مشكلة التحقق من حماية وكيل WSA للتحميل بعد انقطاع الشبكة

المحتويات

مسألة

يذكر Cisco من (WSA) ويب أمان جهاز أن يمكن ،طويلة لفترات الشبكة انقطاع بعد
تم تكوينه لاستخدام وكيل تدفق بيانات من الخادم المحدد من قبل FQDN في إستئناف
حركة مرور البيانات إلى وكيل تدفق بيانات من الخادم وإرسال حركة مرور البيانات مباشرة
"متنحي" على الخادم وكيل بتعليم WSA يقوم عندما المشكلة هذه تظهر .ذلك من بدلا
أثناء انقطاع الشبكة، ولكنه يفشل في التعرف على متى يصبح وكيل الخادم متوفرا مرة
أخرى، حتى بعد إستعادة اتصال الشبكة.

وتشمل الأعراض المحددة التي لوحظت ما يلي:

- = معالجة الأعطال"و FQDN عبر البيانات تدفق وكيل باستخدام WSA تم تكوين
"انتقال مباشر
- انقطاع طويل المدى للشبكة يؤثر على الاتصال بكل من وكيل الخادم وخادم DNS
- بعد إستدراد الشبكة، ال تظهر سجلات الوصول أي عمامات DEFAULT_PARENT، تشير
إلى إستمرار حركة المرور في تجاوز وكيل تدفق البيانات
- تحدث مشكلة على جهاز WSA واحد بينما يعمل جهاز آخر في نفس البيئة بشكل
طبيعي

البيئة

- جهاز أمان الويب (WSA) S-Series من Cisco
- AsyncOS 14.5.2-011 (الإصدار المتأثر)
- الأجهزة: الطراز S695
- وكيل تدفق البيانات الذي تم تكوينه بمواصفات FQDN

- "Go Direct" ك اهنيوكت مت يتلا لاطعألا ةجلاعم
- L2 لوحملل ةيسايسألا ةينبلا عم ةكبشلا ةئيب

رارق

ل حلاصإلا ىلع يوتحي رادصإ ىلإ AsyncOS ةيقرت قيرط نع ةلكشملا هذه لح تم
:هذه AsyncOS تارادصإ يف أطخلا اذه حلاصإ تم .CSCwi13124

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

ةيلاحلا تارادصإلل مؤقت لح

لل خنم مؤقت فيفخت فروتي ،اهتيقرت نكمي ال تلا تائيبلل ةبسنلاب
ضبط الحد الأقصى للمهلة الخاملة للتحقق من بروكسيات تدفق البيانات غير
:المستجيبة

:الوصول إلى واجهة سطر الأوامر (CLI) والانتقال إلى تكوين الوكيل المتقدم :1 ةوطخلا

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

:ةلماخلا ةلهملل ىصقألا دحلا دادعإ ليدعت :2 ةوطخلا

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

ةوطخلا 3: قم بتقليل القيمة القصوى الافتراضية (86400 ثانية/24 ساعة) إلى قيمة
.أصغر لتقليل الوقت بين عمليات التحقق من الصحة

يرفوللا ادرتسالا ةقيرط

إذا كانت المشكلة تؤثر حاليا على تدفق حركة المرور، فيمكن للأمر التالي إستعادة وظائف الوكيل على الفور:

الخطوة 1: الوصول إلى القائمة التشخيصية:

```
CLI > diagnostic > PROXY > kick
```

يؤدي هذا إلى إعادة تشغيل عملية الوكيل واستعادة عمليات وكيل الخادم العادية.

إجراءات التحقق والاختبار

لاختبار ما إذا كانت المشكلة موجودة أو تم حلها بعد الترقية، راجع الخطوات التالية:

الخطوة 1: إنشاء مراقبة خط الأساس

مراقبة سجلات الوصول وسجلات الوكيل لتأكيد إرسال WSA لحركة مرور البيانات إلى وكيل الخادم. تحقق من وصول حركة المرور إلى جانب وكيل الخادم.

الخطوة 2: محاكاة انقطاع الشبكة

بعد تأكيد تدفق حركة المرور العادي إلى وكيل الخادم، قم بقطع اتصال الاتصالات التالية:

- تدفق البيانات من WSA إلى اتصال وكيل
- DNS من WSA إلى اتصال خادم

الخطوة 3: اكتشاف فشل الشاشة

تحقق من سجلات الوكيل وسجلات النظام لهذه المؤشرات:

- "تم الإعلان عن وفاته ..." يمكن لسجل الوكيل إظهار وكيل الخادم
- "اه: تم الوصول إلى الحد الأقصى للفشل في الاستعلام" يمكن لسجل النظام إظهار DNS من خادم ...

الخطوة 4: صيانة الحالة التي تم تعطيلها

من الاتصال بها دون إعادة تشغيل عملية الوكيل، قم بالاحتفاظ بالحالة التي تم قطع الاتصال بها دون إعادة تشغيل عملية الوكيل، قم بالاحتفاظ بالحالة التي تم قطع الاتصال بها من إنشاء الطلبات لمدة 10 ساعات تقريبا. الخطوة 2 واستمر في الخطوة 2.

الخطوة 5: إستعادة الاتصال

2. بعد حوالي 10 ساعات، قم باستعادة الاتصالات التي تم قطع إتصالها في الخطوة 2.

الخطوة 6: مراقبة سلوك الاسترداد

بعد إكمال الخطوة 5، قم بمراقبة سجلات الوصول وسجلات الوكيل دون إعادة تشغيل عملية الوكيل:

- في نظام ثابت: تستأنف حركة المرور المتدفقة من خلال وكيل الخادم، وتظهر سجلات الوكيل انتقالات حالة الصحة العادية
- في الأنظمة المتأثرة: تظهر سجلات الوصول حركة مرور مستمرة في تجاوز وكيل الخادم، ولن تظهر سجلات الوكيل رسائل "كانت صحية، الآن سليمة" وأ "كانت مريضة، الآن مريضة ..."

السبب

يتمثل السبب الجذري لهذه المشكلة في وجود خلل منطقي في آلية التحقق من سلامة وكيل الخادم. عندما يحدد WSA أن وكيل الخادم المكون هو "DEAD" (غير مستجيب)، فإنه يطبق خوارزمية نسخ إحتياطي أسية تضاعف الفاصل الزمني لفحص الصحة بعد كل فشل. يمكن أن يصل هذا الفاصل الزمني إلى 24 ساعة كحد أقصى (86400 ثانية).

تحدث هذه المشكلة عندما يصبح وكيل تدفق البيانات مرة أخرى أثناء إحدى هذه الفواصل الزمنية الموسعة. على الرغم من أن الوكيل قد تعافى ويقوم بالاستجابة بشكل طبيعي، إلا أن WSA لن يقوم بفحص السلامة حتى تنقضي الفترة الزمنية التي تم تكوينها بالكامل. ويمكن أن يؤدي ذلك إلى إستمرار توجيه حركة المرور المباشرة لما يصل إلى 24 ساعة بدلا من إستئناف إستخدام وكيل تدفق البيانات إلى الخادم.

تكوينات WSA حيث يؤثر هذا السلوك على:

- DNS (ليس عنوان IP) ل FQDN/المضيف اسم المضيف بواسطة البث وكيل يتم تحديد
- تم تعيين معالجة الفشل على "مباشرة"
- DNS خادم واتصال خادم وكيل الخادم على كل من الشبكة في المتدة الاضطرابات تؤثر

معرف الخطأ من Cisco: CSCwi13124

المحتوى ذي الصلة

- الدعم الفني والتنزيلات من Cisco

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).