Cisco Secure Endpoint Linux Connector Fault 18

Sommario

Introduzione

Questo documento descrive l'errore 18 sul connettore Secure Endpoint Linux.

Errore 18: monitoraggio degli eventi del connettore sovraccarico

Il motore di protezione comportamentale migliora la visibilità dei connettori nell'attività del sistema. Con questo aumento della visibilità aumenta la possibilità che il monitoraggio dell'attività del sistema da parte del connettore possa essere sopraffatto dalla quantità di attività sul sistema. In questo caso, il connettore genera il messaggio di errore 18 ed entra in modalità degradata. Per ulteriori informazioni sull'errore 18, fare riferimento all'articolo Cisco Secure Endpoint Linux Connector Faults. Sul connettore Linux, status può essere utilizzato nella CLI di Secure Endpoint Linux per verificare se il connettore è in esecuzione in modalità degradata e se vengono generati errori. Se viene generato l'errore 18, eseguire status Il comando nella CLI di Secure Endpoint Linux visualizza il guasto con una delle due possibili gravità:

1. Errore 18 con gravità maggiore

```
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. Errore 18 con gravità critica

```
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
```

Monitoraggio eventi connettore sovraccarico: gravità maggiore

Se l'errore 18 viene generato con un livello di gravità maggiore, significa che il monitoraggio degli eventi del connettore è sovraccarico ma è comunque in grado di monitorare un set ridotto di eventi di sistema. Il connettore passa alla gravità maggiore e controlla meno eventi, come avviene con il monitoraggio disponibile nei connettori precedenti alla versione 1.2.0. Se il flusso di eventi di sistema è breve e il carico di monitoraggio degli eventi diminuisce in un intervallo accettabile, l'errore 18 viene cancellato e il connettore riprende il monitoraggio di tutti gli eventi di sistema. Se il flusso di eventi di sistema peggiora e il carico di monitoraggio degli eventi aumenta fino a raggiungere una quantità critica, l'errore 18 viene generato con gravità critica e il connettore passa alla gravità critica.

Monitoraggio eventi connettore sovraccarico: gravità critica

Quando l'errore 18 viene generato con gravità critica, il connettore sta vivendo una quantità enorme di eventi di sistema che lo espone a rischi. Il connettore passa a una gravità critica più restrittiva. In questo stato, il connettore esegue il monitoraggio solo degli eventi critici per consentire al connettore di eseguire la pulizia e di concentrarsi sul ripristino. Se il flusso di eventi alla fine diminuisce in un intervallo più accettabile, il guasto viene completamente risolto e il connettore riprende il monitoraggio di tutti gli eventi di sistema.

Guida alle azioni da eseguire in caso di errore

Se il connettore solleva l'errore 18 con un livello di gravità principale o critico, è necessario eseguire alcune operazioni per individuare e risolvere il problema. I passaggi per risolvere l'errore 18 variano a seconda di quando e perché l'errore è stato generato:

1. L'errore 18 è stato generato su una nuova installazione del connettore Linux
2. L'errore 18 è stato generato dopo le recenti modifiche apportate al sistema operativo
3. L'errore 18 è stato generato spontaneamente

4. L'errore 18 è stato generato dopo aver eseguito di nuovo il provisioning di un computer con il connettore Linux già installato o dopo aver aggiornato il connettore alla versione 1.2.0+

Caso 1: Nuova installazione

Se il guasto 18 e la modalità degradata vengono osservati al di fuori di una nuova installazione del connettore Linux, è necessario prima verificare che il sistema soddisfi i requisiti minimi di sistema. Dopo aver verificato che i requisiti soddisfino o superino i requisiti minimi, se l'errore persiste, è necessario esaminare i processi più attivi del sistema. È possibile visualizzare i processi attivi correnti su un sistema Linux utilizzando top (o simile) nel terminale. Se è noto che i processi che utilizzano la quantità maggiore di CPU sono benigni, è possibile creare nuove esclusioni di processo per escludere tali processi dal monitoraggio.

Scenario di esempio:

Si supponga che, dopo una nuova installazione, gli errori 18 e la modalità danneggiata siano stati visualizzati tramite la CLI di Secure Endpoint Linux. Resecuzione di top in un computer Ubuntu sono visualizzati i seguenti processi attivi:

```
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
```

Vediamo che esiste un processo molto attivo, chiamato trusted_process in questo esempio. In questo caso conosco bene questo processo ed è affidabile, non c'è motivo per cui io sia sospettoso di questo processo. Per cancellare l'errore 18, è possibile aggiungere il processo attendibile a un'esclusione di processo nel portale. Per ulteriori informazioni sulle procedure consigliate per la creazione di esclusioni, consultare l'articolo Configurazione e identificazione delle esclusioni di Cisco Secure Endpoint.

Caso 2: modifiche recenti

Se sono state apportate modifiche recenti al sistema operativo, ad esempio l'installazione di un nuovo programma, è possibile osservare l'errore 18 e la modalità danneggiata se le nuove modifiche aumentano l'attività del sistema. Utilizzare la stessa strategia di correzione illustrata nella nuova installazionecaso, tuttavia, è consigliabile cercare i processi correlati alle modifiche recenti, ad esempio un nuovo processo eseguito da un programma appena installato.

Caso 3: Attività Dannosa

Il motore di protezione comportamentale aumenta i tipi di attività del sistema monitorati. In questo modo il connettore ha una prospettiva più ampia sul sistema e può rilevare attacchi comportamentali più complessi. Tuttavia, il monitoraggio di una maggiore quantità di attività del sistema comporta anche un rischio maggiore per il connettore di attacchi Denial of Service (DoS). Se il connettore è sovraccarico di attività del

sistema e entra in modalità degradata con errore 18, continua a monitorare gli eventi critici del sistema fino a quando l'attività complessiva del sistema non viene ridotta. Questa perdita di visibilità degli eventi del sistema riduce la capacità del connettore di proteggere il computer. È di fondamentale importanza che il sistema venga immediatamente sottoposto a indagini per individuare eventuali processi dannosi. Utilizzare il `top` (o simile) sul sistema Linux per visualizzare i processi attivi correnti e adottare le misure appropriate per correggere la situazione se vengono identificati processi potenzialmente dannosi.

Caso 4: Requisiti dei connettori

Il motore di protezione comportamentale migliora la capacità del connettore di proteggere l'attività del computer, ma per farlo deve consumare più risorse rispetto alle versioni precedenti. Se l'errore 18 viene sollevato frequentemente, non vi sono processi innocui che causano un carico elevato e non vi sono processi dannosi che agiscono sulla macchina, allora è necessario verificare che il sistema soddisfi i requisiti minimi di sistema.

Vedere anche

- Uso della CLI di Secure Endpoint Mac/Linux
- Errori del connettore Linux dell'endpoint sicuro Cisco
- Configurazione e identificazione delle esclusioni di Cisco Secure Endpoint
- Guida per l'utente di Secure Endpoint (PDF)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).