Risoluzione dei problemi relativi all'ID errore 11 sull'endpoint sicuro SUSE Linux

Sommario

Introduzione

Questo documento descrive il processo di risoluzione Fault ID 11 Secure Endpoint on SUSE Linux Enterprise 15 SP2 .

Requisiti

L'interfaccia della riga di comando (CLI) è disponibile per tutti gli utenti di un sistema, anche se la disponibilità di alcuni comandi dipende dalla configurazione dei criteri e/o dalle autorizzazioni della directory principale. I comandi dipendenti da questa funzione sono illustrati in questo articolo.

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Linux Command Line
- Secure Endpoint

Componenti usati

Le informazioni contenute nel documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

On SUSE Linux Enterprise 15 Service Pack (SP) 2 , con versioni del kernel maggiori o uguali a 5.3.18, il connettore utilizza eBPF moduli per il monitoraggio in tempo reale dei file system e della rete.

OSPF (Open Shortest Path First) eBPF sostituisce Linux Kernel Moduli utilizzati quando è in esecuzione su RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 e precedenti, e Amazon Linux 2 kernel 4.14 o precedente. Per Ubuntu 18.04 e successive, nonché Debian 10 e seguenti, eBPF i moduli sono nativi.

Per una corretta compatibilità, il connettore compila automaticamente eBPF moduli utilizzati dal connettore prima del caricamento e dell'esecuzione nel sistema. Questa compilazione richiede che i file di intestazione per lo sviluppo del kernel che corrispondono al kernel-devel sono installati. In tempo reale filesystem e il monitoraggio della rete è abilitato, il connettore compila eBPF ogni volta che viene avviato il connettore o in tempo reale quando queste funzionalità sono attivate, come parte di un aggiornamento dei criteri.

Quando il sistema non rileva il pacchetto di sviluppo del kernel corrente, il connettore genera l'ID errore 11: Rete in tempo reale e monitoraggio dei file non disponibile. Installare il pacchetto di sviluppo del kernel per il kernel attualmente in esecuzione, quindi riavviare il connettore. Il problema con questo errore è che il connettore Linux funziona in uno stato degradato, il che significa che non funziona come previsto finché il guasto non viene risolto.

Risoluzione dei problemi

Se viene generato l'errore 11, viene visualizzato il seguente log degli errori:

- Cerca righe nel registro eventi di sistema /var/log/messages simili a questo:

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

Il registro indica che la versione corrente del kernel nel computer non utilizza moduli kernel per filesystem e monitoraggio della rete. Nelle versioni del kernel maggiori o uguali a 4.18, il filesystem e la rete sono monitorate con l'utilizzo di eBPF moduli.

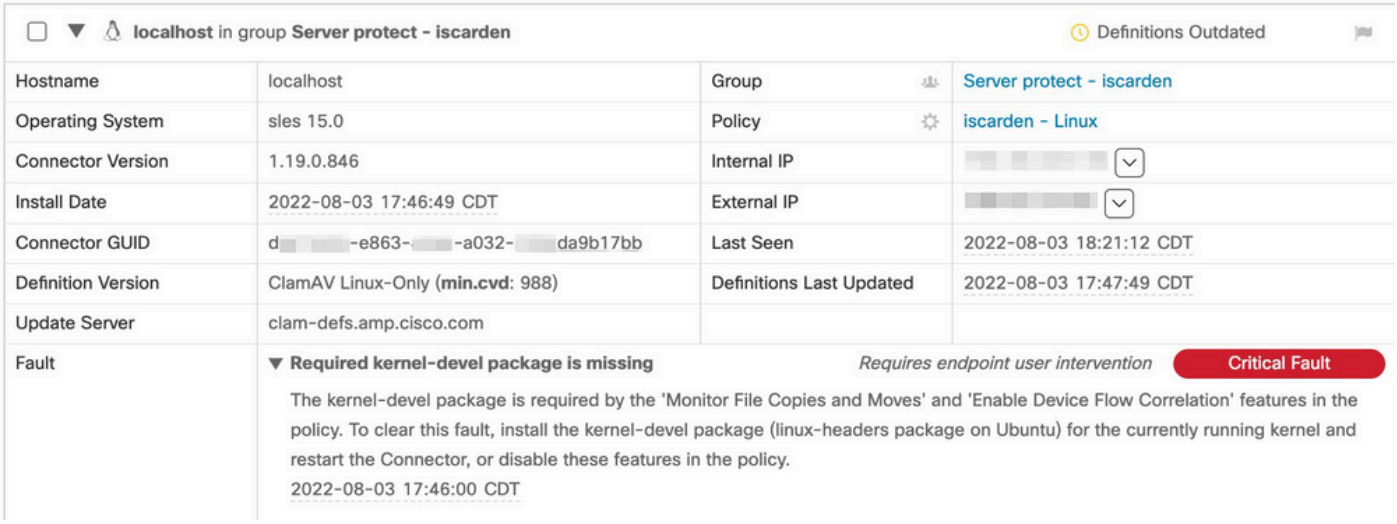
Come identificare le intestazioni del kernel assenti

Quando il connettore viene eseguito su un computer senza intestazioni del kernel, Fault ID 11 (Realtime network and file monitoring is unavailable), il connettore funziona in uno stato degradato senza filesystem o il monitoraggio della rete.
Questa procedura può essere eseguita da una finestra del terminale per stabilire se il connettore kernel-header è presente o no.

Passaggio 1. Dal dispositivo interessato, verificare che il connettore abbia 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.

Dalla console dell'endpoint sicuro individuare il dispositivo interessato ed espandere i dettagli per verificare la sezione relativa all'errore.



Passaggio 2. Controllare il kernel corrente con questo comando:

$ uname -r 5.3.18-150200.24.115-default

Passaggio 3. Per verificare se le intestazioni kernel sono installate:

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

L'output deve essere simile al seguente:

```
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
```

Dove i+ indica che il pacchetto è installato. Se la colonna sinistra è v oppure è **vuoto**, è necessario installare il pacchetto.

OSPF (Open Shortest Path First) SUSE il computer è adatto per l'installazione delle intestazioni del kernel se tutte queste condizioni sono vere:

- Il connettore ha l'ID errore 11.
- Il valore minimo kernel versione 5.3.18.
- OSPF (Open Shortest Path First) kernel intestazioni non installate.

Risoluzione

Se il SUSE Il computer non dispone delle intestazioni del kernel richieste, quindi questa procedura può essere utilizzata per installare le intestazioni del kernel richieste nel computer.

Passaggio 1. Installare le intestazioni del kernel necessarie:

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

Passaggio 2. Riavviare il connettore:

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

Passaggio 3. Confermare la cancellazione dell'errore:

/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

Verifica

Per verificare se le intestazioni del kernel sono state installate, eseguire questi comandi:

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

Prima di eseguire la soluzione, è stato generato un output simile al seguente:

```
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:~>
```

Dopo aver eseguito la soluzione, l'output deve essere simile al seguente:

```
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:~>
```

Informazioni correlate

- Verifica della compatibilità del sistema operativo del connettore Linux dell'endpoint sicuro
- Errore di sviluppo del kernel Linux
- Creazione di moduli kernel per i connettori Linux di Cisco Secure Endpoint

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).