Cisco Secure Endpoint Linux Connector - fout 18

Inhoud

Inleiding

Dit document beschrijft fout 18 op de Secure Endpoint Linux-connector.

Fout 18: Connector voor gebeurtenisbewaking is overbelast

De Behavioral Protection-motor verbetert de zichtbaarheid van connectors in de systeemactiviteit. Door deze toename van het zicht is er een grotere kans dat de monitoring van de systeemactiviteit van de connector kan worden overweldigd door de hoeveelheid activiteit op het systeem. Als dit gebeurt, heft de connector fout 18 op en gaat hij over op gestoord bedrijf. Raadpleeg het artikel Cisco Secure Endpoint Linux Connector voor meer informatie over fout 18. Op de Linux Connector klikt u op de status De opdracht kan in de Secure Endpoint Linux CLI worden gebruikt om te zien of de connector in de gedegradeerde modus werkt en of er fouten worden hersteld. Als fout 18 is opgeheven, voert u de status De opdracht in de Secure Endpoint Linux CLI geeft de fout weer met een van de mogelijke twee snelheden:

1. Fout 18 met aanzienlijke ernst

```
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. Fout 18 met kritische ernst

```
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
```

Connector Event Monitoring is overbelast: zwaar

Wanneer fout 18 met grote strengheid wordt opgeheven, betekent dit dat de controle van de verbindingsgebeurtenis overbelast is maar nog een kleinere reeks systeemgebeurtenissen kan controleren. De connector switch in grote ernst en bewaakt minder gebeurtenissen equivalent aan de bewaking die beschikbaar was in connectors ouder dan 1.2.0. Als de vloed van systeemgebeurtenissen kort is en de gebeurteniscontrolelading in een aanvaardbaar bereik vermindert, dan wordt fout 18 gewist en de connector hervat de controle van alle systeemgebeurtenissen. Als de vloed van systeemgebeurtenissen verergert en de lading van de gebeurteniscontrole tot een kritieke hoeveelheid stijgt, dan wordt fout 18 verhoogd met kritieke strengheid en de schakelaar switches in kritieke strengheid.

Connector Event Monitoring is overbelast: kritieke ernst

Wanneer fout 18 met kritieke strengheid wordt opgeheven, betekent dit dat de connector een overweldigende hoeveelheid systeemgebeurtenissen ervaart die de connector in gevaar brengen. De connector switch in een beperktere kritische ernst. In deze status controleert de connector alleen kritieke gebeurtenissen zodat de connector kan opschonen en zich op herstel kan richten. Als de vloed van gebeurtenissen uiteindelijk terugloopt in een aanvaardbaarder bereik dan wordt de fout volledig gewist en de connector hervat de controle van alle systeemgebeurtenissen.

Advies voor foutactie

Als de connector ooit fout 18 met of grote of kritische ernst naar voren brengt, moeten bepaalde stappen worden genomen om het probleem te onderzoeken en op te lossen. De stappen om fout 18 op te lossen variëren afhankelijk van wanneer en waarom de fout is veroorzaakt:

1. Fout 18 is ontstaan op een nieuwe installatie van de Linux-connector
2. Fout 18 is opgetreden na recente wijzigingen in het besturingssysteem
3. Fout 18 is spontaan verhoogd

4. Fout 18 is opgetreden bij het opnieuw provisioneren van een machine met de Linux-connector die al is geïnstalleerd of bij het bijwerken van de connector naar versie 1.2.0+

Geval 1: Verse installatie

Als fout 18 en gedegradeerde modus worden waargenomen buiten een nieuwe installatie van de Linux-connector, moet u er eerst voor zorgen dat uw systeem aan de minimale systeemeisen voldoet. Nadat u hebt geverifieerd dat de vereisten voldoen aan of hoger zijn dan de minimumvereisten, moet u, als de fout blijft bestaan, de meest actieve processen op het systeem onderzoeken. U kunt de huidige actieve processen op een Linux-systeem bekijken met de top het bevel (of gelijkaardig) in de terminal. Als bekend is dat de processen die de hoogste CPU-hoeveelheid verbruiken benigne zijn, kunt u nieuwe procesuitsluitingen maken om te voorkomen dat deze processen worden bewaakt.

Voorbeeldscenario:

Veronderstel na nieuwe installatie, fout 18 en gedegradeerde wijze werden getoond via Secure Endpoint Linux CLI. Rde top de opdracht in een Ubuntu-machine toont deze actieve processen:

```
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
```

We zien dat er een zeer actief proces is, genaamd trusted_process in dit voorbeeld. In dit geval ben ik bekend met dit proces en het wordt vertrouwd, er is geen reden voor mij om wantrouwig te zijn over dit proces. Om fout 18 te verwijderen, kan het vertrouwde proces worden toegevoegd aan een procesuitsluiting in de Portal. Raadpleeg het artikel Cisco Secure Endpoint Exclusions configureren en identificeren om meer informatie te krijgen over de beste praktijken bij het maken van uitsluitingen.

Zaak 2: Recente veranderingen

Als u recente wijzigingen in uw besturingssysteem hebt aangebracht, zoals het installeren van een nieuw programma, kan fout 18 en een beschadigde modus worden waargenomen als deze nieuwe wijzigingen de systeemactiviteit vergroten. Gebruik dezelfde saneringsstrategie als in de nieuwe installatie is beschrevengeval, echter moet u op zoek zijn naar processen die verband houden met de recente wijzigingen, zoals een nieuw proces dat wordt uitgevoerd door een nieuw geïnstalleerd programma.

Zaak 3: Kwaadaardige activiteit

De Behavioral Protection-engine verhoogt de typen systeemactiviteit die worden gemonitord. Dit biedt de connector een breder perspectief op het systeem en geeft het de mogelijkheid om complexere gedragsaanvallen te detecteren. Nochtans, brengt de controle van een grotere hoeveelheid systeemactiviteit ook de schakelaar op een groter risico voor de ontkenning-van-dienst (Dos) aanvallen. Als de connector overweldigd is door systeemactiviteit en in de gestoorde modus terechtkomt met fout 18, blijft hij de

systeemkritische gebeurtenissen bewaken tot de totale systeemactiviteit is verminderd. Dit verlies in het zicht van systeemgebeurtenissen vermindert het vermogen van de connector om uw machine te beschermen. Het is van cruciaal belang dat u het systeem onmiddellijk onderzoekt voor kwaadaardige processen. Gebruik de `top` commando (of soortgelijk) op uw Linux-systeem om de huidige actieve processen te bekijken en passende actie te ondernemen om de situatie te verhelpen als er mogelijk schadelijke processen worden geïdentificeerd.

Geval 4: Connectorvereisten

De Behavioural Protection engine verbetert de mogelijkheid van de connector om uw machineactiviteit te beschermen, maar om dit te doen moet het meer resources verbruiken dan in eerdere versies. Als fout 18 vaak wordt opgeheven, zijn er geen goedaardige processen die zware lading veroorzaken, en er schijnen geen kwaadwillige processen te zijn die op de machine handelen, dan moet u ervoor zorgen uw systeem aan de minimum systeemvereisten voldoet.

Zie ook

- Gebruik de Secure Endpoint Mac/Linux CLI
- Fouten in Cisco Secure Endpoint Linux-connector
- Uitsluitingen van Cisco Secure Endpoint configureren en identificeren
- Gebruikershandleiding Secure Endpoint (PDF)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.