أستكشاف أخطاء المستخدم المفرط للأقراص وإصلاحها على أجهزة Sourcefire

المحتويات

المقدمة
خطوات التحقق
إذا كان قسم /وحدة التخزين ممتلئا
ملفات النسخ الاحتياطي القديمة
ملفات تحديث وتصحيح البرامج القديمة
قاعدة بيانات كبيرة لتخزين الأحداث
إستلام تنبيهات الحالة الصحية لاستخدام الأقراص بنسبة تزيد عن 85٪
تحتوي الملفات /var/log/messages على بيانات أقدم من 24 ساعة، أو أكبر من 25 ميغابايت
إذا كان قسم الجذر (/) ممتلئا
يتم حفظ ملفات المستخدم على القسم الجذر (/)
تتم كتابة العمليات غير المدعومة إلى قسم الجذر (/)

المقدمة

يمكن أن تنفد مساحة القرص الخاصة بمركز إدارة FireSIGHT أو جهاز FirePOWER لأسباب مختلفة. عند حدوث ذلك، تقوم ميزة "الاستخدام العالي للقرص" بتشغيل "تنبيه الحماية" أو قد تفشل محاولة تحديث البرنامج. تصف هذه المقالة الأسباب الجذرية للاستخدام المفرط للأقراص وبعض خطوات أستكشاف الأخطاء وإصلاحها.

خطوات التحقق

تحديد القسم الذي يتم إستخدامه بشكل كبير. يظهر الأمر التالي إستخدام القرص:

على مركز إدارة FireSIGHT،

```
admin@3DSystem:~# df -TH
```

في أجهزة 7000 و 8000 Series والأجهزة الظاهرية NGIPS،

```
> show disk
```

يظهر كل من الأمرين مخرجات مثل أدناه:

```
Filesystem            Size  Used Avail Use% Mounted on
/ dev/sda5 2.9G 566M 2.2G 21%/
dev/sda1 99M 16M 79M 17% /boot/
dev/sda7 52G 8.5G 41G 18% /Volume/
```

```
none 11G 20K 11G 1% /dev/shm
dev/sdb1 418G 210M 395G 1% /var/storage/
```

ملاحظة: يمكن أن يختلف حجم القرص واستخدامه على طرز أجهزة مختلفة. إذا كان هذا جهاز ظاهري NGIPS، فتحقق من توافق حجم الأقسام مع الحد الأدنى لمتطلبات مساحة القرص.

تحذير: أي تقسيم إضافي غير ظاهر أعلاه غير معتمد.

في أجهزة السلسلتين 7000 و 8000 وفي الأجهزة الافتراضية NGIPS، يمكنك تشغيل الأمر التالي لعرض إحصائيات تفصيلية حول إستخدام الأقراص:

```
> show disk-manager
```

إخراج مثال:

```
> show disk-manager
                                  Silo Used Minimum Maximum
                  Temporary Files 143.702 MB 402.541 MB 1.572 GB
                  Action Queue Results 0 KB 402.541 MB 1.572 GB
                  Connection Events 17.225 GB 3.931 GB 23.586 GB
                  User Identity Events 0 KB 402.541 MB 1.572 GB
                                UI Caches 587 KB 1.179 GB 2.359 GB
                                    Backups 0 KB 3.145 GB 7.862 GB
                                  Updates 13 KB 4.717 GB 11.793 GB
                  Other Detection Engine 0 KB 2.359 GB 4.717 GB
                  Performance Statistics 72.442 MB 805.082 MB 9.435 GB
                                Other Events 669.819 MB 1.572 GB 3.145 GB
                  IP Reputation & URL Filtering 0 KB 1.966 GB 3.931 GB
                  Archives & Cores & File Logs 1.381 GB 3.145 GB 15.724 GB
                                RNA Events 0 KB 3.145 GB 12.579 GB
                  File Capture 12.089 MB 4.717 GB 14.152 GB
                                IPS Events 3.389 GB 7.076 GB 15.724 GB
```

إذا كان قسم /وحدة التخزين ممتلئا

ملفات النسخ الاحتياطي القديمة

- إذا قمت بتخزين كميات كبيرة من ملفات النسخ الاحتياطي القديمة على النظام، فقد يستغرق ذلك مساحة كبيرة على القرص.

خطوات أستكشاف الأخطاء وإصلاحها

- حذف ملفات النسخ الاحتياطي القديمة باستخدام واجهة مستخدم ويب. لإزالة ملفات النسخ الاحتياطي، انتقل إلى **النظام > أدوات > النسخ الاحتياطي/الاستعادة**.

تلميح: في نظام FireSIGHT، يمكنك تكوين التخزين عن بعد لتخزين ملفات النسخ الاحتياطي الكبيرة.

ملفات تحديث وتصحيح البرامج القديمة

- إذا كنت تحتفظ دائما بملفات تحديث البرامج السابقة وترقيتها وتصحيحها (مثل 5.0 أو 5.1)، فيمكن للنظام تشغيل مساحة على القرص.

خطوات أستكشاف الأخطاء وإصلاحها

- احذف ملفات التحديث والتصحيح القديمة التي لم تعد ضرورية. من أجل حذفها، الرجاء الانتقال إلى **النظام > التحديثات**.

يتم تخزين ملفات الأحداث الزائدة

- قد يكون الجهاز المدار أو المستشعر قد توقف عن إرسال الأحداث إلى مركز إدارة FireSIGHT.
- قد يقوم الجهاز بتوليد أحداث أكثر من تلك التي يقوم مركز الإدارة بتصميمها للاستقبال (في الثانية).
- قد تكون هناك مشكلة اتصال بين الجهاز المدار ومركز الإدارة.

خطوات أستكشاف الأخطاء وإصلاحها

- قم بإعادة تطبيق السياسة المرتبطة بالحدث. على سبيل المثال، إذا لم تكن ترى أحداث اتصال، فأعد تطبيق نهج التحكم في الوصول وانظر ما إذا كان يتم إستلام أي أحداث جديدة الآن بواسطة مركز الإدارة.
- إذا تعذر على "مركز إدارة FireSIGHT" تلقي أحداث IPS جديدة، فيرجى التحقق من وجود أي مشاكل في الاتصال بين الجهاز الذي تتم إدارته ومركز الإدارة.

الملفات غير المعروفة الزائدة

- يقوم نظام FireSIGHT بتخزين بيانات اكتشاف الشبكة **غير المعروفة** (معلومات نظام التشغيل والمضيف والخدمة).

خطوات أستكشاف الأخطاء وإصلاحها

- إذا تعذر على النظام تحديد نظام التشغيل على جهاز مضيف على الشبكة، فيمكنك إستخدام برنامج Nmap لإجراء فحص فعال للمضيف. تستخدم NMAP المعلومات التي تحصل عليها من الفحص لتقييم أنظمة التشغيل المحتملة. ومن ثم تستخدم نظام التشغيل الذي يعد صاحب أعلى تصنيف من حيث تعريف نظام التشغيل المضيف.
- قم بإنشاء قاعدة إرتباط يتم تشغيلها عندما يكتشف النظام مضيفا بنظام تشغيل غير معروف.
يجب أن يتم تشغيل القاعدة عند **حدوث حدث اكتشاف** وعند **تغيير معلومات نظام التشغيل للمضيف** وهي تفي بالشروط التالية: **اسم نظام التشغيل غير معروف**.

قاعدة بيانات كبيرة لتخزين الأحداث

- إذا قمت بزيادة الحد الأقصى لحدث قاعدة البيانات بما يتجاوز الإرشادات أو أفضل الممارسات، فيمكن أن ينفد من مساحة القرص لمركز إدارة FireSIGHT.

خطوات أستكشاف الأخطاء وإصلاحها

- تحقق من قيم حد قاعدة البيانات. لتحسين إستخدام القرص والأداء، يجب أن تضع حدود للحدث لتناسب عدد الأحداث التي **تعمل** معها **بانتظام**. بالنسبة لبعض أنواع الأحداث، يمكنك تعطيل التخزين.
- لتغيير حد قاعدة البيانات، الرجاء الانتقال إلى صفحة "نهج النظام"، وانقر فوق **تحرير** الموجود بجوار اسم نهج النظام، ثم انقر فوق **قاعدة البيانات** الموجودة على المقطع الأيسر. للوصول إلى صفحة **نهج النظام**، الرجاء الانتقال إلى **النظام > محلي > نهج النظام**.

إستلام تنبيهات الحالة الصحية لاستخدام الأقراص بنسبة تزيد عن 85٪

الأسباب المحتملة

- قد يكون معدل الحدث مرتفعا للغاية. وبالتالي يقوم الجهاز بتوليد وتخزين العديد من الأحداث.
- مشكلات الاتصال بين الجهاز المدار و FireSIGHT Management Center.

خطوات أستكشاف الأخطاء وإصلاحها

- يمكن أن يكون تغيير مستوى حد التنبيه إلى 87٪ (تحذير) و 92٪ (حرج) حلا بسيطا لتنبيهات الصحة المتكررة.
- اقرأ ملاحظات الإصدار لمعرفة ما إذا كانت هناك مشكلة معروفة في نظام التنقيح. عند توفر حل، يرجى تحديث إصدار البرنامج إلى أحدث إصدار لمعالجة هذه المشكلة.

تحتوي الملفات /var/log/messages على بيانات أقدم من 24 ساعة، أو أكبر من 25 ميغابايت

الأسباب المحتملة

- قد لا يعمل برنامج Logrotate Daemon بشكل صحيح.

خطوات أستكشاف الأخطاء وإصلاحها

- إذا واجهت هذه المشكلة، فيرجى تحديث إصدار البرنامج الخاص بأنظمة FireSIGHT إلى أحدث إصدار. إذا كنت تشغل الإصدار الأحدث، ولا تزال تواجه هذه المشكلة، فرجاء الاتصال بمركز المساعدة التقنية (TAC) من Cisco.

إذا كان قسم الجذر (/) ممتلئا

يتم حفظ ملفات المستخدم على القسم الجذر (/)

الأسباب المحتملة

- قسم الجذر (/) هو حجم ثابت ولا يستهدف التخزين الشخصي.
- يتم إستخدام الدليل /var/tmp يدويا للتخزين المؤقت، بدلا من الدليل /var/common.

خطوات أستكشاف الأخطاء وإصلاحها

- تحقق من وجود ملفات غير ضرورية على المجلد /root و/home و/tmp. بما أن هذه المجلدات لا يتم إنشاؤها للتخزين الشخصي، يمكنك حذف أي ملف شخصي باستخدام أمر rm.

تتم كتابة العمليات غير المدعومة إلى قسم الجذر (/)

الأسباب المحتملة

- إذا قمت بتثبيت برنامج من إنتاج جهة خارجية يقوم بإنشاء ملفات على قسم الجذر (/)، فيمكنك تجربة تنبيه السلامة للاستخدام العالي للقرص.

خطوات أستكشاف الأخطاء وإصلاحها

- تحقق مما إذا تم تثبيت أي حزم غير مدعومة. قم بتشغيل الأمر التالي للعثور على الحزم المثبتة:

```
admin@3DSystem:~$ rpm -qa --last
```

- تحقق من pstree و top لمعرفة ما إذا كانت العمليات غير المدعومة قيد التشغيل أم لا. قم بتشغيل الأوامر التالية:

```
admin@3DSystem:~$ pstree -ap
```

```
admin@3DSystem:~$ top
```

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).