Probleemoplossing met fout-id 11 op SUSE Linux Secure Endpoint

Inhoud

Inleiding

In dit document wordt beschreven hoe het proces moet worden opgelost Fault ID 11 van Secure Endpoint on SUSE Linux Enterprise 15 SP2 .

Vereisten

De opdrachtregelinterface (CLI) is beschikbaar voor alle gebruikers van een systeem, hoewel de beschikbaarheid van sommige opdrachten afhankelijk is van de beleidsconfiguratie en/of de root permissies. De opdrachten die hiervan afhangen, worden in dit artikel openbaar gemaakt.

Cisco raadt kennis van de volgende onderwerpen aan:

- Linux Command Line
- Secure Endpoint

Gebruikte componenten

De in het document gebruikte informatie is gebaseerd op deze softwareversies:

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 kernel versie 5.3.18-24.96-default

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

On SUSE Linux Enterprise 15 Service Pack (SP) 2, met kernel versies groter dan of gelijk aan 5.3.18, connector gebruik eBPF modules voor real-time bestandssysteem en netwerkbewaking. Het eBPF

modules vervangt de Linux Kernel Modules die worden gebruikt wanneer de projector aanstaat RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 en eerder, en Amazon Linux 2 kernel 4.14 of eerder. Voor Ubuntu 18.04 en later, alsmede Debian 10 en later, eBPF modules zijn native.

Voor juiste compatibiliteit compileert de connector automatisch de eBPF modules die door de connector worden gebruikt voordat deze wordt geladen en op het systeem wordt uitgevoerd. Deze compilatie vereist dat de bestanden van de kernel-ontwikkelingsheader die overeenkomen met de huidige kernel-devel geïnstalleerd zijn. In real time filesystem en netwerk controle is ingeschakeld, compileert de connector de eBPF modules telkens wanneer de connector wordt gestart, of in real time wanneer deze functies zijn ingeschakeld, als onderdeel van een beleidsupdate.

Wanneer het systeem het huidige kernel-devel pakket mist, verhoogt de connector fout-ID 11: Realtime netwerk- en bestandsbewaking is niet beschikbaar. Installeer het kernel-ontwikkelpakket voor de momenteel actieve kernel en start vervolgens de Connector opnieuw. Het probleem met deze fout is dat de Linux-connector in een gedegradeerde staat draait. Dit betekent dat de connector niet werkt zoals verwacht totdat de fout is opgelost.

Problemen oplossen

Als fout 11 is opgeheven, wordt dit foutenlogboek weergegeven:

- Zoek logregels in het systeemlogboek /var/log/messages die vergelijkbaar zijn met deze:

init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.3.18-24.96-default'; skipping reinstalling kernel modules

In het logboek staat dat de huidige kernel-versie op de computer geen kernel-modules gebruikt voor filesystem en netwerkbewaking. Op kernel versies groter dan of gelijk aan 4.18, de filesystem en netwerken worden bewaakt met behulp van eBPF modules.

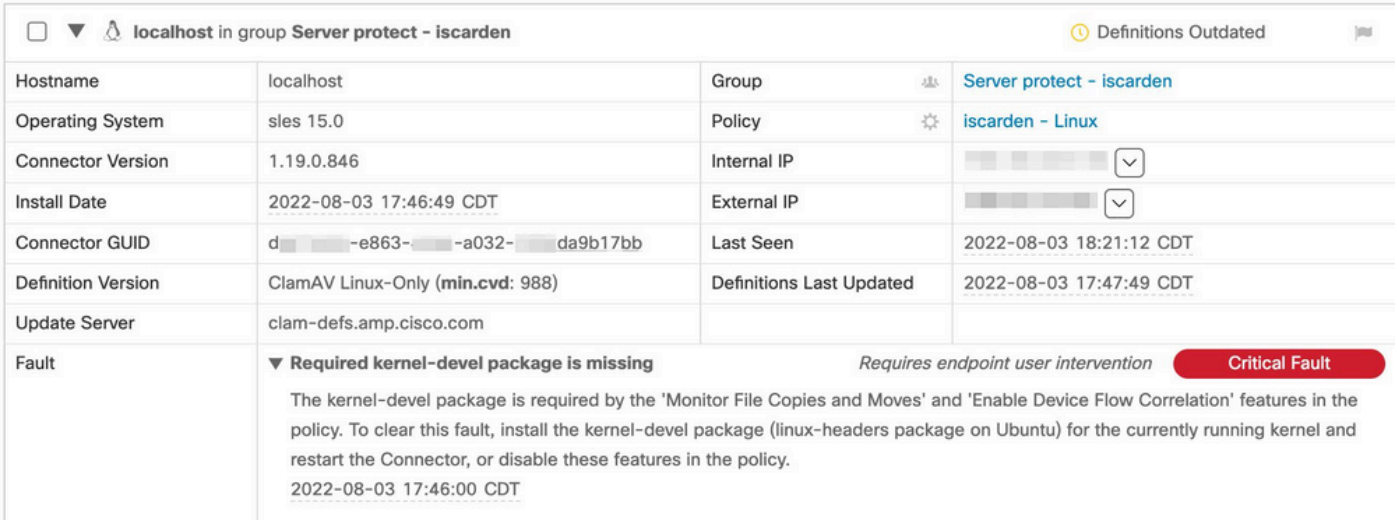
Hoe te om Absent Kernel-Headers te identificeren

Als de connector op een computer zonder kernelkoppen werkt, Fault ID 11 (Realtime network and file monitoring is unavailable), de connector in een afgebroken toestand werkt zonder filesystem of netwerkbewaking.
Deze stappen kunnen vanuit een terminalvenster worden uitgevoerd om te bepalen of de connector kernel-header aanwezig is of niet.

Stap 1. Controleer vanuit het betreffende apparaat of de -aansluiting Fault ID 11 :

/opt/cisco/amp/bin/ampcli # status [logger] Set minimum reported log level to notice Trying to connect... Connected. Status: Connected Mode: Degraded Scan: Ready for scan Last Scan: 2022-08-03 06:31:42 PM Policy: iscarden - Linux (#22192) Command-line: Enabled Orbital: Disabled Faults: 1 Critical Fault IDs: 11 ID 11 - Critical: Realtime network and file monitoring is unavailable. Install the kernel-devel package for the currently running kernel, then, restart the Connector.

Zoek vanuit de Secure Endpoint-console het betreffende apparaat en vouw de details uit om de foutsectie te verifiëren.



Stap 2. Controleer de huidige kernel met deze opdracht:

$ uname -r 5.3.18-150200.24.115-default

Stap 3. Om te controleren of de metalen headers al dan niet geïnstalleerd zijn:

zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")

De output moet als dit zijn:

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
```

Waar de i+ aangeeft dat het pakket is geïnstalleerd. Indien de linkerkolom v is **leeg**, moet het pakket worden geïnstalleerd.

Het SUSE de computer is geschikt voor de installatie van kernelkoppen als al deze waar zijn:

- De connector heeft fout-id 11.
- Het minimum kernel versie 5.3.18.
- Het kernel Kop- en kopregels zijn niet geïnstalleerd.

Resolutie

Indien de SUSE de machine heeft niet de vereiste kernelkoppen, dan kan deze procedure worden gebruikt om de vereiste kernelkoppen op de machine te installeren.

Stap 1. Installeer de benodigde kernelkoppen:

sudo zypper install --oldpackage kernel-default-devel=$(uname -r | sed 's/-default//') # sudo zypper install --oldpackage kernel-devel=$(uname -r | sed 's/-default//')

Stap 2. Start de connector opnieuw:

sudo systemctl stop cisco-amp # sudo systemctl start cisco-amp

Stap 3. Bevestig dat de fout is gewist:

/opt/cisco/amp/bin/ampcli # status Trying to connect... Connected. ampcli> status Status: Connected Mode: Normal Scan: Ready for scan Last Scan: 2022-08-05 01:29:47 PM Policy: iscarden - Linux (#22201) Command-line: Enabled Orbital: Disabled Faults: None ampcli > quit

Verifiëren

Om te controleren of de kernel headers nu geïnstalleerd zijn, voert u deze opdrachten uit:

zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")

Voordat u de tijdelijke oplossing uitvoerde, had u een output gelijkend op dit:

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed 's/
-default//') $ zypper se -s kernel-devel | grep $(uname -r | sed 's/-default//')
isaac@localhost:~>
```

Nadat u de tijdelijke oplossing hebt uitgevoerd, moet de uitvoer vergelijkbaar zijn met dit:

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~> zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")
i | kernel-devel | package | 5.3.18-24.96.1   | noarch | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~>
```

Gerelateerde informatie

- Controleer de compatibiliteit van Secure Endpoint Linux Connector
- Linux Kernel-Devel-fout
- Kernelmodules voor Cisco Secure Endpoint Linux-connector bouwen

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.