

Contenido

[Introducción](#)

[Síntomas](#)

[Verificación](#)

[Solución](#)

Introducción

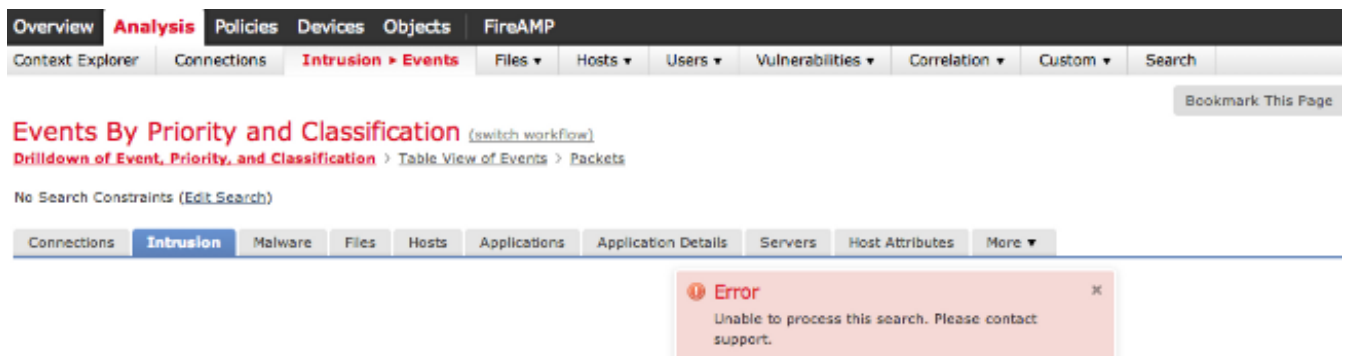
Cuando usted está trabajando en un sistema de FireSIGHT, usted puede recibir un mensaje para el error entrada-salida o el error de la entrada-salida. Este documento describe cómo investigar este problema, y cómo resolverlo problemas.

Síntomas

- Incapaz de aplicar la directiva de la intrusión. **El estatus de la tarea** puede visualizar el mensaje de error siguiente:

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

- Una interrogación para los eventos de la intrusión falla. El resultado de la búsqueda puede mostrar el error siguiente:



The screenshot shows the FireSIGHT web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. Below this, there are tabs for 'Context Explorer', 'Connections', 'Intrusion > Events', 'Files', 'Hosts', 'Users', 'Vulnerabilities', 'Correlation', 'Custom', and 'Search'. The main content area is titled 'Events By Priority and Classification' with a '(switch workflow)' link. Below the title, there are links for 'Drilldown of Event, Priority, and Classification', 'Table View of Events', and 'Packets'. A search bar is present with the text 'No Search Constraints (Edit Search)'. At the bottom of the interface, there is a navigation bar with tabs for 'Connections', 'Intrusion', 'Malware', 'Files', 'Hosts', 'Applications', 'Application Details', 'Servers', 'Host Attributes', and 'More'. An error message box is displayed in the bottom right corner, containing the text: 'Error: Unable to process this search. Please contact support.'

- Incapaz de cargar el control de salud en la interfaz del Web User.
- Incapaz de ver los dispositivos administrados.

Verificación

Para verificar el problema, siga los pasos abajo:

Paso 1: Conecte con su sistema de FireSIGHT vía el Secure Shell (SSH).

Paso 2: Eleve su privilegio al usuario raíz:

- En el centro de administración de FireSIGHT y el dispositivo de la potencia de fuego, ejecútese:

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

- En el dispositivo de la potencia de fuego, ejecútese:

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

Paso 3: Funcione con los siguientes comandos de investigar este problema:

- La salida del comando `dmesg` muestra el error de la entrada-salida. Por ejemplo:

```
root@FireSIGHT:~# dmesg
-sh: /bin/dmesg: Input/output error
```

- El comando `ls` vuelve el error de la entrada-salida. Por ejemplo:

```
admin@FireSIGHT:~$ ls
ls: reading directory .: Input/output error
```

- Una tentativa de generar el archivo del Troubleshooting genera el error de la entrada-salida. Por ejemplo: `admin@FireSIGHT:~$ sudo sf_troubleshoot.pl`

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

- Los mensajes de error entrada-salida se encuentran en `/var/log/messages`. Por ejemplo:

```
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
```

- El error de la entrada-salida se encuentra en `/var/log/action_queue.log`:
Error in tempdir() using `/var/tmp/PolicyExport_XXXXX`: Could not create directory
`/var/tmp/PolicyExport_XXXXX`: Input/output error

Solución

Reinicie agraciado su dispositivo para realizar un control de sistema de archivos:

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

Si esto no resuelve el problema, realice una reinicialización forzada en el dispositivo:

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

Después de que usted funcione con el comando `-f` de la reinicialización, los reinicios de sistema de FireSIGHT y realizan un control de sistema de archivos. Por ejemplo:

```
/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%
```

Después de una reinicialización forzada, si usted todavía está encontrando este problema, entre en contacto por favor el Soporte técnico de Cisco para la ayuda.