

أطخ" ةلاس ر عاجراب FireSIGHT ماظن موقوي "جارخ إلال/الإخراج"

المحتويات

[المقدمة](#)

[الأعراض](#)

[التحقق](#)

[الحل](#)

المقدمة

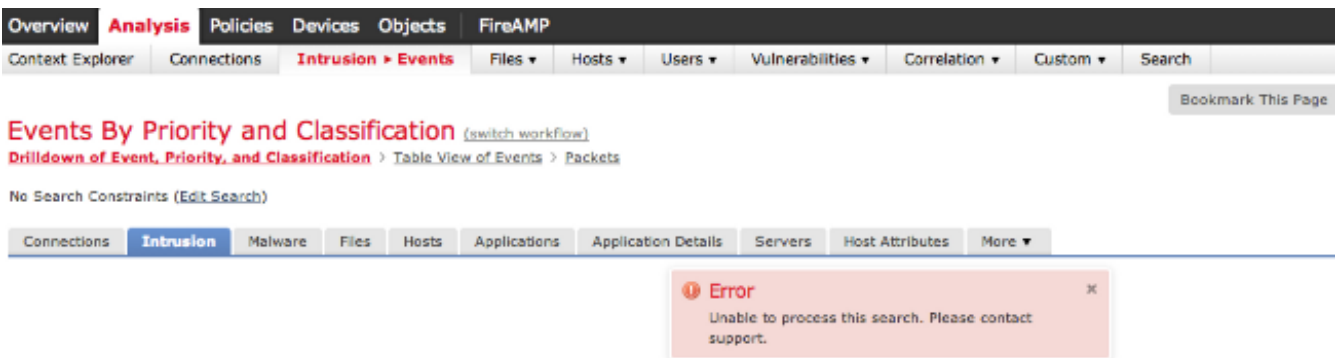
عند العمل على نظام FireSIGHT، قد تتلقى رسالة لخطأ الإدخال/الإخراج أو خطأ الإدخال/الإخراج. يوضح هذا المستند كيفية التحقيق في هذه المشكلة، وكيفية أستكشاف الأخطاء وإصلاحها.

الأعراض

• يتعذر تطبيق نهج التطفل. قد تعرض حالة المهمة رسالة الخطأ التالية:

```
:Could not create directory /var/tmp/PolicyExport_XXXX  
Input/output error
```

• فشل الاستعلام عن أحداث التطفل. قد تظهر نتيجة البحث الخطأ التالي:



The screenshot shows the FireAMP interface with the 'Intrusion > Events' tab selected. The main content area displays 'Events By Priority and Classification' with a search bar and a 'Bookmark This Page' button. Below the search bar, there is a navigation menu with options like 'Connections', 'Intrusion', 'Malware', 'Files', 'Hosts', 'Applications', 'Application Details', 'Servers', and 'Host Attributes'. A red error message box is visible in the bottom right corner, stating: 'Error: Unable to process this search. Please contact support.'

• يتعذر تحميل مراقبة الصحة على واجهة مستخدم ويب.
• يتعذر عرض الأجهزة المدارة.

التحقق

للتحقق من المشكلة، اتبع الخطوات التالية:

الخطوة 1: اتصل بنظام FireSIGHT لديك من خلال (SSH Secure Shell).

الخطوة 2: ترقية امتيازك إلى جذر المستخدم:

• FireSIGHT Management Center وخدمة FirePOWER، التشغيل:

```
#~:admin@FireSIGHT:~$ sudo su -root@FireSIGHT
```

• جهاز أمان FirePOWER، شغل:

```
expert <
- admin@FirePOWER:~$ sudo su
#~:root@FirePOWER
```

الخطوة 3: قم بتشغيل الأوامر التالية للتحقيق في هذه المشكلة:

• يعرض إخراج الأمر `dmesg` خطأ إدخال/إخراج. على سبيل المثال:

```
root@FireSIGHT:~# dmesg
```

```
sh: /bin/dmesg: Input/output error-
```

• يقوم الأمر `ls` بإرجاع خطأ الإدخال/الإخراج. على سبيل المثال:

```
admin@FireSIGHT:~$ ls
```

```
ls: reading directory .: Input/output error
```

• تقوم محاولة إنشاء ملف أكتشاف الأخطاء وإصلاحها بإنشاء خطأ في الإدخال/الإخراج. على سبيل المثال:

```
admin@FireSIGHT:~$ sudo sf_troubleshoot.pl
```

```
usr/local/sf/bin/sf_troubleshoot.pl: Input/output error/
```

• تم العثور على رسائل خطأ الإدخال/الإخراج على `/var/log/messages`. على سبيل المثال:

```
admin@FireSIGHT:~$ grep -i error /var/log/messages
```

```
Sourcefire3D kernel: sd 2:2:0:0: scsi: Device offlined - not ready after error recovery
Sourcefire3D kernel: end_request: I/O error, dev sda, sector 1109804126
Sourcefire3D kernel: Buffer I/O error on device sda7, logical block 0
Sourcefire3D kernel: lost page write due to I/O error on sda7
Sourcefire3D kernel: Buffer I/O error on device sda7, logical block 137396224
Sourcefire3D kernel: lost page write due to I/O error on sda7
Sourcefire3D kernel: EXT2-fs error (device sda7): read_block_bitmap: Cannot read block
bitmap - block_group = 4208, block_bitmap = 13
```

• تم العثور على خطأ الإدخال/الإخراج على `/var/log/action_queue.log`:

```
Error in tempdir() using /var/tmp/PolicyExport_XXXXX: Could not create directory
var/tmp/PolicyExport_XXXXX: Input/output error/
```

الحل

أعد تمهيد الجهاز الخاص بك بسهولة لإجراء فحص لنظام الملفات:

```
root@FireSIGHT:~# reboot
```

إن لا يحل هذا إصدار، أنجزت جزمة reboot على الأداة:

```
root@FireSIGHT:~# reboot -f
```

بعد تشغيل الأمر **reboot -f**، يعيد نظام FireSIGHT تشغيل وإجراء فحص لنظام الملفات. على سبيل المثال:

```
/boot: 34/26104 files (29.4% non-contiguous), 48680/104388 blocks
e2fsck 1.42.2 (27-Mar-2012)
/Volume contains a file system with errors, check forced.
Pass 1: Checking inodes, blocks, and sizes
Inode 1036407, i_size is 14921607, should be 14929920. Fix? yes

Inode 1036407, i_blocks is 29184, should be 29200. Fix? yes

Volume: |=====| 37.4%
```

بعد إعادة التشغيل الإجباري، إذا كنت لا تزال تواجه هذا الإصدار، فيرجى الاتصال بدعم Cisco التقني للحصول على مساعدة.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة يرش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا