Troubleshooting de Secure Endpoint Linux Connector Fault 18

Contenido

Introducción

Este documento describe el Fault 18 en el conector Secure Endpoint Linux.

Falla 18: La supervisión de eventos del conector está sobrecargada

El motor de protección del comportamiento mejora la visibilidad de los conectores en la actividad del sistema. Con este aumento de la visibilidad hay una mayor posibilidad de que la supervisión de la actividad del sistema del conector se vea desbordada por la cantidad de actividad del sistema. Si esto sucede, el conector genera la falla 18 e ingresa en el modo degradado. Refiérase al artículo Errores del Conector de Linux de Cisco Secure Endpoint para obtener detalles sobre el fallo 18. En el conector de Linux, el status se puede utilizar en la CLI de Secure Endpoint Linux para ver si el conector se está ejecutando en modo degradado y si se ha producido algún fallo. Si se produce el fallo 18, ejecute el status en la CLI de Secure Endpoint Linux muestra el fallo con una de las dos gravedades posibles:

1. Falla 18 con gravedad mayor

```
ampcli> status
Status:                 Connected
Mode:                   Degraded
Scan:                   Ready for scan
Last Scan:              2023-06-19 02:02:03 PM
Policy:                 Audit Policy for FireAMP Linux (#1)
Command-line:           Enabled
Orbital:                Disabled
Behavioural Protection: Protect
Faults:                 1 Major
Fault IDs:      18
                ID 18 - Major: Connector event monitoring is overloaded. Investigate the most acti
```

2. Falla 18 con gravedad crítica

```
ampcli> status
Status:                 Connected
Mode:                   Degraded
Scan:                   Ready for scan
Last Scan:              2023-06-19 02:02:03 PM
Policy:                 Audit Policy for FireAMP Linux (#1)
Command-line:           Enabled
Orbital:                Disabled
Behavioural Protection: Protect
Faults:                 1 Critical
Fault IDs:      18
                ID 18 - Critical: Connector event monitoring is overloaded. Investigate the most a
```

La supervisión de eventos de conector está sobrecargada: gravedad mayor

Cuando el fallo 18 se provoca con una gravedad mayor, esto significa que la supervisión de eventos del conector está sobrecargada pero todavía puede supervisar un conjunto más pequeño de eventos del sistema. El conector cambia a gravedad mayor y supervisa menos eventos equivalentes a la supervisión que estaba disponible en los conectores anteriores a 1.2.0. Si la inundación de eventos del sistema es corta y la carga de monitoreo de eventos disminuye nuevamente a un rango aceptable, entonces se borra el fallo 18 y el conector reanuda la supervisión de todos los eventos del sistema. Si la inundación de eventos del sistema empeora y la carga de monitoreo de eventos aumenta a una cantidad crítica, entonces el fallo 18 se eleva con una gravedad crítica y el conector cambia a una gravedad crítica.

La supervisión de eventos de conector está sobrecargada: gravedad crítica

Cuando el fallo 18 se plantea con una gravedad crítica, esto significa que el conector está experimentando una cantidad abrumadora de eventos del sistema que pone en riesgo el conector. El conector cambia a una gravedad crítica más restrictiva. En este estado, el conector solo supervisa los eventos críticos para permitir que el conector se limpie y se centre en la recuperación. Si la avalancha de eventos finalmente vuelve a disminuir a un rango más aceptable, entonces la falla se borra por completo y el conector reanuda la supervisión de todos los eventos del sistema.

Guía de acción de fallas

Si el conector genera alguna vez la falla 18 con una gravedad importante o crítica, se deben tomar algunos pasos para investigar y resolver el problema. Los pasos para resolver el fallo 18 varían en función de cuándo y por qué se ha producido el fallo:

1. La falla 18 se originó en una instalación nueva del conector Linux
2. El fallo 18 se produjo después de cambios recientes en el sistema operativo
3. La falla 18 se planteó espontáneamente

4. La falla 18 surgió al reaprovisionar una máquina con el conector Linux ya instalado o al actualizar el conector a la versión 1.2.0+

Caso 1: Instalación nueva

Si se observa un fallo 18 y un modo degradado fuera de una instalación nueva del conector Linux, primero debe asegurarse de que su sistema cumpla con los requisitos mínimos del sistema. Después de comprobar que los requisitos cumplen o superan los requisitos mínimos, si el error persiste, debe investigar los procesos más activos del sistema. Puede ver los procesos activos actuales en un sistema Linux mediante el top (o similar) en el terminal. Si se sabe que los procesos que consumen la mayor cantidad de CPU son benignos,

puede crear nuevas exclusiones de procesos para excluir esos procesos de la supervisión.

Situación de ejemplo:

Supongamos que después de una instalación nueva, se visualizó el modo degradado y el fallo 18 a través de la CLI de Secure Endpoint Linux. Rejecución del top en una máquina Ubuntu mostraba estos procesos activos:

```
Tasks: 223 total,   5 running, 218 sleeping,   0 stopped,   0 zombie
%Cpu(s): 29.4 us, 34.3 sy,  0.0 ni, 36.2 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :   7943.0 total,   3273.9 free,   2357.6 used,   2311.5 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   5141.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  34896 user1     20   0   18136   3292   3044 R  96.7   0.0   0:04.89 trusted_process
   4296 user1     20   0  823768  52020  38900 R  48.0   0.6   0:10.90 gnome-terminal-
    117 root      20   0       0      0      0 I  12.3   0.0   0:01.86 kworker/u64:6-events_unbound
  34827 root      20   0       0      0      0 I  10.3   0.0   0:00.47 kworker/u64:2-events_unbound
   1880 user1     20   0  353080 101600  70164 S   6.3   1.2   0:30.37 Xorg
  34576 root      20   0       0      0      0 R   6.3   0.0   0:01.46 kworker/u64:1-events_unbound
   2089 user1     20   0 3939120 251332 104008 S   3.0   3.1   0:23.25 gnome-shell
    132 root      20   0       0      0      0 I   1.3   0.0   0:02.67 kworker/2:2-events
   6951 root      20   0 1681560 213536  74588 S   1.3   2.6   0:41.30 ampdaemon
    741 root      20   0  253648  13352   9280 S   0.3   0.2   0:01.54 polkitd
    969 root      20   0  153600   3788   3512 S   0.3   0.0   0:00.36 prlshprint
   2291 user1     20   0  453636  29388  20060 S   0.3   0.4   0:03.75 prlcc
      1 root      20   0  169608  13116   8524 S   0.0   0.2   0:01.95 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
```

Vemos que hay un proceso muy activo, llamado trusted_process en este ejemplo. En este caso estoy familiarizado con este proceso y es de confianza, no hay razón para sospechar de este proceso. Para solucionar el error 18, el proceso de confianza se puede agregar a una exclusión de proceso en el portal. Consulte el artículo Configure and Identification Cisco Secure Endpoint Exclusions para obtener información sobre las prácticas recomendadas al crear exclusiones.

Caso 2: cambios recientes

Si ha realizado cambios recientes en el sistema operativo, como la instalación de un programa nuevo, se puede observar el modo de fallo 18 y degradado si estos cambios aumentan la actividad del sistema. Utilice la misma estrategia de corrección que se describe en la instalación nueva, busque procesos que estén relacionados con los cambios recientes, como un nuevo proceso ejecutado por un programa recién instalado.

Caso 3: Actividad maliciosa

El motor de protección conductual aumenta los tipos de actividad del sistema que se supervisan. Esto proporciona al conector una perspectiva más amplia del sistema y le permite detectar ataques de comportamiento más complejos. Sin embargo, la supervisión de una mayor cantidad de actividad del sistema también expone al conector a un mayor riesgo de ataques de denegación de servicio (DoS). Si el

conector se ve saturado por la actividad del sistema e ingresa en el modo degradado con falla 18, continúa monitoreando los eventos críticos del sistema hasta que se reduce la actividad general del sistema. Esta pérdida de visibilidad de eventos del sistema reduce la capacidad del conector para proteger su equipo. Es fundamental que investigue el sistema inmediatamente en busca de procesos maliciosos. Use el comando `top` (o similar) en su sistema Linux para ver los procesos activos actuales y tomar las medidas adecuadas para remediar la situación si se identifica algún proceso posiblemente malicioso.

Caso 4: Requisitos del conector

El motor de protección conductual mejora la capacidad del conector para proteger la actividad de la máquina, pero para ello debe consumir más recursos que en versiones anteriores. Si el fallo 18 se genera con frecuencia, no hay procesos benignos que causen una carga pesada y no parece que haya ningún proceso malicioso actuando en la máquina, debe asegurarse de que el sistema cumple los requisitos mínimos del sistema.

Vea también

- Uso de la CLI de Mac/Linux para terminales seguros
- Errores del conector de Cisco Secure Endpoint Linux
- Configuración e identificación de exclusiones de terminales seguros de Cisco
- Guía del usuario de terminales seguros (PDF en inglés)

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).