هذه إختبار نشر المقال مع الترخيص كيفية

المقدمة

يصف هذا المستند المنهجية العامة لاستكشاف أخطاء تجربة واجهة المستخدم الرسومية (GUI) لـ APIC البطيئة وإصلاحها.

البدء السريع

غالبا ما يتم العثور على أن مشاكل واجهة المستخدم الرسومية (GUI) لـ APIC البطيئة هي نتيجة لمعدل مرتفع من طلبات API التي تم الحصول عليها من برنامج نصي أو تكامل تمت تطبيقه. يقوم Access.log الخاص بـ APIC بتسجيل كل طلب من طلبات API التي تمت معالجتها. يمكن تحليل Access.log for APIC بسرعة باستخدام البرنامج النصي Access Log Analyzer ضمن مشروع ACI-TAC-Scripts الخاص بمجموعة Github DataCenter.

معلومات أساسية

NGINX - خادم ويب APIC

NGINX هو المسؤول عن نقاط نهاية API المتوفرة على كل APIC. إذا كان NGINX معطلا، فإن DME الخاص به، لذلك من الممكن أن يكون هناك فقط واجهة برمجة تطبيقات فردية واحدة NGINX يمكن أن تواجه مشاكل NGINX إذا كانت واجهة برمجة التطبيقات هذه مستهدفة من قبل أي مستعلم عدواني.

تقوم واجهة برمجة تطبيقات APIC بتنفيذ طلبات API متعددة لملء كل صفحة. بالمثل، تقوم واجهة برمجة تطبيقات Python التي هي مغلفات للبرامج النصية لـ APIC (CLI نمط NXOS) بإنشاء العديد من طلبات API، وتعالج الاستجابة، ثم تخدمها للمستخدم.

السجلات ذات الصلة

اسم ملف السجل	الموقع	أي دعم فني هو في	التعليقات
access.log	/var/log/dme/log	APIC 3of3	ACI ال أعلم، تعطي سطر واحد لكل طلب API
خطأ.log	/var/log/dme/log	APIC 3of3	عدم تطابق ACI، يعرض أخطاء NGINX (متضمنا التقييد)

لوصولا يف مكحتلا ةهجاول ددحم DME تاكرح ليجستب موقي ،(ACI)	APIC 3of3	/var/log/dme/log	nginx.bin.log
يف مكحتلا ةمئاق ددحم" يوتحي لوصولا (ACI)" ىلع تالجس لكشت ةروطخ +اريذحت	APIC 3of3	/var/log/dme/log	nginx.bin.warnplus.log

ةيجهنم

يلوألا لغشملا لزع

؟رثؤي يذلا ام

- لك وأ ،ريثك ،دحاو ؛لوكوتوربلاب ةلومشملا قطانملا اهب رثأتت يتلا قطانملا (أ) APICs؟
- وأ (CLI) رماوألا رطس ةهجاو رماوأ وأ مدختسملا ةهجاو لالخ نم ؛نيبم فيوستلا نيو كليهام؟
- ؟ةئيطب مدختسملا ةهجاوب ةصاخلا رماوألا وأ تاحفصلا يه ام

؟ءطبلا رابتخإ يرجي فيك

- ؟دحاو مدختسمل ةددعتم تاضرعتسم ربع اذه رهظي له
- نم طقف ةيعرف/ةدحاو ةعومجم نع وأ ءطبلا نع غالبإلاب نيمدختسم ةدع موقي له نيمدختسملا؟
- نم ةكبش راسم وأ لثامم يفارغج عقوم يف نوررضتملا نومدختسملا كراشي له APIC؟ ىلإ ضرعتسملا

؟الوا ءطبلا انظحال ىتم

- ؟ارخؤم يصن جمانرب وأ ACI لماكت ةفاضإ تمت له
- ؟ارخؤم ضرعتسملا قحلم نيكمت مت له
- ؟(ACI) لوصولا يف مكحتلا ةمئاق نيوكت يف ثيدح رييغت كانه ناك له

ةحصو NGINX مادختسإ نم ققحتلا

Access.log لاخدإ قيسنت

access.log وه ةزيم ل NGINX، يلاتلابو ،وهف الا ملعأ APIC. يمثل لك رطس بلط HTTP دحاو (APIC). تاقيبطت ةجمرب ةهجاول NGINX مادختسإ مهفل لجسلا اذه عجار .APIC هتقلت يذلا

قيسنت access.log الافتراضي على ACI الإصدار 5.2+:

```
log_format proxy_ip '$remote_addr ($http_x_real_ip) - $remote_user [$time_local]'
                    '"$request" $status $body_bytes_sent '
                    '"$http_referer" "$http_user_agent"';
```

يمثل هذا السطر إدخال access.log عند تنفيذ moquery -c fvTenant:

```
127.0.0.1 (-) - - [07/Apr/2022:20:10:59 +0000]"GET /api/class/fvTenant.xml HTTP/1.1" 200 15863 "-" "Pyt
```

خريطة مثال access.log entry to log_format:

حقل log_format	محتوى من مثال	التعليقات
$remote_addr	127.0.0.1	IP الخاص بالمضيف الذي أرسل هذه الطلب
$http_x_real_ip	-	IP آخر طالب إذا كانت الوكالاء قيد الاستخدام
$remote_user	-	غير مستخدم بشكل عام. تحقق من nginx.bin.log لتعقب المستخدم الذي سجل الدخول لتنفيذ الطلبات
$time_local	07/APR/2022:20:10:59 +000	عند معالجة الطلب
$ طلب	احصل على /api/class/fvTenant.xml http/1.1	أسلوب HTTP (GET، POST، DELETE) و URI
$ حالة	200	رمز حالة إستجابة HTTP
$body_bytes_sent	1586	حجم حمولة الاستجابة
$http_reference	-	-
$http_user_agent	بايثون أورليب	نوع العميل الذي أرسل الطلب

Access.Log Behaviors

إرتفاع معدل الطلبات يشتعل على مدى فترة زمنية طويلة:

- في الثانية في 40 عن تزيد لطلبات المستمرة التشغيل عمليات تتسبب أن يمكن
  واجهة المستخدم بطء
- تحديد المضيف (المضيفين) المسؤول عن الاستعلامات
- قم بتقليل مصدر الاستعلامات أو تعطيله لمعرفة ما إذا كان هذا يؤدي إلى تحسين وقت إستجابة APIC.

استجابات متناسقة بمعدل 4xx أو 5xx:

- إن وجد، عينت الخطأ رسالة من nginx.bin.log

يمكن تحليل Access.log for APIC بسرعة باستخدام البرنامج النصي Access Log Analyzer المخاص بمجموعة Github DataCenter. ضمن مشروع ACI-TAC-Scripts

التحقق من إستخدام مورد NGINX

يمكن التحقق من وحدة المعالجة المركزية (CPU) الخاصة ب NGINX واستخدام الذاكرة باستخدام الأمر top من APIC:

```
<#root>

top - 13:19:47 up 29 days, 2:08, 11 users, load average: 12.24, 11.79, 12.72
Tasks: 785 total, 1 running, 383 sleeping, 0 stopped, 0 zombie
%Cpu(s): 3.5 us, 2.0 sy, 0.0 ni, 94.2 id, 0.1 wa, 0.0 hi, 0.1 si, 0.0 st
KiB Mem : 13141363+total, 50360320 free, 31109680 used, 49943636 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 98279904 avail Mem

PID   USER PR NI VIRT    RES    SHR    S %CPU %MEM TIME+     COMMAND
21495 root 20 0  4393916 3.5g 217624 S

2.6

2.8  759:05.78

nginx.bin
```

يمكن أن يرتبط الاستخدام المرتفع لموارد NGINX مباشرة بارتفاع معدل الطلبات التي تمت معالجتها.

التحقق من المراكز

لا يدعم NGINX نموذجيا للمشكلات الخاصة بواجهة المستخدم الرسومية (GUI) ل APIC. ارجع إلى دليل الدعم الفني لقائمة التحكم في الوصول (ACI) للحصول على خطوات للتحقق من المراكز.

التحقق من زمن انتقال العميل إلى الخادم

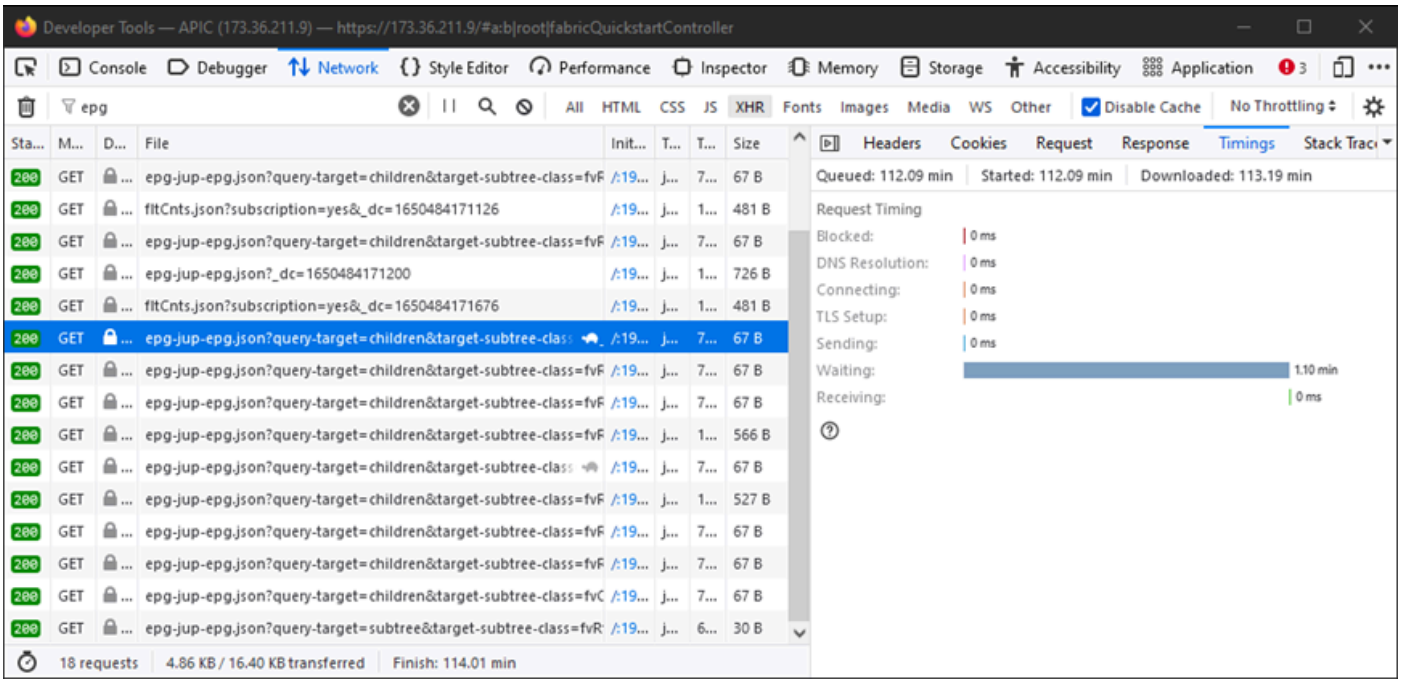
إذا لم يتم العثور على طلبات سريعة ولكن يستمر المستخدم في عرض بطء واجهة المستخدم، فإن المشكلة يمكن أن تكون زمن انتقال العميل (المتصفح) إلى الخادم (APIC).

في هذه السيناريوهات، تحقق من مسار البيانات من المستعرض إلى APIC (المسافة الجغرافية والشبكة الخاصة الظاهرية (VPN)، وما إلى ذلك). إذا أمكن، قم بنشر واختبار الوصول من خادم الانتقال السريع الموجود في نفس المنطقة الجغرافية أو مركز البيانات مثل APICs لعزل. التحقق من الصحة إذا قام المستخدمون الآخرون بعرض قدر مماثل من زمن الوصول.

علامة تبويب شبكة أدوات تطوير المستعرض

يمكن لجميع المستعرضات التحقق من صحة طلبات HTTP واستجاباتها من خلال مجموعة أدوات تطوير المستعرض الخاصة بها، وعادة ما تكون ضمن علامة تبويب الشبكة.

يمكن إستخدام هذه الأداة للتحقق من مقدار الوقت المستغرق لكل مرحلة من الطلبات المستمدة من المستعرض كما هو موضح في الصورة.



مثال على المستعرض الذي ينتظر 1.1 دقيقة لكي يستجيب APIC

تحسينات لصفحات واجهة مستخدم معينة

صفحة مجموعة النهج:

معرف تصحيح الأخطاء من Cisco CSCvx14621 - يتم تحميل واجهة المستخدم الرسومية (GUI) "البنية" ل APIC بطء على سياسات IPG في علامة التبويب.

الواجهة الموجودة ضمن صفحة المخزون:

معرف تصحيح الأخطاء من Cisco CSCvx90048 - الحمل الأولي من "الطبقة 1 تشكيل الواجهة

المادية" علامة التبويب التشغيلية طويل/يحفز على "تجميد".

توصيات عامة للعميل > زمن انتقال الخادم

تتيح بعض المستعرضات، مثل Firefox، المزيد من إتصالات الويب لكل مضيف بشكل افتراضي.

- التحقق مما إذا كان هذا الإعداد قابلا للتكوين على إصدار المستعرض المستخدم
- هذا الأمر أكثر أهمية للصفحات متعددة الاستعلامات، مثل صفحة مجموعة النهج

تعمل الشبكة الخاصة الظاهرية (VPN) والمسافة التي تصل إلى APIC على زيادة بطء واجهة المستخدم الإجمالي نظرا لطلبات مستعرض العميل ووقت سفر إستجابة APIC. يقلل مربع الانتقال المحلي جغرافيا إلى APICs بشكل كبير المتصفح إلى أوقات السفر APIC.

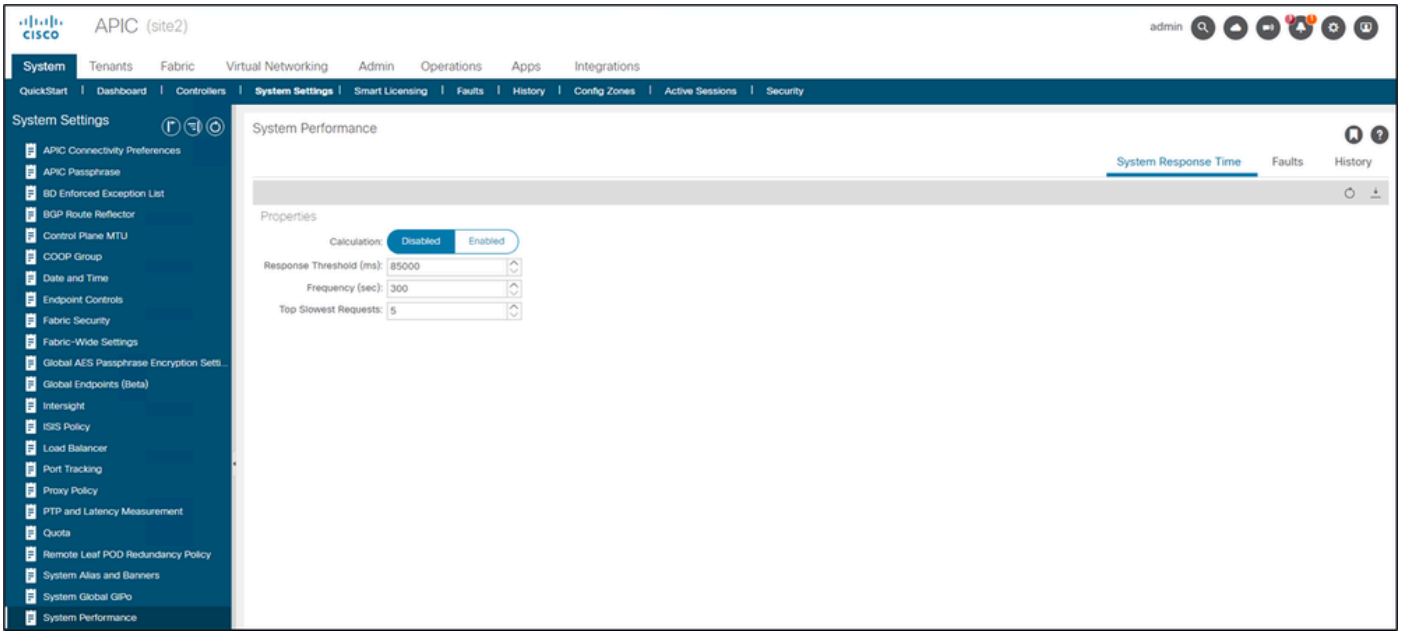
التحقق من طلبات الويب الطويلة

إذا كان خادم ويب (NGINX على APIC) يعالج كمية كبيرة من طلبات الويب الطويلة، فقد يؤثر ذلك على أداء الطلبات الأخرى المتلقاة بالتوازي.

ويصدق هذا بوجه خاص على النظم التي لديها قواعد بيانات موزعة، مثل APICs. قد يتطلب طلب واجهة برمجة تطبيقات (API) واحدة طلبات وعمليات بحث إضافية يتم إرسالها إلى عقد أخرى في البنية مما قد يؤدي إلى أوقات إستجابة أطول بشكل متوقع. يمكن أن يؤدي اندفاع طلبات الويب الطويلة هذه في إطار زمني صغير إلى مضاعفة مقدار المواراد المطلوبة وإلى أوقات إستجابة أطول بشكل غير متوقع. علاوة على ذلك، يمكن للطلبات المتلقاة بعد ذلك انقضاء المهلة (90 ثانية) مما يؤدي إلى سلوك غير متوقع للنظام من منظور المستخدم.

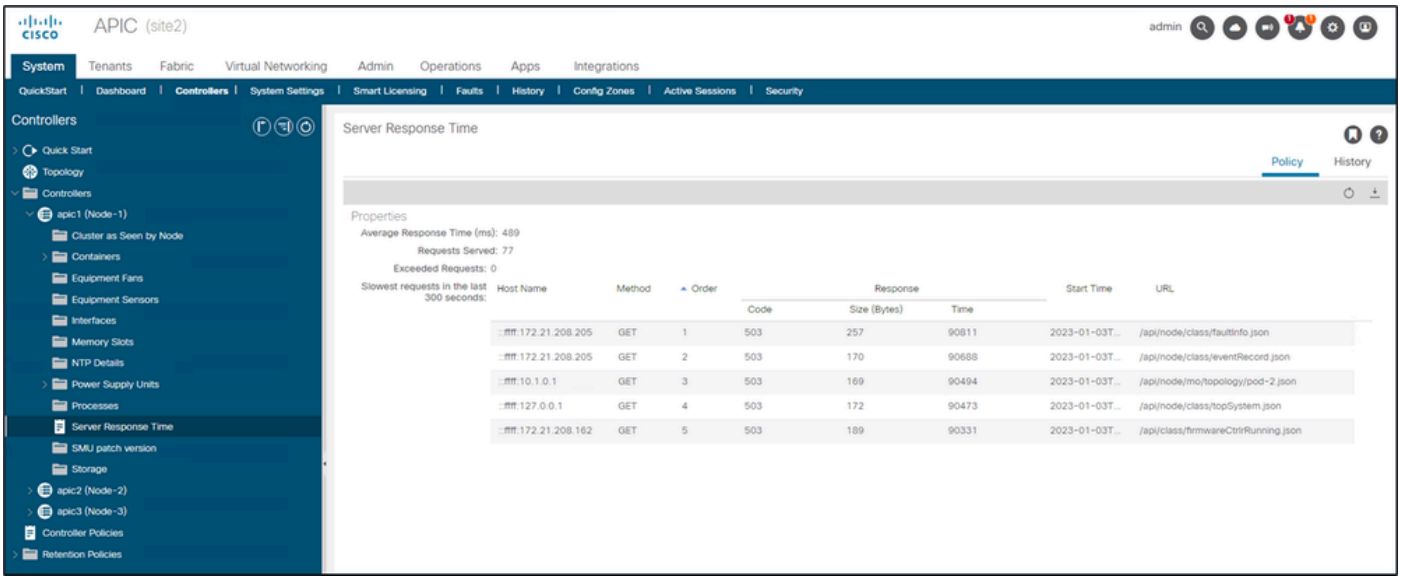
وقت إستجابة النظام - تمكين الحساب لوقت إستجابة الخادم

في 4.2(1)+، يمكن للمستخدم تمكين "حساب أداء النظام" الذي يتتبع طلبات واجهة برمجة التطبيقات (API) التي استغرقت وقتا طويلا لمعالجتها ويسلط الضوء عليها.



يمكن تمكين الحساب من النظام - إعدادات النظام - أداء النظام

بمجرد تمكين "الحساب"، يمكن للمستخدم الانتقال إلى عنوان APIC معينة ضمن وحدات التحكم لعرض أبطأ طلبات API خلال آخر 300 ثانية.



النظام - وحدات التحكم - مجلد وحدات التحكم - APIC X - وقت إستجابة الخادم

إعتبارات إستخدام API

مؤشرات عامة للتأكد من أن البرنامج النصي لا يضر NGINX

- يقوم كل ملف APIC بتشغيل ملف NGINX DME الخاص به.
  - 3 NGINX الخاص ب APIC 2 و يقوم APIC 1 فقط. ال طلبات NGINX الخاصة ب APIC بمعالجة هذه الطلبات.
- وبشكل عام، يتسبب ما يزيد عن 40 طلبا من طلبات واجهة برمجة التطبيقات في فترة زمنية طويلة في إضعاف NGINX. الثانية على مدى.
  - وإذا وجدت، فقل من حدة الطلبات.
  - إذا تعذر تعديل مضيف الطلبات، فاعتبر حدود معدل NGINX على APIC.

أوجه القصور في البرامج النصية للعنوان

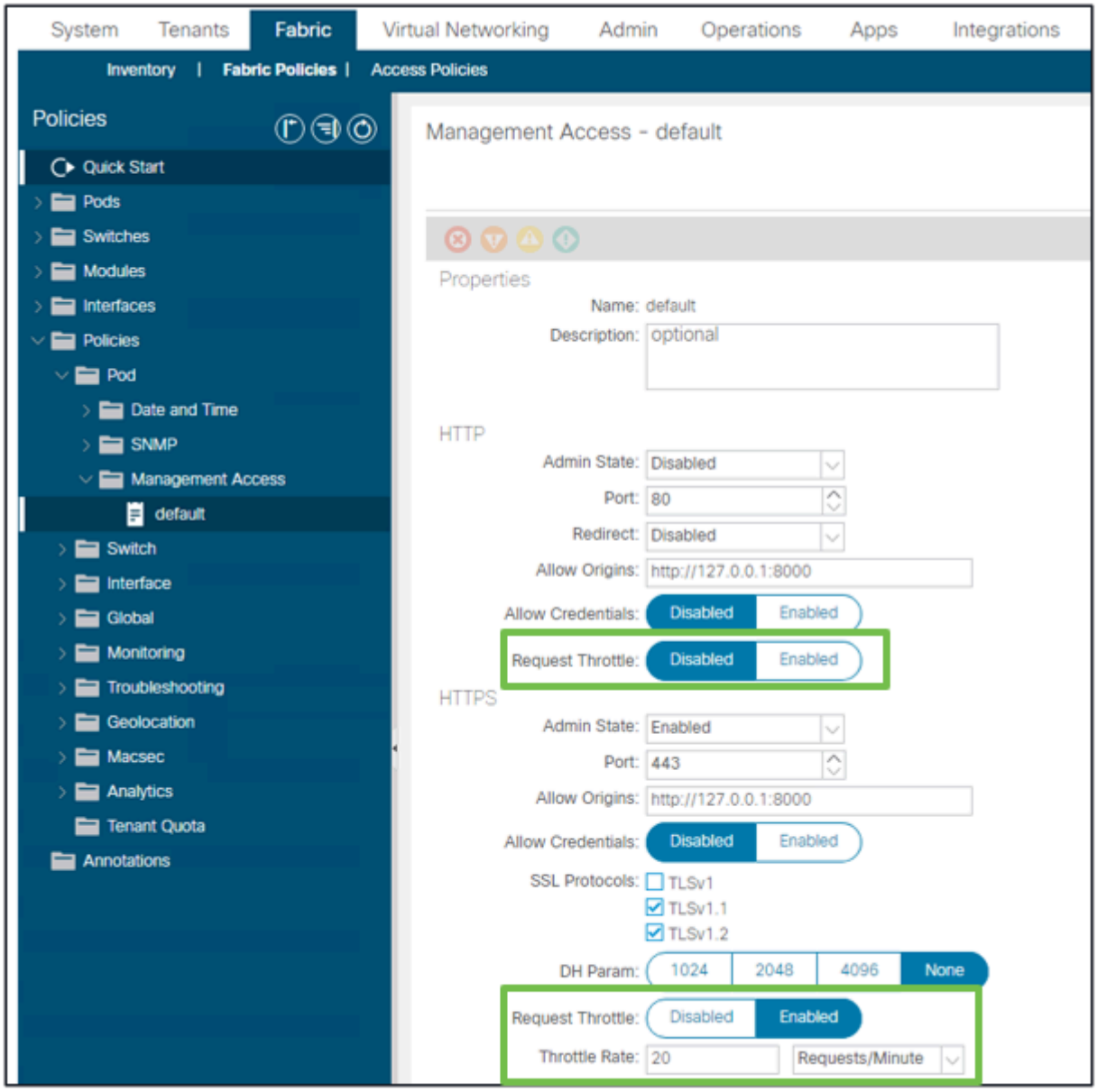
- عدم تسجيل الدخول/تسجيل الخروج قبل كل طلب من طلبات واجهة برمجة التطبيقات.
  - المهلة الافتراضية لجلسة عمل تسجيل دخول واحدة هي 10 دقائق. يمكن إستخدام نفس جلسة العمل هذه لطلبات متعددة ويمكن تحديثها لتمديد وقت الصلاحية.
  - راجع دليل تكوين واجهة برمجة التطبيقات (APIC) REST API من Cisco - الوصول إلى واجهة برمجة التطبيقات (REST) - المصادقة على جلسة عمل واجهة برمجة التطبيقات (API) وصيانتها.
- إذا كان البرنامج النصي الخاص بك يستعلم عن العديد من DNs التي تشترك في أصل، بدلا من طي الاستعلامات إلى استعلام أصل منطقي واحد باستخدام عوامل تصفية الاستعلام.
  - راجع دليل تكوين واجهة برمجة التطبيقات (APIC) REST API من Cisco - تكوين استعلامات REST API - تطبيق عوامل تصفية نطاق الاستعلام.

- [ضع في الاعتبار اشتراكات](#) إذا كنت بحاجة إلى تحديثات لكائن أو فئة كائن، WebSocket بدلا من طلبات API السريعة.

تقييد طلب NGINX

يستطيع المستخدم، المتوفر في 4.2(1)+، تمكين تقييد الطلب مقابل HTTP و HTTPS بشكل مستقل.

ملاحظة: بدءا من الإصدار 6.1(2) من واجهة برمجة التطبيقات، تم تخفيض المعدل الأقصى المدعوم لهذه الميزة إلى 40 طلبا في الثانية (r/s) أو 2400 طلب في الدقيقة (r/m) من 10000 r/m.



Fabric - سياسات البنية - مجلد السياسات - مجلد الوصول إلى الإدارة - الافتراضي

عند التمكين:

- تمت إعادة تشغيل NGINX لتطبيق تغييرات ملف التكوين

- ◦ تمت كتابة منطقة جديدة، httpsClientTagZone، إلى تكوين nginx
- يمكن تعيين معدل الكبح في طلبات في الدقيقة (r/m) أو طلبات في الثانية (r/s).
- تنفيذ حد المعدل المضمن في NGINX على الطلب يدعم تقييد
  - ◦ المحدد URI الكبح لمعدل مقابل (API) التطبيقات برمجة واجهة طلبات مستخدم بواسطة المستخدم + الاندفاع= (الكبح لمعدل x 2) + التأخير عدم
    - ◦ وجود خانق غير قابل للتكوين (zone aaaApiHttps) لـ /api/aaaLogin و/api/aaaRefresh أي حد للمعدل عند 2r/s + burst=4 + nodelay
  - ◦ يتم تعقب تقييد الطلب على أساس عنوان IP لكل عميل
  - ◦ طلبات API التي يتم الحصول عليها من APIC Self-IP (UI + CLI) تتجاوز الكبح
  - ◦ أي عنوان IP للعميل الذي يعبر معدل الكبح المعرف من قبل المستخدم + حد APIC من 503 إستجابة يستلم الاندفاع
  - ◦ يمكن ربط هذه الأجهزة 503s لداخل السجلات لوصول
  - ◦ يحتوي Error.log على إدخالات تشير إلى الوقت الذي تم فيه تنشيط التقييد (المنطقة httpsClientTagZone) وعلى أي مضيف من العملاء

<#root>

```
apic#

less /var/log/dme/log/error.log

...
2023/04/17 20:19:14 [error] ...

limiting requests

, excess: 40.292 by zone "

httpsClientTagZone

", client: h.o.s.t, ... request: "GET /api/class/...", host: "a.p.i.c"
2023/04/17 20:19:14 [error] ...

limiting requests

, excess: 40.292 by zone "

httpsClientTagZone

", client: h.o.s.t, ... request: "GET /api/node/...", host: "a.p.i.c"
```

كقاعدة عامة، يعمل "خانق الطلب" فقط على حماية الخادم (APIC) من الأعراض الشبيهة بأعراض DDoS التي تحدث من قبل العملاء الذين لا يتورعون عن الاستعلام. من المهم للعميل الذي يدعم الطلب وعزل الحلول النهائية في منطق التطبيق/البرنامج النصي.

توصيات

صممت هذه التوصيات للمساعدة على تقليل الحمل والتوتر التشغيلي على API، ولا سيما في السيناريوهات التي لا يكون فيها مصدر واحد موسوم عن عدد كبير من المكالمات API. من خلال تنفيذ أفضل الممارسات هذه، يمكنك تقليل العمليات غير الضرورية للمعالجة والتسجيل وإنشاء الأحداث عبر البنية الخاصة بك إلى الحد الأدنى، مما يؤدي إلى

تحسين إستقرار النظام والأداء. وتكتسي هذه الاقتراحات أهمية خاصة في البيئات التي تساهم فيها السلوكيات الكلية بدل من الحوادث المعزولة في حدوث إجهاد خاص بالجهاز.

تعطيل تسجيل قائمة التحكم في الوصول (ACL)

تأكد من إيقاف تشغيل تسجيل قائمة التحكم في الوصول أثناء العمليات العادية. قم بتمكينها فقط أثناء إطارات الصيانة المجدولة لاستكشاف الأخطاء وإصلاحها أو تصحيح الأخطاء. يمكن أن يؤدي التسجيل المستمر إلى توليد رسائل إعلامية مفرطة، خاصة مع حالات هبوط حركة مرور البيانات كبيرة الحجم عبر محولات متعددة، مما يزيد من حمل عمل APIC.

لمزيد من التفاصيل، راجع دليل تكوين أمان واجهة برمجة التطبيقات من Cisco (إرتباط دليل 5.2.x):
https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/security-configuration/cisco-apic-security-configuration-guide-release-52x/security-policies-52x.html

الحد من تحويل Syslog إلى الأحداث الهامة

قم بتكوين النظام حتى يتم تحويل رسائل syslog فقط التي تحتوي على تنبيه الخطورة إلى EventRecords. تجنب تحويل مستوى المعلومات (والذي يتضمن ACL.Logging) لمنع الأحداث المزعجة من تجاوز APIC:

1. انتقل إلى سياسات البنية → الليفية → السياسات → المراقبة → السياسة المشتركة → نهج رسائل Syslog → الافتراضي.
2. قم بضبط عامل تصفية التسميات لتعيين خطورة syslog للتنبيه.

رموز الحدث غير الأساسي

لتقليل الضوضاء. (Squelch) غير ذات الصلة باحتياجات المراقبة الخاصة بك منع رموز الأحداث
لإسكات رمز حدث E4204939، أستخدم هذا الأمر على أي CLI واجهة سطر الأوامر:

```bash
icurl -k -sX POST -d '<fabricInst><monCommonPol><eventSevAsnP code="E4204939" sev="squelched"/></monCom
```

للتحقق من:

```bash
icurl -k -sX GET 'https://localhost/api/node/class/eventSevAsnP.xml' | xmllint --format -
```

مدختسملا ةهجاو ربع ققحت ،كلذ نم الدب:
ةروطخ نييعت ةسايس < ةماع ةسايس < ةبقارم < تاسايس < ةيوينب تاسايس < جسن ثدحلا

تحسين تحديثات اشتراك ND

رادصإلا قبست يتلا ND تارادصإ ةطساوب اهترادإ متت يتلا ةيفيللا تاونقلل ةبسنلاب لصاوف نيسحتل ثدحأ رادصإ وأ تارادصإلا هذه دحأ ىلإ ةيقرتلاب مق ،4.1.1g وأ رتم 3.2.2 ،تانايب لقن ةيلمع لكل ةيناث 45 لك ةقباسلا تارادصإلا ثيدحت متي .كارتشالا ثيدحت ديزت .مويلا يف APIC بلط 300000 نم رثكأ ،عساو قاطن ىلع ،هنع جتني نأ نكمي امم تايلمع نم لليقي امم ،(ةدحاو ةعاس) ةيناث 3600 ىلإ كارتشالا ةلهم ةثدحملا تارادصإلا .مويلا يف 5000 يلاوح ىلإ ثيدحتلا

مراقبة الاستعلامات ذات الصلة ب Intersight

نم ةيرود يساسأ ماظن تامالعتسا ءاشنإب Intersight ةزيم نيكمت مت يتلا ىنبلا موقت .APIC لمح ىلإ فيضي امم ،(ةيناث 15 لك) DC لصوم .فيلاكتلا ليلقتل مالعتسالا اذه نيسحت مت ،ثدحألا تارادصإلاو 6.1.2 رادصإلا يف

ضبط نهج الاستبقاء للسجلات

مكارتلا عنمل 1000 ىلإ healthRecord و faultRecord و eventRecord ل ءاقبتسالا جهن نييعت لكشب تالجسلا هذه جرختست امدنع صاخ لكشب اديفم اذه نوكي .تالجسلل طرفملا لباقم ةبقارملا ةقد ليلقت ريثأت مييقتب امئاد مق .نيعم يليغشت طاشن يأل مظتنم .اهلحو تالكشملا فاشكتسأ تابلطتمو ةيليغشتلا كتابلطتم

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).