف النظير البطيء بشكل افتراضي في Cisco IOS XR الذي يبدأ من الإصدار 7.1.2. النظراء البطيئون هم النظراء الذين يتباطئون في تلقي تحديثات BGP الواردة ومعالجتها والتعرف على التحديثات الخاصة بالمرسل. إذا كان النظير البطيء يشارك في مجموعة التحديث نفسها مثل النظراء الآخرين، فقد يؤدي ذلك إلى إبطاء عملية التحديث لجميع النظراء. في هذا الإصدار، عند اكتشاف IOS XR لنظير بطيء، سيقوم بإنشاء syslog الذي يحتوي على تفاصيل حول النظير المحدد.

تقارب سريع باستخدام تقارب مستقل لبادئات BGP

بالنسبة لبادئات BGP، يتم تحقيق التقارب السريع باستخدام التقارب المستقل لبادئات BGP (PIC)، حيث يقوم BGP بحساب أفضل مسار بديل وأفضل مسار أساسي ويثبت كلا المسارين في جدول التوجيه كمسارات أساسية ومسارات إحتياطية.

إذا أصبح بعد الخطوة التالية BGP غير قابل للوصول، فإن BGP يتحول على الفور إلى المسار البديل باستخدام BGP PIC بدلا من إعادة حساب المسار بعد الفشل.

إذا كان EHop Remote P-BGP Next حيا، ولكن هناك فشل مسار، يقوم LFA FRR-IGP TI بمعالجة إعادة التقارب السريع للمسار البديل، ويقوم BGP بتحديث الخطوة التالية ل IGP ل PE البعيد.

يتم تكوين بطاقة BGP PIC ضمن مجموعة عناوين VRF للتقارب السريع لبادئات VPN إذا أصبح PE البعيد غير قابل للوصول إليه.

لمزيد من المعلومات حول تقارب بادئات BGP المستقل، راجع:
-x/bgp76-ncs5500-cg-bgp-https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b
pic.html

أمان BGP باستخدام FlowSpec BGP

BGP FlowSpec، باختصار، هي ميزة تسمح لك باستلام مواصفات تدفق حركة مرور IPv4/IPv6 (المصدر X والوجهة Y والبروتوكول UDP والمنفذ المصدر A وما إلى ذلك) والإجراءات التي يلزم إتخاذها على حركة المرور هذه (مثل الإسقاط أو الشرطة أو إعادة التوجيه) عبر تحديث BGP.

داخل تحديث BGP، يتم تمثيل معايير مطابقة FlowSpec بواسطة BGP NLRI، وتمثل مجتمعات BGP الموسعة الإجراءات.

تستند هذه الميزة إلى RFC 5575 ويمكن إستخدامها للمساعدة في تخفيف هجمات رفض الخدمة. عند مهاجمة مضيف معين داخل شبكة، يمكننا إرسال تحديث FlowSpec إلى الموجهات الطرفية بحيث يمكن تنظيم حركة مرور الهجمات أو إسقاطها، أو حتى إعادة توجيهها إلى مكان آخر، ربما إلى جهاز يمكنه تنظيف حركة المرور (تصفية حركة مرور "سيئة" وإعادة توجيه حركة مرور "جيدة" فقط إلى المضيف المتضرر).

بمجرد إستلام FlowSpec بواسطة موجه وبرمجة في بطاقات الخط القابلة للتطبيق، فإن أي منافذ L3 نشطة على بطاقات الخط تلك ستبدأ معالجة حركة مرور الدخول وفقا لقواعد FlowSpec.

لمزيد من المعلومات حول تنفيذ BGP FlowSpec، راجع:

- التقرير الرسمي عن تدفق BGP: /ncs5500-on-flowspec-https://xrdocs.io/ncs5500/tutorials/bgp
- دليل تكوين BGP: -ncs5500-cg-bgp-https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b
bxq_h2b_bgp.html#concept_uqv-x/implementing76

ميزة الحد الأقصى لبادئة BGP

تكون ميزة الحد الأقصى للبادئة مفيدة عندما يبدأ الموجه، عند تغيير السياسة الصادرة في موقع التجميع عن بعد، في إستقبال بادئات أكثر من موارد موجه نظير التي يمكن معالجتها ولكنه أيضا يحمي الموارد أو نظراء BGP الداخليين حيث سيتم إعادة توجيه هذه البادئات الخارجية. وقد تكون هذه التكاليف الإضافية المترتبة على الموارد معطلة للنظام.

تفرض ميزة الحد الأقصى لبادئة BGP حدا أقصى على عدد البادئات التي يتم استقبالها من أحد الجيران لعائلة عنوان معينة. بشكل افتراضي، عند تجاوز عدد البادئات المستلمة، الحد الأقصى للعدد الذي تم تكوينه، ترسل جلسة عمل BGP إعلام إيقاف التنفيذ إلى المجاور ويتم إنهاء الجلسة. سيؤدي عبور عائلة عنوان واحدة للحد الأقصى من البادئة إلى انهيار جلسة BGP بالكامل، مما يؤثر على جميع عائلات العناوين الأخرى التي تم تمكينها في جلسة BGP هذه.

تستخدم هذه الميزة عادة لنظراء BGP الخارجيين لحماية البنية الأساسية الداخلية لمزود الخدمة. وهو يخدم كحماية لمنع إستنزاف موارد الموجه الذي يمكن أن يكون ناجما عن تكوين غير صحيح، إما محليا أو على المجاور البعيد. يوصى بشدة بتكوين الحد الأقصى للبادئة لحمايتها من التكوينات غير الصحيحة المحلية أو البعيدة التي يمكن أن تؤدي إلى تشغيل فيضان جدول المسار. يحمي هذا أيضا ضد هجمات إلغاء تجميع البادئة.

يجب تمكين تكوين الحد الأقصى لبادئة BGP بشكل صريح على جميع موجهات eBGP لتحديد عدد البادئات التي يجب أن تتلقاها من جار معين، سواء كان العميل أو نظير AS. يوصى بأن يقوم المشغل بتكوين هامش مقبول للبادئات الإضافية التي قد يتمكن النظام من الحفاظ عليها بعد إجراء تقييم دقيق لذاكرة النظام المتوفرة. ينبغي ملاحظة أنه لا يوجد حجم واحد يناسب جميع التكوين الذي قد يتم تطبيقه على جميع الموجهات ويجب تعديل الحد بعناية استنادا إلى دور الجهاز في الشبكة. على سبيل المثال، إذا تم تكوين الحد الأقصى لبادئة BGP على جيران IBGP، فيجب أن تكون قيمة الحد الأقصى للبادئة أقل على الجيران الذين تم تكوينهم على عاكس المسار مقابل تلك الخاصة بالجيران التي تم تكوينها على عملاء عاكس المسار. يقوم عاكس المسار بتجميع البادئات الواردة من موجهات نظير متعددة ثم إعادة الإعلان عن الجدول الكامل إلى عملاء عاكس المسار. لذلك، سيعلن عاكس المسار عن المزيد من البادئات لعملائه مقارنة بما يتلقاه من كل نظير فردي. وبالمثل، قد يقوم موجه نظير أيضا بإعادة الإعلان عن المزيد من البادئات نحو عاكس المسار مقارنة بما يتلقاه من كل نظير خارجي فردي.

وخلاصة القول، يوصى بمراجعة الإجراء المناسب وتكوينه بعناية لاتخاذه عند الوصول إلى الحد الأقصى للبادئة على جهاز الإنتاج. يتم وصف بعض خصائص خيارات أمر الحد الأقصى للبادئة كما يلي:

- عندما يتم تكوين جلسة BGP بشكل صريح باستخدام ميزة الحد الأقصى للبادئة بدون أي كلمات أساسية إضافية (مثل التحذير فقط أو إعادة التشغيل المحتملة)، سيتم تقسيم جلسة العمل كسلوك افتراضي. والإجراء الافتراضي لجلسة عمل النظير التي يتم تخفيضها دون إسترداد تلقائي قد يؤدي إلى انقطاع طويل داخل القلب.

```
%BGP-routing-5-adjchange_detail: جار 10.10.10.10 أسفل - إعلام BGP مستلم،
الحد الأقصى لعدد البادئات التي تم الوصول إليها (VRF: افتراضي؛ AFI/SAFI: 1/1،
128/1، 4/2، 128/2، 133/1، 133/2) (as: 65000)
%BGP-Routing-5-NBR_NSR_DISABLED_STANDBY: تم تعطيل NSR على المجاور
10.10.10.10 على RP الاحتياطي بسبب تجاوز النظير للحد الأقصى للبادئة (VRF:
الافتراضي)
```

- يؤدي تكوين خيار تجاهل المسارات الإضافية إلى إسقاط جميع البادئات الزائدة التي يتم استقبالها من المجاور أعلى حد الحد الأقصى للقيمة الذي تم تكوينه. لا ينتج عن هذا الإسقاط رفرفة جلسة العمل. تتضمن فوائد هذا الخيار تحديد إستخدام ذاكرة عملية BGP ووقف رفرفة الأقران ضمن الشبكة الأساسية. ومع ذلك، قد يؤدي ذلك إلى حلقات إعادة التوجيه للبادئات التي يتم التخلص منها حيث قد تصبح إدخالات إعادة التوجيه غير متناسقة بين الموجهات في الشبكة.
- عند إستخدام مسار إضافي، يتم تطبيق قيمة الحد الأقصى للبادئة التي تم تكوينها على المسارات بدلا من البادئات حيث يتم عمل NLRI من البادئة وسمات المسار. راجع مرجع الأوامر التالي للحصول على مزيد من المعلومات:

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

التوصية: قم بتقييم الخيارات التالية بعناية عند تكوين أمر الحد الأقصى للبادئة:

- **لم يتم تعريف أي إجراء صريح**: سيقوم الموجه بإنزال الجلسة وإبقاء علاقة BGP المجاورة معطلة حتى يقوم المشغل بمسح جلسة BGP يدويا. [أمر مسح BGP]
- **إعادة تشغيل [interval-time]**: قم بإنزال جلسة العمل وحاول إعادة التشغيل التلقائية لجلسة BGP بشكل دوري بعد مؤقت تم تكوينه. وسوف ينجح هذا إذا توقف النظير البعيد عن الإعلان عن البادئات الزائدة وإلا فإن جلسة BGP سوف تنزل مرة أخرى (وبالتالي تتسبب في عدم إستقرار دوري).
- **تجاهل المسارات الإضافية**: باستخدام خيار تجاهل المسارات الإضافية، تبقى جلسة BGP عالية لكن البادئات التي تتجاوز حد الحد الأقصى للبادئة يتم تجاهلها. لا يؤثر هذا الخيار على عائلات العناوين الأخرى حيث لم يتم الوصول إلى الحد الأقصى للبادئة ويضمن عدم استنفاد الموارد المحلية ولكن قد يؤدي ذلك إلى حلقات إعادة التوجيه للبادئات التي يتم التخلص منها. لاحظ أنه لا يمكن أن يتواجد خيار تجاهل المسارات الإضافية مع مقبض إعادة التكوين البسيط.
- **تحذير فقط**: سجل تحذير فقط عندما يتم الوصول إلى الحد حتى يتمكن المشغل من إتخاذ إجراءات يدوية لمسح الشرط.

للحصول على مزيد من المعلومات، يرجى الرجوع إلى دليل تكوين التوجيه على النحو التالي:

-r7-sr9000/software/asr9khttps://www.cisco.com/c/en/us/td/docs/routers/a
-x/implementing73-asr9000-cg-routing-routing/configuration/guide/b/3
BGP.html#concept_5AF38064B1D044B7B5F439C10BCF9808

أفضل الممارسات والتوصيات

تقدم القائمة التالية لمحة عامة عن أفضل الممارسات والتوصيات العامة، المدرجة في قائمة غير محددة الترتيب:

■ تدقيق الشبكة من أجل الصحة العامة للنظام. ابدأ بتدقيق التكوين وانتقل بشكل تسلسلي من تكوينات الواجهة إلى التوجيه والخدمات.
■ وضع إستراتيجية للمراقبة. على الرغم من أن بروتوكول SNMP هو ممارسة قياسية، فكر في نشر تقنيات وصفية أكثر فعالية باستخدام بيانات تتبع الدفق. راجع التقرير الرسمي التالي للحصول على توصيات أفضل الممارسات حول تنفيذ القياس عن بعد على موجه IOS XR:
https://xrdocs.io/telemetry/

بروتوكول أقصر مسار أولاً (OSPF)

فيما يلي أفضل الممارسات والتوصيات العامة المتعلقة ب OSPF:

■ تنفيذ تلخيص المسارات للمسارات الداخلية ل OSPF.
■ قم بتكوين الموجه-id بشكل صريح داخل OSPF كأحد عناوين الاسترجاع التي تم تمكين OSPF عليها.
■ تصميم شبكة هرمية لتحديد شبكات LSA داخل منطقة ما ل OSPF. احتفظ بعدد وحدات التحكم في الوصول (ABR) لمنطقة داخل نطاق معقول (~3 إلى 4).
■ تطبيق تكوين "الحد الأقصى ل OSPF" ل OSPF، أو ما يعادله، لتحديد LSAs في قاعدة البيانات للاستخدام الفعال لذاكرة النظام.
■ تحديد الحد الأقصى لعدد المسارات التي يمكن توزيعها من BGP إلى OSPF. في XR-IOS، الحد الافتراضي هو 10 كيلو.
■ إستخدام سياسة المسار (RPL) لإعادة توزيع الموجهات إلى OSPF.

- تلخيص المسارات المشتركة بين المناطق والطرق الخارجية من النوع 5 حيثما ينطبق ذلك.
- إستخدام المصادقة عند الضرورة.
- أستخدم NSF و NSR دائما.
- شكلت redistribution بيصفي في المصدر بدلا من الغاية.
- إستخدام الواجهة الخاملة حيثما ينطبق ذلك.
- يجب أن يحمل OSPF فقط مسارات الاسترجاع وواجهة الموجه - إزالة أي إعادة توزيع أخرى لبروتوكول BGP إلى OSPF.
- النظر في نقل كل مركز رئيسي إلى منطقته.
- إستخدام BFD للكشف السريع عن الأعطال مقابل مؤقتات بروتوكول التوجيه القوية.
- لا تستخدم الأمر ignore-mtu قدر الإمكان.
- جرب إستخدام مزامنة LDP-IGP في بيئة MPLS لتجنب إرسال حركة مرور البيانات على مسار غير مسمى.
- ضع في حسبانك المقياس ضمن حدود النظام الأساسي المعتمد (عدد البادئات وعدد التسميات وبروتوكول تصحيح الأخطاء (ECMP) وعدد المناطق وما إلى ذلك).
- تجنب إعادة التوزيع المتبادل عند نقاط متعددة.
- قم بتكوين المسافة الإدارية حتى يتم الوصول إلى كل بادئة أصلية إلى كل بروتوكول أو عملية عبر بروتوكول أو عملية المجال المطابقة.
- التحكم في البادئات (باستخدام المسافة أو مجموعة قائمة البادئات) حتى لا يتم الإعلان عن نفس البادئة مرة أخرى إلى المجال الأصلي.
- على الرغم من أن معرف عملية OSPF له أهمية محلية للموجه، فمن المستحسن أن يكون له نفس معرف العملية لجميع الموجهات في مجال OSPF نفسه. وهذا يحسن تناسق التكوين وييسر مهام التكوين التلقائي.
- عند تكوين OSPF للبيئات المحورية، قم بتصميم مناطق OSPF بعدد أقل من الموجهات.
- قم بتكوين النطاق الترددي المرجعي للتكلفة التلقائية ل OSPF من خلال مجال OSPF إلى أعلى إرتباط للنطاق الترددي في الشبكة.
- من منظور تصميمي، نوصي بتنفيذ نظير IGP مع المجالات تحت نفس عناصر التحكم الإدارية أو التشغيلية للمساعدة في تجنب تحديث IGP غير المخطط له أو الدخيلة الذي يتم نشره عبر الشبكة. يجب أن يتيح ذلك قابلية صيانة أفضل وسهولة أستكشاف الأخطاء وإصلاحها في حالة حدوث أخطاء. في حال كان مجال IGP الكبير ضرورة عمل، خطط على إستخدام BGP في تلك الحالات للحد من عدد المسارات في مجال شبكة IGP.
- إذا كنت بحاجة إلى اتصال MPLS شامل، فاستمر في إستخدام التسلسل الهرمي/التقسيم وخيارات الاستخدام مثل BGP LU-RFC3107 أو حساب المسار بين المجالات عبر PCE أو حدد إعادة التوزيع/التسرب باستخدام السياسة كحل أخير.
- يمكن إستخدام ميزة التحكم في أول مسار لبروتوكول فتح أقصر مسار أولا OSPF لتكوين جدولة SPF في فواصل زمنية بالمللي ثانية واحتمال تأخير حسابات SPF أثناء عدم إستقرار الشبكة.
- تتيح ميزة تحديد أولوية بادئات OSPF SPF للمسؤول إمكانية تجميع البادئات المهمة بشكل أسرع أثناء تثبيت المسار.

IS-IS

وفيما يلي أفضل الممارسات والتوصيات العامة لنظام المعلومات الإدارية المتكامل:

- إذا قمت بتشغيل شبكة مسطحة أحادية المستوى، فكر في المقياس. تكوين جميع الموجهات على أنها L2 فقط. يكون الموجه L2-L1 بشكل افتراضي، ويتم تمكين تسريب معلومات التوجيه من L1 إلى L2 بشكل افتراضي. وقد يؤدي ذلك إلى قيام جميع الموجهات بتسريب جميع مسارات L1 إلى L2، وبالتالي تفتيت قاعدة بيانات حالة الارتباط.
- إذا قمت بتشغيل شبكة متعددة المستويات (مناطق متعددة)، فتأكد من أن مخطط الطبقة الثالثة يتبع تسلسل ISIS الهرمي. لا تقم بإنشاء روابط خلفية بين مساحات L1.
- إذا قمت بتشغيل شبكة متعددة المستويات (مناطق متعددة)، فتأكد من توصيل موجهات L1 و L2 عبر كل من مناطق L1 و L2. لا يتطلب ذلك إتصالات مادية أو ظاهرية متعددة فيما بينهم، قم بتشغيل الرابط بين موجهات L1 و L2 كدائرة L1/L2.
- إذا قمت بتشغيل شبكة متعددة المستويات (مناطق متعددة)، فعليك تلخيص ما يمكن تلخيصه - على سبيل المثال، في حالة MPLS، يلزم نشر إسترجاع موجهات PE بين المناطق، ولكن عناوين إرتباط البنية الأساسية لا يتم ذلك.
- قم بإنشاء خطة العنونة المناسبة واتباعها إن أمكن. الذي يسمح بالتلخيص ويساعد على التطوير.
- تعيين مدة صلاحية LSP إلى 18 ساعة كحد أقصى.
- تجنب إعادة التوزيع بأي وسيلة. إن إعادة التوزيع معقدة وتحتاج إلى أن تتم إدارتها يدويا لتجنب حلقات التوجيه. أستخدم التصميم متعدد المناطق/المستوى إن أمكن.
- إذا كان يجب عليك إستخدام إعادة التوزيع، أستخدم تمييز المسار أثناء إعادة التوزيع وتصفية "list in-distribute" استنادا إلى العلامات لإدارتها. التلخيص أثناء إعادة التوزيع إن أمكن.
- قم بتكوين الواجهات ك "من نقطة إلى نقطة" كلما أمكن. وهذا يحسن من أداء البروتوكول وقابليته للتطوير.
- لا تستعملوا تنظيم "الدولة الإسلامية" في طوبولوجيا مدموجة للغاية. لا تتصرف بروتوكولات حالة الارتباط بشكل جيد في البيئات ذات الشبكات العالية.
- قم بتكوين قياس افتراضي عالي في الوضع الفرعي لعنوان family-ISIS. وهذا يمنع الارتباطات التي تمت إضافتها حديثا من جذب حركة المرور إذا تم تكوينها دون قصد بدون قياس.
- قم بتكوين "تغيير تسجيل التجاور" للمساعدة في أستكشاف أخطاء الاتصال وإصلاحها.

■ أستخدم "style wide-Metric" ضمن الوضع الفرعي لعنوان IPv4 لعائلة ISIS. المقاييس الضيقة ليست مفيدة جدا ولا تدعم ميزات مثل توجيه المقطع أو algo-Flex.
■ إذا كنت تستخدم LFA-MPLS TI-SR فتذكر إضافة "IPv4 غير المرقمة eng Loopback0-MPLS traffic" إلى التكوين للسماح ل ISIS بتخصيص أنفاق البيانات عند الحاجة.
■ أترك التكوينات الافتراضية "interval-gen-LSP" و"interval-SPF" ما لم تكن متأكدا من أن التقارب الأصلي الأسرع مطلوب. مع لا يعد التقارب الأصلي ل LFA-TI بهذا القدر من الأهمية، نظرا لأن التحويل السريع سيعالج تغييرات المخطط الأحادي في 50 مللي ثانية أو أقل.
■ إذا قمت بتعديل "tervalin-gen-lsp" أو "interval-spf" لا تستخدم وقتا أوليا للتأخير أقصر من 50 مللي ثانية.
■ في معظم الحالات، فإن "بت التحميل الزائد للمجموعة" هو إختيار أفضل من "القياس الأقصى" لأنه تغيير ذري مدعوم بإعادة التوجيه السريع.
■ إستخدام المصادقة المشفرة ل hello) asswordp-Hellos) وlsp) password-LSPs). توفر سلاسل المفاتيح أقصى قدر من المرونة ويمكنها
إستيعاب عمليات إعادة توجيه المفاتيح المستمرة.
■ تكوين "NSF Cisco" للمصادقة المستمرة لعمليات إعادة تشغيل عملية ISIS وتثبيت SMU. وعلى الرغم من الاسم، فإن هذا يوفر إمكانية تشغيل أفضل مع الموردين الآخرين من "nsf ietf".
■ على نظام أساسي مزود ب RPs مزدوجة، قم أيضا بتكوين "NSR" لمعالجة محولات RP.
■ أستخدم القوالب "group" و"group-apply" لتكوين أقسام التكوين المتكررة. وهذا أقل عرضة للخطأ وأسهل في التغيير إذا لزم الأمر.
■ في شبكة متعددة المستويات، فكر بعناية فيما إذا كنت بحاجة إلى إستخدام "النشر" لتسريب البادئات من المستوى 2 إلى المستوى 1. وهذا يمكن أن يحد من قابلية التطوير، وغالبا ما يكون المسار الافتراضي للمستوى 1 الذي توفره وحدة بت المرفقة كافيا.
■ إذا كنت تستخدم مثيلات ISIS متعددة في نفس VRF، فاعتبر تكوين قيم "مسافة" فريدة لها. وهذا من شأنه أن يجعل تثبيت المسار في RIB أكثر تحديدا إذا كان لكل مسار إلى البادئة نفسها.
■ إستخدام بروتوكول BFD لاكتشاف الارتباط المنسدل السريع. مع قيام BFD بتوفير هذه الوظيفة، يمكن أن تتم زيادة الفاصل الزمني الخاص ب ISIS بأمان لتحسين قابلية التطوير.

BGP

فيما يلي أفضل الممارسات والتوصيات العامة لبروتوكول بوابة الحدود:

■ أستخدم NSR و NSF / إعادة تشغيل تتسم بالسلاسة مع مؤقتات مضبوطة بعناية بناء على المقياس المتوقع.
■ قم بتكوين BGP باستخدام واجهة الاسترجاع "دائما up"، وليس الواجهة المادية لتقسيم IBGP.
■ لا تقم بإعادة توزيع مسارات بروتوكول بوابة الحدود (BGP) (كبيرة الحجم) إلى بروتوكول العبارة الداخلية (IGP) (منخفضة الحجم نسبيا) والعكس صحيح من دون قائمة تكرار حلقي (RPL) مناسبة، مما يحد من عدد المسارات التي تتم إعادة توزيعها من بروتوكول بوابة الحدود (BGP) إلى بروتوكول العبارة الداخلية (OSPF/ISIS).
■ قد يؤدي تنفيذ BGP لإعادة توزيع IGP بدون سياسة مناسبة تم إختبارها بشكل جيد (ACL) إلى إستهلاك المورد (الذاكرة) على الموجه.
■ إستخدام المسارات الموجزة في بروتوكول بوابة الحدود (BGP) لتقليل حجم جدول التوجيه واستخدام الذاكرة. قم بتجميع المسارات بالموجز فقط حيثما يكون ذلك منطقيا
■ إستخدام تصفية المسار للإعلان عن المسارات المستقبلة بكفاءة، وخاصة في بروتوكول BGP.
■ نوصي باستخدام عاكس المسار (RR) والكونفدرالية لتوسيع الشبكة.
■ بعض اعتبارات تصميم عاكس المسار هي:
■ يزيد قياس المسار بناء على عدد العملاء/غير العملاء.
■ في وحدات الاستجابة السريعة (RR) الهرمية، أستخدم معرف المجموعة نفسه في نفس المستوى (RR المتكرر) لمنع التكرار والتوسع.
■ تحكم في MTU ضمن مسار BGP أو أستخدم بروتوكول PMTUD لضبط BGP MSS تلقائيا.
■ إستخدام مؤقتات BFD أو ضبط مؤقتات BGP للكشف عن الأخطاء بشكل أسرع.
■ يكون قياس BGP وفقا للتكوين وحالة الاستخدام، ولا يوجد حجم واحد يناسب الجميع. عليك أن تكون لديك فكرة جيدة عن:
■ مسار المسار
— مقياس المسار (مع إعادة تهيئة ناعمة، سيزيد)
— مقياس السمة
■ إذا تم تكوين المسار الإضافي، فإنه يستهلك المزيد من الذاكرة.
■ الفهم الدقيق لسياسات مجاورة BGP:
— قد تتسبب وحدة all-pass (وخاصة في موجه حدودي) في حدوث تلف عندما ترتفع سعة الذاكرة.
— أستخدم تكوينات النهج التي ستتجنب تطابقات التعبير العادي في RPL.
■ باستخدام NSR، سيستخدم RP الاحتياطي ذاكرة افتراضية أكثر بنسبة 30٪ من الذاكرة النشطة. ضع هذا في الاعتبار إذا كان هناك إستعداد.
■ انتبه إلى مصدات مستمرة في عدد كبير من الطرق (مصدات الإصدار). قد يؤدي ذلك إلى الاحتفاظ بذاكرة إنشاء التحديث في علامة مائية عالية.

■ حماية الأقران باستخدام مقبض الحد الأقصى للبادئة.
■ إستخدام معلمات تأخير الخطوة التالية عند بدء التشغيل وفقا لأهداف النطاق والتلاقي.
■ في تصميم الشبكة، حاول تجنب الخصائص الجديدة. تؤدي السمات الفريدة إلى عدم كفاءة التعبئة مما يؤدي إلى إجراء المزيد من تحديثات BGP.
■ يمكن أن يؤدي تكوين مسارات متعددة عبر الشبكة إلى حلقات إعادة التوجيه. الاستخدام بعناية.
■ إستخدام نهج الجدول لتجنب تثبيت المسار إلى RIB إذا لم يكن RR مضمنا-RR (لا يوجد نهج الخطوة التالية الذاتي)

مراقبة ذاكرة النظام لعمليات التوجيه

لا يحتوي أي جهاز على موارد لا نهائية - إذا قمنا بإرسال عدد لا نهائي من الموجهات إلى جهاز ما، فيجب أن يختار الجهاز كيفية فشله. ستحاول الموجهات خدمة جميع المسارات حتى يتم استنفاد حدود الذاكرة، وقد يؤدي ذلك إلى فشل جميع بروتوكولات التوجيه وعملياتها.

تحتوي كل عملية في الموجه الرئيسي على "RLIMIT" معرف. "RLIMIT" هي مقدار ذاكرة النظام المسموح لكل عملية باستهلاكها.

يصف هذا القسم بعض التقنيات القياسية لمراقبة ذاكرة النظام المستخدمة من قبل عملية BGP والتحقق منها.

ذاكرة العملية

إظهار مقدار الذاكرة المستهلكة بواسطة عملية ما.

```
show#5501-RP/0/RP0/CPU0:NCS بروتوكول ذاكرة
العملية الديناميكية لمكدس البيانات (كيلوبايت) لنص JID (كيلوبايت)
- - - - - -
  lspv_server 3462 136 368300 896 1150
parser_server 32775 136 1877872 316 380
          bgp 31703 136 2425220 2092 1084
     ipV4_rib 31691 160 1566272 1056 1260
     ipV6_rib 28962 152 1161960 1304 1262
         PIM6 21555 136 1479984 4276 1277
ema_serversch 21372 136 227388 80 1301
          PIM 20743 136 1677244 4272 1276
 invmgr_proxy 20647 136 692436 124 250
   l2vpn_mgr 20133 136 2072976 4540 1294
   sdr_invmgr 19408 136 692476 212 211
statsd_manager_g 17454 136 679752 4 1257
```

يتم تخصيص حد أقصى للذاكرة المسموح باستهلاكها لكل عملية. هذا يعرف على أنه الحد الأقصى.

```
show#5501-RP/0/RP0/CPU0:NCS تفاصيل ذاكرة البروتوكول
Tot-TOT PHY-Limit SHM-JID Text Stack Dynamic Dyn العملية الديناميكية لحزمة بيانات
==========================================================================
==========================================================================
==========================================================================
==========================================================================
==========
  lspv_server 1150 896K 359M 136K 32M 1024M 18M 24M الخادم
          M 2368M 136K 30M 7447M 43M 69M BGP2 1084
     M 1529M 160K 30M 8192M 38M 52M ipV4_rib1 1260
```

```
الطراز 380 Parser_Server316 94M 25M 2048M 29M 136K 1833M K
                                  M 1262 31 22M 8192M 28M 152K 1134M IPv6_rib1M
                                  M 1277 PIM64 41M 18M 1024M 21M 136K 1445M
                                  K 1301 Schema_server80 33M 5M 300M 20M 136K 222M
                                  M 1276 مليو 1637M41M 19M 1024M 20M 136K
                                  K 250 invmgr_proxy124 31M 9M 1024M 20M 136K 676M
                                  M 1294 l2vpn_mgr4 66M 48M 1861M 19M 136K 2024M
                                  K 211 sdr_invmgr212 29M 9M 300M 18M 136K 676M
                                  K 1257 Statsd_manager_g4 39M 20M 2048M 17M 136K 663M
                                  K 288 Statsd_manager_l4 33M 15M 2048M 16M 136K 534M
                                  □ ...
```

أفضل مستهلكي الذاكرة□

```
show#5501-RP/0/RP0/CPU0:NCS مستهلكون متفوقون للذاكرة
########################################################################################
########################
أفضل مستهلكات الذاكرة على CPU0/0/0 (في APR/13/15:54:12/2022)
########################################################################################
########################
إجمالي (ميغابايت) كومة (ميغابايت) العملية المشتركة (ميغابايت)
FIA_DRIVER 826 492.82 321 3469
fib_mgr 175 1094.43 155 4091
124 □68spp 130 9 3456
dpa_port_mapper 108 1.12 105 4063
Packet 104 1.36 101 3457
l2fib_mgr 86 52.01 71 5097
bfd_agent 78 6.66 66 4147
ETH_EA 66 4.76 61 4958
Optics_Driver 62 141.23 22 4131
الإصدار السادس من بروتوكول الإنترنت وفقا للمعيار 4090_الثاني 55 4.13 49
########################################################################################
########################
أفضل مستهلكي الذاكرة على rp0/cpu0/0 (عند xx/mmm/hh:mm:ss20)
########################################################################################
########################
إجمالي (ميغابايت) كومة (ميغابايت) العملية المشتركة (ميغابايت)
114 □62spp 119 9 3581
dpa_port_mapper 106 2.75 102 4352
```

```
fib_mgr 99 7.71 90 4494
الحزمة 3582 96 48 1 94
Parser_Server 95 64.27 25 3684
te_control 71 15.06 55 8144
70bgp  8980، 61 27 44
l2vpn_mgr 67 23.64 48 7674
mibd_interface 65 35.28 28 8376
GSP 65 15.75 48 3608
```

إجمالي الذاكرة - المستخدمة والمتوفرة

تحتوي مكونات النظام على مقدار ثابت من الذاكرة المتوفرة.

show#5501-rp/0/rp0/cpu0:NCS الذاكرة موجز موقع الكل

العقدة0_0_CPU0

```
–
الذاكرة الفعلية: إجمالي 8192 م (6172 م متوفرة)
ذاكرة التطبيق: 8192 م (6172 م متوفر)
الصورة: 4 م (ذاكرة مؤقتة: 0 م)
محجوز: 0m، m0، IOMem: 0m، flashFSYS: 0m
إجمالي النافذة المشتركة: 226 مترا
عقدة: node0_rp0_cpu0
–
الذاكرة الفعلية: إجمالي 18432 م (يتوفر 15344 م)
ذاكرة التطبيق: M18432 (يتوفر M15344)
الصورة: 4 م (ذاكرة مؤقتة: 0 م)
محجوز: 0m، m0، IOMem: 0m، flashFSYS: 0m
إجمالي النافذة المشتركة: 181 مترا
```

يوفر نافذة الذاكرة المشتركة معلومات عن عمليات تخصيص الذاكرة المشتركة على النظام.

show#5501-RP/0/RP0/CPU0:NCS الذاكرة ملخص موقع RP0/CPU0/0

```
عقدة: node0_rp0_cpu0
–
الذاكرة الفعلية: إجمالي 18432 م (يتوفر 15344 م)
ذاكرة التطبيق: M18432 (يتوفر M15344)
الصورة: 4 م (ذاكرة مؤقتة: 0 م)
محجوز: 0m، m0، IOMem: 0m، flashFSYS: 0m
إطار مشترك غير متزامن-app-1: k243.328
K3.328 :12-Shared Window Soasync
```

...
إعادة كتابة النافذة المشتركة-db: 272.164K
نافذة مشتركة l2fib_brg_shm: 139.758K
ndow im_rules: 384.211KShared Wi
شبكة النافذة المشتركة_svr_shm: 44.272M
بروتوكول SPP للنافذة المشتركة: M86.387
نافذة مشتركة im_db: 1.306m
مجموع النافذة المشتركة: 180.969 م
الذاكرة المخصصة: G2.337
نص البرنامج: 993 ر 127
بيانات البرنامج: g64.479
مجموعة البرامج: g2.034
ذاكرة الوصول العشوائي (RAM) للنظام: 1932735283218432) M)
المجموع المستخدم: 3088 مترا (3238002688)
مستخدم خاص: 00) m)
مستخدم 3238002688) shared: 3088m)

يمكنك التحقق من عمليات المشارك باستخدام نافذة ذاكرة مشتركة.

sh shmwin spp#5501-RP/0/RP0/CPU0:NCS قائمة المشاركين
بيانات الإطار "spp":
–
قائمة المشاركين الحاليين:-
فهرس JID الخاص ب Name
SPP 3581 113 0
Packet 3582 345 1
ncd 4362 432 2
نتيو 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
...
SNMP 8171 1002 44
بروتوكول فتح أقصر مسار أولا 8417 1030 45
MPLS_LDP 7678 1292 46

BGP 8980 1084 47

CDP 9295 337 48

1-sh shmwin soasync#5501-RP/0/RP0/CPU0:NCS قائمة المشاركين

بيانات الإطار "1-Soasync":

–

قائمة المشاركين الحاليين:-

فهرس JID الخاص ب Name

بروتوكول 0 168 5584 TCP

BGP 8980 1084

مراقبة الموارد وأجهزة المراقبة

تتم مراقبة إستخدام الذاكرة من خلال مراقبة النظام في cXR ومع Resmon في eXR.

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

–node0_rp0_cpu0 –

معلومات الذاكرة:

الذاكرة الفعلية: 18432.0 ميجابايت

ذاكرة حرة: 15348.0 ميجابايت

حالة الذاكرة: عادي

#5501-rp/0/rp0/cpu0:NCS

show#5501-RP/0/RP0/CPU0:NCS موقع إعدادات حد الذاكرة الطرفية 0/RP0/CPU0

–node0_rp0_cpu0 –

حدود الذاكرة الافتراضية:

صغير: 1843 ميجابايت - 10٪

شديد: 1474 ميجابايت - 8٪

هام: 921.599 ميجابايت - 5٪

معلومات الذاكرة:

الذاكرة الفعلية: 18432.0 ميجابايت

ذاكرة حرة: 15340.0 ميجابايت

حالة الذاكرة: عادي

#5501-rp/0/rp0/cpu0:NCS

config)#watchdog)5501-RP/0/RP0/CPU0:NCS حد الذاكرة الثانوية ؟

<5-40> إستهلاك الذاكرة بالنسبة المئوية

يطبع تحذير إذا تم تجاوز الحدود.

RP/0/RP0/cpu0:فبراير 17:23:30:21.663 :[425]resmon :UTC٪HA-HA_WD-4-HA_ALARM-MEMORY: تم تجاوز حد الذاكرة: صغير الحجم مع ذاكرة خالية سعة 1840.000 ميجابايت. الحالة السابقة: عادي

RP/0/RP0/CPU0:17 شباط 23:30:21.664 [25UTC: resmon[4 ٪HA_WD-HA-6-
TOP_MEMORY_USERS_INFO: أفضل 5 مستهلكين لذاكرة النظام (1884160 كيلو بايت مجانا):

RP/0/RP0/cpu0:فبراير 17 23:30:21.664 UTC: resmon[425]: ٪HA_WD-HA-6-
top_MEMORY_USER_INFO: 0 اسم العملية: [0]bgp، pid: 7861، إستخدام كومة الذاكرة المؤقتة: 12207392
كيلوبايت.

RP/0/RP0/CPU0:17 شباط 23:30:21.664 UTC: resmon[425]: ٪HA_WD-HA-6-
TOP_MEMORY_USER_INFO: 1 اسم العملية: [0]ipV4_rib، pid: 4726، إستخدام كومة الذاكرة المؤقتة:
708784 كيلوبايت.

RP/0/RP0/CPU0:17 شباط 23:30:21.664 UTC: resmon[425]: ٪HA_WD-HA-6-
top_MEMORY_USER_INFO: 2 اسم العملية: [0]fib_mgr، pid: 3870، إستخدام كومة الذاكرة المؤقتة:
584072 كيلوبايت.

RP/0/RP0/cpu0:17 شباط 23:30:21.664 UTC: resmon[425]: ٪HA_WD-HA-6-
top_MEMORY_USER_INFO: 3 اسم العملية: [0]netconf، pid: 9260، إستخدام كومة الذاكرة المؤقتة:
553352 كيلو بايت.

RP/0/RP0/cpu0:17 شباط 23:30:21.664 UTC: resmon[425]: ٪HA_WD-HA-6-
top_MEMORY_USER_INFO: 4 اسم العملية: [0]netio، pid: 3655، إستخدام كومة الذاكرة المؤقتة: 253556
كيلو بايت.

MEMORY_ALARM-4-HA_WD-HA٪ :[LC/0/3/CPU0:Mar 8 05:48:58.414 PST: resmon[172: حد
الذاكرة تم تجاوزه: قوي مع مساحة خالية تبلغ 600.182 ميجابايت. الحالة السابقة: عادي

-4-HA_WD-HA٪LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]:
TOP_MEMORY_USERS_WARNING: أفضل 5 مستهلكين لذاكرة النظام (624654 كيلوبايت مجانا):

-4-HA_WD-HA٪LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]:
TOP_MEMORY_USER_WARNING: 0 اسم العملية: [0]fib_mgr، pid: 5375، إستخدام كومة الذاكرة المؤقتة
1014064 كيلوبايت.

-4-HA_WD-HA٪LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]:
ING: 1TOP_MEMORY_USER_WARN اسم العملية: [0]ipV4_mfwd_partner، pid: 5324، إستخدام كومة
الذاكرة المؤقتة 185596 كيلوبايت.

-4-HA_WD-HA٪LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]:
TOP_MEMORY_USER_WARNING: 2 اسم العملية: [0]nfsvr، pid: 8357، إستخدام كومة الذاكرة المؤقتة
183692 كيلوبايت.

-4-HA_WD-HA٪LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]:
TOP_MEMORY_USER_WARNING: 3 اسم العملية: [0]fia_Driver، pid: 3542، إستخدام كومة الذاكرة المؤقتة
177552 كيلوبايت.

-4-HA_WD-HA٪LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]:
P_MEMORY_USER_WARNING: 4TO اسم العملية: [0]npu_driver، pid: 3525، إستخدام كومة الذاكرة المؤقتة
177156 كيلوبايت.

قد تتخذ بعض العمليات إجراءات محددة استنادا إلى حالة ذاكرة الجهاز المراقب. على سبيل المثال، يقوم BGP بما يلي:

- في الحالة الثانوية، يتوقف BGP عن تربية أقران جدد
- في هذه الحالة الشديدة، يعمل بروتوكول بوابة الحدود (BGP) على خفض عدد النظراء تدريجيا.
- في حالة حرجة، يتم إيقاف تشغيل عملية BGP.

يمكن تكوين العمليات للتسجيل في إعلامات حالة الذاكرة.

إظهار المراقبة أو العملية القائمة على الوعي

يمكن للمستخدمين تعطيل إيقاف تشغيل العملية تلقائيا بسبب مهلة المراقبة.

شاشة إعادة تشغيل وحدة الذاكرة - تعطيل الخنزير

أين يمكن العثور على مزيد من المعلومات؟

- مستودع مدونات وتقارير Cisco IOS XR (xrdocs.io)
  - تصميم البنية الأساسية: https://xrdocs.io/design/blogs/latest-hld-fabric-core : يناقش هذا التقرير الرسمي الاتجاهات الحديثة والتطور في الشبكات الأساسية.
  - تصميم Fabric Peering: https://xrdocs.io/design/blogs/latest-hld-fabric-peering : يقدم هذا التقرير الرسمي نظرة عامة شاملة على التحديات والتوصيات المتعلقة بأفضل الممارسات لتصميم Peering مع التركيز على تبسيط الشبكة.
- مرجع دليل التكوين: تنفيذ BGP https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp-cg-bgp-x/b710-ncs5500-x/implementing-bgp.html

تحسينات الميزات

عزل موجه حدود النظام الذاتي والتحكم في التجاور لعمليات تجاوز LSA	تم تقديمه في 7.10.1 على موجهات المنافذ الثابتة NCS 5500: موجهات NCS 5700 ذات المنافذ الثابتة في الشبكة التي تستخدم موجه حدود النظام الذاتي (ASBR) والموجهات الأخرى، أنت الآن متأكد من تدفق حركة المرور دون انقطاع حتى إذا كان ASBR يقوم بإنشاء LSAs التي تتجاوز الحد الذي قمت بتكوينه. وقد تم جعل هذا ممكنا حيث يمكنك الآن عزل ASBRs والتحكم أيضا في مدة التجاور في مرحلة Exchange أو التحميل. ومن خلال عزل بروتوكول تحليل العناوين (ASBR) عن جيرانه المباشرين، يمكن أن تستمر مخطط الشبكة المتبقي في العمل دون انقطاع، مما يمنع بفعالية أي تأثير ضار على تدفق حركة المرور. ويبسط هذا النهج أيضا عملية الإنعاش، لأن التدخل اليدوي لا يكون ضروريا إلا للجيران المباشرين لموجهات التحويل المحوسب. تقدم هذه الميزة التغييرات التالية: **CLI:** • **الحد الأقصى-خارجي-lsa** • **مؤقت التبادل** **نموذج بيانات يانغ:** • `cfg.yang-ospf-IPV4-XR-IOS-Cisco` • `er.yangop-ospf-IPV4-XR-IOS-Cisco` • `cfg.yang-ospf-router-um-XR-IOS-Cisco` (راجع GitHub، متصفح نماذج بيانات YANG)
إعادة إنشاء جلسة عمل BGP المجاورة تلقائيا	تم تقديمه في هذا الإصدار على: موجهات المنافذ الثابتة NCS 5500، موجهات المنافذ الثابتة NCS 5700، الموجهات النمطية NCS 5500 (بطاقات الخط NCS 5500، بطاقات الخط NCS 5700 [الوضع: التوافق؛ أصلي]) يمكنك الآن تكوين الموجه لإعادة إنشاء جلسة BGP المجاورة تلقائيا والتي تم تعطيلها بسبب تجاوز حد الحد الأقصى لبادئة BGP. تقدم الميزة التغييرات التالية: CLI • مدة إعادة تشغيل البادئة القصوى نموذج بيانات يانغ: • XPaths جديد لـ ngneighbor.ya-bgp-openConfig(راجع GitHub، متصفح نماذج بيانات YANG)
مواصفات BGP على الواجهات الظاهرية لمجموعة الجسر	تم تقديمه في إصدار 7.10.1 في: الموجهات النمطية NCS 5500 Modular Routers (بطاقات الخط NCS 5700 Line Cards [الوضع: أهلي طبيعي]) يمكنك الآن إستخدام مواصفات BGP بشكل فعال على واجهة مجموعة الجسر الظاهرية (BVI) للاتصال بمجالات البث التي تحتوي على الأجهزة المضيفة، كما في حالة شبكات المؤسسة. يعني هذا الدعم أنه يمكن لعملائك حماية شبكاتهم من تهديدات الشبكة مثل هجمات رفض الخدمة الموزعة (DDoS) الواردة من خلال معرف فئة المورد (BVI).
تجاهل رسالة تحديث BGP الواردة	تم تقديمه في الإصدار 7.10.1 في: موجهات المنافذ الثابتة NCS 5500، موجهات المنافذ الثابتة NCS 5700، الموجهات النمطية NCS 5500 (بطاقات الخط NCS 5500، بطاقات الخط NCS 5700 [الوضع: التوافق؛ أصلي])

	يمكنك الآن تجنب إعادة تعيين جلسة العمل عندما تواجه جلسة BGP أخطاء أثناء تحليل رسالة التحديث التي تم تلقيها. هذا ممكن لأن الميزة تتيح تجاهل رسالة التحديث الواردة كرسالة سحب. CLI: • تحديث في معالجة الأخطاء عند السحب نموذج بيانات يانغ: • XPaths جديدة لـ neighbor.yang-bgp-openConfig (راجع GitHub، متصفح نماذج بيانات YANG)	
إستبعاد تخصيص التسمية للمسارات غير المعلن عنها	تم تقديمه في الإصدار 7.10.1 في: موجهات المنافذ الثابتة NCS 5500، موجهات المنافذ الثابتة NCS 5700، الموجهات النمطية NCS 5500 (بطاقات الخط NCS 5500، بطاقات الخط NCS 5700 [الوضع: التوافق؛ أصلي]) لقد تمكنا من تحسين إدارة مساحة الملصقات واستخدام موارد الأجهزة من خلال جعل تخصيص ملصقات MPLS أكثر مرونة. وتعني هذه المرونة أنه يمكنك الآن تخصيص هذه التسميات لتلك الموجهات فقط التي يتم الإعلان عنها لمسارات الأجهزة النظيرة الخاصة بها، مما يضمن إدارة مساحة التسميات واستخدام موارد الأجهزة بشكل أفضل. وقبل هذا الإصدار، تم تخصيص التسمية بغض النظر عما إذا كانت الموجهات التي يتم الإعلان عنها أم لا. وأدى ذلك إلى عدم كفاءة إستخدام مساحة التسمية.	
حماية جيران eBGP المتصلين مباشرة من خلال معرف LPTS المستند إلى الواجهة	تم تقديمه في الإصدار 7.10.1 في: موجهات المنافذ الثابتة NCS 5500 لقد قمنا بتعزيز أمان الشبكة لجيران بروتوكول eBGP المتصل مباشرة من خلال ضمان إمكانية عبور الحزم التي تنشأ من جيران بروتوكول eBGP المحددين عبر واجهة واحدة فقط، وبالتالي منع انتحال عناوين IP. وقد أصبح هذا ممكنا لأننا أضفنا الآن معرف واجهة لخدمات نقل الحزم المحلية (LPTS). يقوم LPTS بتصفية الحزم وتخطيطها استنادا إلى نوع معدل التدفق الذي تقوم بتكوينه. تقدم الميزة ما يلي: CLI: • binding-secure-BGP lpts نموذج بيانات يانغ: • cfg-bgp-router-um-XR-Cisco IOS (راجع GitHub، متصفح نماذج بيانات YANG)	
تقليل تكرارات تجدولة eBGP على عنوان الاسترجاع على الواجهة الظاهرية لمجموعة الجسر	تم تقديمه في إصدار 7.10.1 في: الموجهات النمطية NCS 5500 Modular Routers (بطاقات الخط NCS 5700 Line Cards [الوضع: أهلي طبيعي]) يمكنك الآن تحقيق تجميع eBGP على واجهات الاسترجاع في الواجهة الظاهرية لمجموعة الجسر (BVI) وتقليل مستوى التكرار من ثلاثة إلى إثنين. وهذا الخفض في مستوى التكرار، والذي يتحقق من خلال إزالة الحاجة إلى إستخدام اسم BVI في تكوين المسارات الثابتة، يسمح بإعادة توجيه الحزم بشكل أسرع والاستفادة بشكل أفضل من موارد الشبكة.	
محاسبة سياسة BGP	تم تقديمه في الإصدار 7.9.1: تدابير محاسبة سياسة بروتوكول العبارة الحدودية (BGP) ويصنف حركة مرور IP التي يتم استقبالها من أقران مختلفين. يمكنك تحديد جميع حركات المرور حسب العميل وإعداد حسابات لها ثم إعداد الفاتورة وفقا لذلك. يتم تمكين محاسبة النهج على أساس واجهة إدخال فردية. باستخدام محاسبة سياسة BGP، يمكنك الآن حساب حركة المرور وفقا للمسار الذي تجتازه. يتم دعم هذه الميزة الآن على الموجهات التي تحتوي على بطاقات الخط المستندة إلى Cisco NC57 مع TCAM الخارجي (eTCAM) وتعمل في الوضع الأصلي. تقدم هذه الميزة التغييرات التالية: • **CLI**: تقدم الميزة الأمر **mode-stats bgppa fib module-hw**. • **نموذج بيانات Yang**: XPaths جديد لـ Cisco-IOS-XR-um-hw-module-profile-cfg.yang (راجع GitHub، متصفح نماذج بيانات ANGY)	
اكتشاف النظير البطيء في مجموعة BGP	تم تقديمه في الإصدار 7.9.1: يقوم نظراء BGP بمعالجة رسائل تحديث BGP الواردة بمعدلات مختلفة. النظير البطيء هو نظير يقوم بمعالجة رسائل تحديث BGP الواردة ببطء شديد على مدى فترة زمنية طويلة مقارنة بالأقران الآخرين في المجموعة الفرعية للتحديث.	

	ان المعالجة البطيئة للنظراء مهمة عندما تتغير المسارات باستمرار على مر فترة طويلة من الوقت. من المهم تنظيف المعلومات القديمة في قائمة الانتظار وإرسال أحدث حالة فقط. من المفيد معرفة ما إذا كان هناك نظير بطيء، وهو ما يشير إلى وجود مشكلة في الشبكة، مثل إزدحام الشبكة المستمر أو أن المستقبل لا يعالج التحديثات في الوقت المناسب، والتي يمكن أن يعالجها مسؤول الشبكة.
تحديد أرقام LSA في قاعدة بيانات حالة إرتباط OSPF	تم تقديمه في الإصدار 7.9.1: تقتصر إعلانات حالة الارتباط غير المنشأة ذاتيا (LSAs) لعملية فتح أقصر مسار أولا (OSPF) على 500000. تمنع آلية الحماية هذه الموجهات من تلقي العديد من LSAs، مما يمنع فشل وحدة المعالجة المركزية (CPU) ونقص الذاكرة، ويتم تمكينها بشكل افتراضي من هذا الإصدار فصاعدا. إذا كان لديك أكثر من 500000 LSAs في شبكتك، فقم بتكوين الأمر **lsa-max** باستخدام مقياس LSA المتوقع قبل الترقية إلى هذا الإصدار أو الأحدث. تعدل هذه الميزة الأوامر التالية: • **إظهار OSPF** لعرض الحد الأقصى لعدد البادئات المعاد توزيعها. • **عرض تفاصيل ملخص قاعدة بيانات OSPF** لعرض عدد عمليات تعداد LSA لكل موجه. • **show ospf database-adv summary** router id لعرض معلومات الموجه و LSAs التي تم استقبالها من موجه خاص.
تحديد الحد الأقصى لبادئات LSA النوع-3 التي تمت إعادة توزيعها في FOSP	تم تقديمه في الإصدار 7.9.1: بشكل افتراضي، يقتصر الحد الأقصى لبادئات LSA 3-Type المعاد توزيعها لعملية OSPF معينة الآن على 100000. تمنع هذه الآلية OSPF من إعادة توزيع عدد كبير من البادئات على هيئة LSAs من النوع 3 وبالتالي منع إستخدام وحدة المعالجة المركزية (CPU) بشكل مرتفع ونقص الذاكرة. بمجرد الوصول إلى عدد البادئات التي تمت إعادة توزيعها أو تجاوز قيمة الحد الفاصل، يتم إنشاء رسالة سجل النظام، ولا يتم إعادة توزيع المزيد من البادئات.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).