فهم أداء موصل Active Directory

المحتويات

المقدمة

يصف هذا المستند أداء موصل Active Directory ل Umbrella DNS.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Umbrella DNS.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة

يتم إستخدام خدمة Umbrella Connector لمراقبة أحداث تسجيل دخول المستخدم/الكمبيوتر كجزء من تكامل Active Directory ل Umbrella. تقرأ خدمة OpenDNS Connector معلومات تسجيل الدخول من سجل أحداث الأمان لكل وحدة تحكم بمجال AD في موقعها.

في البيئات التي بها معدل كرار مرتفع لأحداث تسجيل دخول المستخدم، من المهم مراجعة إرشادات الأداء هذه. للحصول على تعريف دقيق للمستخدم، يجب أن تكون خدمة Connector قادرة على إستيراد معلومات تسجيل الدخول بسرعة.

الحد الأقصى للأحداث/الثانية

لا يوجد حد ثابت لعدد الأحداث التي يمكن معالجتها. يتم إختبار خدمة Umbrella Connector لدعم 850 حدث متواصل في الثانية عبر جميع وحدات التحكم بالمجال في "موقع". يعتمد هذا على بيئة معملية مخصصة بدون تشغيل برامج الطرف الثالث. قد تختلف نتائج العالم الحقيقي استنادا إلى زمن انتقال الشبكة والاختناقات الأخرى.

يمكن للعملاء تحديد عدد تقريبي من الأحداث/الأحداث من خلال قراءة القسم "أحداث في الثانية" في وقت لاحق من هذه المقالة.

المميزات الجديدة

بالنسبة للعملاء الذين يقومون بعمليات نشر أكبر حجما ويتمتعون بتوتر عال من أحداث تسجيل الدخول، فإن Umbrella تتميز بميزات جديدة قائمة على الأداء. بالإضافة إلى توصيات الأداء العام، يرجى قراءة الإرشادات الحالية في هذه المقالة حول موازنة الأحمال، الاتصال المتوازي، واتصال قارئ سجل الأحداث المباشر.

توصيات الأداء

تحجيم الموصل

يجب أن يحتوي الخادم الذي يقوم بتشغيل خدمة Active Directory Connector على وحدة المعالجة المركزية (CPU) وموارد الذاكرة كما هو محدد في دليل تغيير حجم وثائق Umbrella.

موصل مخصص

على الرغم من إمكانية تثبيت خدمة Connector على وحدة تحكم بالمجال مباشرة، إلا أن Cisco Umbrella توصي بتثبيت الموصل على خادم عضو مخصص لخدمة Connector. يجب ألا يكون لدى خادم العضو هذا أي برنامج آخر من برامج الجهات الخارجية مثبت. اقرأ المزيد حول عملية التثبيت في وثائق Umbrella.

مواقع Umbrella

وحيثما كان ذلك ممكنا، يجب فصل عمليات نشر Umbrella في "مواقع" تقيد المكونات التي تتصل عبر الشبكة. يمكن لخدمة Connector الاتصال بالمكونات الموجودة في موقع Umbrella نفسه فقط. يجب إستخدام هذه الميزة دائما عندما يتم توزيع المستخدمين على مناطق جغرافية كبيرة.

عادة ما يتم إنشاء موقع Umbrella لكل موقع مادي. يجب أن تكون مواقع Umbrella هذه القواعد في وثائق Umbrella.

من شأن الاستخدام المناسب لمواقع Umbrella أن يحسن عملية النشر إلى حد كبير ويمنع اتصال المكونات عبر الشبكة الواسعة.

زمن انتقال الشبكة

يمكن نقل أحداث تسجيل الدخول إلى الموصل عبر الشبكة. من المهم وجود اتصال عالي السرعة بين الموصل وكل وحدة تحكم بالمجال لتقليل التأخيرات المتعلقة بالشبكة. يمكن وضع الموصل في موقع أقرب ما يمكن إلى وحدة (وحدات) التحكم بالمجال والأجهزة الظاهرية.

عدد الموصلات

يلزم توفر موصل واحد لكل موقع Umbrella. من الممكن توفر عدة موصلات في موقع Umbrella، ولكنها مطلوبة فقط لأغراض التكرار. يؤدي وجود موصلات إضافية إلى وضع حمل إضافي على وحدات التحكم بالمجال حيث إنها تقوم بمضاعفة نفس وظيفة الموصل الأول. توصي Umbrella بوجود موصلين كحد أقصى لكل موقع Umbrella.

حجم سجل الأحداث

قد يكون لسجلات أحداث أمان Windows الكبيرة تأثير ضار على أداء عملية WMI هذه. توصي Umbrella بتحديد حجم سجل الأحداث. تم العثور على أفضل أداء مع ملف سجل < 512 ميغابايت، ومع ذلك، يمكن ضبط هذا مع متطلبات الاحتفاظ بالسجل الخاص بك. يمكن ضبط حجم ملف التدوين باستخدام الإرشادات التالية:

1. افتح تطبيق عارض الأحداث (eventVWR.msc).

2. انتقل إلى سجلات Windows > النظام

3. انقر بزر الماوس الأيمن فوق سجل النظام وحدد خصائص.

4. قم بضبط أقصى حجم لملف السجل حسب الرغبة وحدد موافق.

برامج الطرف الثالث

يستخدم عدد من منتجات البرامج الأخرى أيضا WMI التي يمكنها إنشاء إزدحام في WMI على وحدة التحكم بالمجال. ويمكن أن يشمل ذلك ما يلي:

- برنامج تحليلي/أمان من إنتاج جهات خارجية يراقب سجلات الأحداث

- إعادة توجيه سجل أحداث Windows
- جمد SIEM والبرامج الأخرى التي تقارت بسجالت الأحداث

إذا لم يعد أي من اذه البرنامج مطلوبا، يوصى بتعطيله. و الدب من ذلك، يمكن الحد من هذه المشكلة باستخدام الطريقة الموضحة في الملحق "اتصال قارئ سجل الأحداث المباشرة".

برامج مكافحة الفيروسات

إستبعاد اذه المجلد وهذه الملفات التنفيذية من الفحص باستخدام برنامج Anti-Virus:

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\OpenDNSAuditService.exe
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>OpenDNSAuditClient.exe
```

وحدات التحكم الإضافية في المجال

يقوم نظام إعلام WMI الموجود على قوائم انتظار وحدة التحكم بالمجال بمعالجة كل إدخال من الأحداث هذه فيما يتعلق بآلية فعل الحذر WMI. الحذر يرسل إلى مشتركي الإعلام والإرسال إلى الأحداث لسجل. والعكس قبل العاصمة. وعلى هذا النحو، يمكن أن يكون هناك إدراجات في الأداء على وحدة التحكم بالمجال نفسها أثناء إستردادات مدى سرعة إرسال الأحداث.

يمكن الحد من هذه الاختناقات من خلال إضافة وحدات تحكم بالمجال إضافية إلى بيئة AD. تم قياس Umbrella باختبار وحدة تحكم مجال واحدة لما يصل إلى 850 حدث/ثانية.

إستثناءات حساب الخدمة

تقليل عدد عمليات تسجيل الدخول إلى AD التي تم الكشف عنها بواسطة Umbrella عن طريق إستبعاد حسابات الخدمة. يجب إستبعاد هذه الحسابات على أية حال لتطبيق النهج الصحيح. يمكنك أيضا إستبعاد الخوادم والأجهزة الأخرى التي لا تستخدم سياسات AD User ولكن يمكن أن يكون لها حجم كبير من تسجيلات دخول المستخدم.

عقب WMI

الرجاء التأكد من أن وحدة التحكم بالمجال وخادم الموصل محدثان باستخدام أحدث تصحيحات Microsoft. توجد انه أمثلة على الإصلاحات العاجلة التي تحل مشاكل أداء WMI المعروفة.

ذاكرة WMI وحدود المؤشر

تحتوي WMI على حدودها الداخلية والتي يمكن أن تتسبب في حدوث إدراجات. ويقصد اذه على سبيل المثال، يوجد مكثفة. عمليات WMI تنفيذ بشكل خاص عندما تقوم برامج أخرى أيضا بتنفيذ كيفية زيادة هذه الحدود في وثائق Microsoft.

يتعذر على Umbrella تقديم معلومات بشأن الحدود الصحيحة لبيئتك. الرجاء الاتصال ب Microsoft للحصول على المساعدة.

موازنة حمل التيار المباشر

تدعم Umbrella الآن ميزة موازنة الأحمال التي تكون مفيدة عندما يحتوي الموقع على وحدات تحكم بالمجال متعددة وعدد كبير من أحداث تسجيل الدخول. في هذا السيناريو، يتم تثبيت موصلات إضافية، ثم يتم تعيين وحدات التحكم في المجال لموصل عبر مجموعة موازنة الأحمال.

في بيئة بسيطة، فإن موازنة الأحمال سيعمل على النحو التالي:

- يتم تعيين DC_A وDC_B إلى موازنة حمل Group_1 التي تتم معالجتها بواسطة Connector_1.
- يتم تعيين DC_C وDC_D إلى موازنة حمل Group_2 والذي تتم معالجته بواسطة Connector_2.
- لا تزال الأجهزة الظاهرية تتلقى أحداث من كل الموصلين، لذلك لا تزال على دراية بجميع أحداث تسجيل الدخول.
- إذا كان التكرار مطلوبا، يمكن تثبيت موصل إضافي في كل مجموعة لموازنة الحمل.

لهذه الميزة هذه الميزات:

- ويتم تخفيض حمل العمل بشكل كبير في كل موصل. يقوم كل موصل بمعالجة عدد أقل من وحدات التحكم بالمجال.
- وعادة ما يساعد ذلك في السيناريوهات التي يكون فيها هناك تأخير كبير في تلقي الأحداث من مركز البيانات.

يمكن زيادة موازنة الأحمال ليتم إستخدامها في بيئات معقدة متعددة المواقع مع العديد من وحدات التحكم بالمجال. لا يوجد أي دعم لاستخدام موازنة الأحمال بخلاف تثبيت موصلات إضافية.

في هذا الوقت، يجب تمكين ميزة "موازنة الأحمال" بواسطة دعم Umbrella. يرجى الاتصال بدعم Umbrella لمناقشة متطلباتك.

الاتصال المتوازي للجهاز الظاهري

أصبح الموصل الآن قادرا على إرسال أحداث تسجيل الدخول إلى العديد من الأجهزة الظاهرية بالتوازي، بدلا من إستخدام الطريقة التسلسلية الافتراضية. ويكون هذا مفيدا عندما يكون للموقع عدة أجهزة افتراضية وعدد كبير من أحداث تسجيل الدخول.

لهذه الميزة هذه الميزات:

- يقلل أي تأخير في إرسال معلومات تسجيل الدخول عندما تكون هناك أجهزة متعددة. يمكن إرسال حدث إلى جميع الأجهزة في آن واحد.
- يمنع حدوث مشكلة في الاتصال أو انقطاع في جهاز واحد له تأثير الدقل على الأجهزة الأخرى. يتم الاحتفاظ بقائمة انتظار أحداث منفصلة لكل حدث.

يتم الآن تمكين هذه الميزة تلقائيا، ولكن فقط عندما يفي الخادم بتوصيات وحدة المعالجة المركزية والذاكرة .

الإرسال السريع لأحداث تسجيل دخول المستخدم

أصبح الموصل قادرا الآن على إرسال أحداث تسجيل دخول المستخدم في الدفعات، مما يزيد بشكل ملحوظ من عدد الأحداث في الثانية التي يمكن إرسالها إلى الجهاز الظاهري (في الثانية). ويعد هذا الأمر مهما بشكل خاص للموصلات التي تتصل بالأجهزة الافتراضية في المواقع البعيدة.

يمكن تمكين هذه الميزة الآن تلقائيا ولكنها تشتمل على المتطلبات التالية:

- يجب تمكين الاتصال الموازي (أعلاه). يجب أن يفي الخادم بتوصيات وحدة المعالجة المركزية والذاكرة.
- ADC الإصدار 1.8+ مطلوب
- يلزم توفر الإصدار 3.2.0+ من الموصل

اتصال قارئ سجل الأحداث المباشرة

يدعم الإصدار 1.4+ من موصل Active Directory طريقة جديدة للاتصال مباشرة بسجل أحداث الأمان الخاص بوحدة (وحدات) التحكم بالمجال دون إستخدام استعلام WMI. وهذا يقلل من WMI كعنق زجاجة.. وهذا مفيد بشكل خاص في السيناريوهات التي تقوم فيها وحدات التحكم الفردية بالمجال بمعالجة عدد كبير من أحداث تسجيل الدخول.

تعمل هذه الميزة باستخدام آلية سحب حيث يقوم الموصل بسحب الأحداث الجديدة كل 5 ثوان، على هذا النحو يكون هناك تأخير قصير (على سبيل المثال، 5 ثوان) في تحديد المستخدم الصحيح.

هذا التحسين الآن مكنت افتراضيا. لمزيد من المعلومات حول هذه الميزة، يرجى الاتصال بدعم Umbrella.

الأحداث في الثانية

من الممكن حساب عدد الأحداث الأخيرة على وحدة التحكم بالمجال لتقدير الأحداث في الثانية. توصي Umbrella بالقيام بذلك في وقت الذروة:

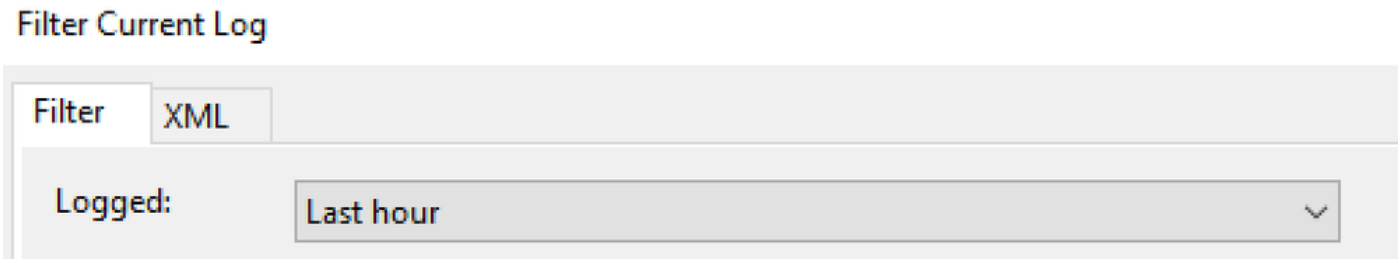
1. افتح تطبيق عارض الأحداث (eventVWR.msc).

2. انتقل إلى سجلات Windows > النظام.

3. حدد تصفية السجل الحالي وحدد الأحداث التي تم تسجيل الدخول إليها في الساعة الأخيرة.

4. حدد OK.

وبمجرد تحميل عامل التصفية، يمكن لسجل الأحداث عرض عدد الأحداث في الساعة الأخيرة. يمكن تقسيم هذه القيمة على 3600 لتقدير الأحداث في الثانية.



360024901511

360024894112

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).