Risoluzione dei problemi relativi ai connettori Linux dell'endpoint sicuro

Sommario

Introduzione

In questo documento vengono descritti gli errori utilizzati dal connettore Cisco Secure Endpoint Linux per notificare le condizioni che influiscono sul corretto funzionamento.

Premesse

Il connettore Cisco Secure Endpoint Linux notifica con un evento Generato da errore quando rileva una condizione che influisce sul corretto funzionamento del connettore. Analogamente, un evento Fault Cleared indica che la condizione non è più presente.

Tabella degli errori dei connettori Linux dell'endpoint sicuro

Nella tabella vengono descritti gli errori e i passi di diagnostica associati.

ID errore	Descrizione	Risoluzione dei problemi
5	Utente del servizio di digitalizzazione non disponibile	Il connettore non è riuscito a creare un utente per eseguire il processo di scansione dei file. Il connettore utilizza l'utente root per eseguire scansioni dei file come soluzione alternativa. Ciò si discosta dalla progettazione prevista e non è previsto. Se il `cisco-amp-scan-svc` l'utente o il gruppo è stato eliminato oppure la configurazione dell'utente e del gruppo è stata modificata, quindi è possibile reinstallare il connettore per ricreare l'utente e il gruppo con le configurazioni necessarie. Ulteriori informazioni sono disponibili all'indirizzo */var/log/cisco/ampdaemon.log*. Se la creazione del gruppo di utenti è limitata dalle impostazioni in **/etc/login.defs**, è necessario modificare temporaneamente il file durante l'esecuzione del programma di installazione per consentire la creazione dell'utente e del gruppo. A tale scopo, modificare **usergroups_enab** da no a yes. Questo errore può essere generato nei connettori Linux 1.15.1 e versioni successive se un altro programma ha modificato una delle autorizzazioni

		della directory del connettore (ovvero /opt/cisco o una directory figlio). Per risolvere questo problema, è necessario ripristinare le autorizzazioni predefinite della directory modificata (ad esempio 0755), assicurarsi che in futuro nessun programma modifichi la directory /opt/cisco (o eventuali directory figlio) e riavviare il servizio connettore.
6	Riavvio frequente del servizio di digitalizzazione	Il processo di scansione dei file del connettore ha rilevato errori ripetuti e il connettore è stato riavviato nel tentativo di cancellare l'errore. È possibile che uno o più file nel sistema causino l'arresto anomalo dell'algoritmo di scansione durante la scansione. Il connettore continua con le scansioni nel miglior modo possibile. Se l'errore non viene risolto automaticamente entro 10 minuti dall'avvio del connettore, significa che è necessario un ulteriore intervento dell'utente e che la capacità del connettore di eseguire scansioni è ridotta. Per ulteriori informazioni, visitare i siti Web agli indirizzi */var/log/cisco/ampdaemon.log*e */var/log/cisco/ampscansvc.log*.
7	Impossibile avviare il servizio di analisi	Impossibile avviare il processo di scansione dei file del connettore. Il connettore è stato riavviato nel tentativo di eliminare il problema. La funzionalità di analisi dei file è disabilitata quando viene generato l'errore. Questo errore può essere attivato se si verifica un errore durante il caricamento di un file di definizione dei virus (file con estensione cvd) appena installato. Il connettore esegue una serie di controlli di integrità e stabilità prima di attivare nuovi file con estensione cvd per evitare questo errore. Al riavvio, il connettore rimuove tutti i file .cvd non validi in modo che il connettore possa riprendere. Se il problema non viene risolto al riavvio del connettore, significa che è necessario un ulteriore intervento da parte dell'utente. Se l'errore si ripete a ogni aggiornamento con estensione cvd, significa che un file cvd non valido non viene rilevato correttamente dai controlli di integrità del file cvd del connettore. Questo errore può essere attivato nei connettori Linux se la memoria disponibile del computer è insufficiente e il servizio scanner non è in grado di avviarsi. Per i requisiti minimi di sistema su Linux, consultare la "Guida per l'utente di Secure Endpoint (in precedenza AMP for Endpoints)". Per ulteriori informazioni, visitare i siti Web agli indirizzi */var/log/cisco/ampdaemon.log*e */var/log/cisco/ampscansvc.log*.
8	Impossibile avviare il monitoraggio del file system in tempo reale	â€‹Il modulo del kernel che fornisce il monitoraggio dell'attività del file system in tempo reale non è stato caricato e per il criterio di connessione è abilitato "Controlla copie e spostamenti file". Queste funzioni di monitoraggio non sono disponibili nel connettore quando viene generato l'errore. Questo errore viene generato quando il connettore Secure Endpoint non è in grado di caricare il modulo kernel sottostante

		necessario per il monitoraggio dell'attività del file system. UEFI Secure Boot deve essere disabilitato sul sistema. Se l'avvio protetto è disabilitato, questo errore può essere causato da un'incompatibilità tra il modulo del kernel ampavflt o ampfsm fornito con il connettore Secure Endpoint e il kernel di sistema o altri moduli del kernel di terze parti installati nel sistema. Per informazioni dettagliate, vedere */var/log/messages* oppure disabilitare il monitoraggio dei file nelle impostazioni dei criteri del connettore per eliminare l'errore. L'errore può essere causato anche quando si esegue una versione del kernel non supportata dal connettore. In questo caso può essere cancellato creando un modulo del kernel ampfsm personalizzato per il kernel del sistema in esecuzione corrente. (Applicabile al connettore Linux versione 1.16.0 e successive). Per ulteriori informazioni sulla creazione di moduli kernel personalizzati, vedere: Building Cisco Secure Endpoint Linux Connector Kernel Modules
9	Impossibile avviare Monitoraggio rete in tempo reale	Il modulo del kernel che fornisce il monitoraggio in tempo reale dell'attività di rete non è stato caricato e nel criterio del connettore è abilitato "Abilita correlazione flusso dispositivo". Questa funzione di monitoraggio non è disponibile nel connettore quando viene generato l'errore. Questo errore viene generato quando il connettore Secure Endpoint non è in grado di caricare il modulo kernel sottostante necessario per il monitoraggio dell'attività del file system. UEFI Secure Boot deve essere disabilitato sul sistema. Se l'avvio protetto è disabilitato, questo errore può essere causato da un'incompatibilità tra il modulo del kernel ampavflt o ampfsm fornito con il connettore Secure Endpoint e il kernel di sistema o altri moduli del kernel di terze parti installati nel sistema. Per informazioni dettagliate, vedere */var/log/messages* oppure disabilitare il monitoraggio dei file nelle impostazioni dei criteri del connettore per eliminare l'errore. L'errore può essere causato anche quando si esegue una versione del kernel non supportata dal connettore. In questo caso può essere cancellato creando un modulo del kernel ampfsm personalizzato per il kernel del sistema in esecuzione corrente. (Applicabile al connettore Linux versione 1.16.0 e successive). Per ulteriori informazioni sulla creazione di moduli kernel personalizzati, vedere: Building Cisco Secure Endpoint Linux Connector Kernel Modules
11	Manca il pacchetto di sviluppo del kernel richiesto	Per le distribuzioni basate su Red Hat, il pacchetto di sviluppo del kernel richiesto per il monitoraggio in tempo reale del file system e dell'attività di rete è mancante e il criterio di connessione ha "Monitora copie e spostamenti file" o "Abilita correlazione flusso dispositivo" abilitato. Questo errore viene generato quando il connettore Secure Endpoint non è in grado di compilare e caricare il modulo eBPF sottostante necessario per il monitoraggio dell'attività del file system.

		Installare il pacchetto di sviluppo del kernel per il kernel attualmente in esecuzione e riavviare il connettore oppure disattivare queste funzionalità nel criterio per eliminare l'errore. (Applicabile solo ai connettori Linux versione 1.13.0 e successive). Per Oracle Linux UEK 6 e versioni successive, per queste funzioni è richiesto il package kernel-uek-devel. Installare il pacchetto kernel-uek-devel per il kernel attualmente in esecuzione e riavviare il connettore oppure disattivare queste funzionalità nel criterio per eliminare l'errore. (Applicabile solo ai connettori Linux versione 1.18.0 e successive). Per le distribuzioni basate su Debian, il pacchetto linux-headers è richiesto per queste funzioni. Installare il pacchetto linux-headers per il kernel attualmente in esecuzione e riavviare il connettore, o disabilitare queste funzionalità nel criterio per cancellare questo errore. (Applicabile al connettore Linux versione 1.15.0 e successive). Per maggiori informazioni, vedere: Errore di sviluppo del kernel Linux
16	Kernel incompatibile	Il kernel attualmente in esecuzione non è compatibile con il connettore in esecuzione e per il criterio del connettore è abilitato "Controlla copie e spostamenti file" o "Abilita correlazione flusso dispositivo". Effettuare il downgrade del kernel a una versione supportata o aggiornare il connettore a una versione più recente che supporta questo kernel. Per i dettagli sulle versioni del kernel supportate, vedere: Compatibilità con Cisco Secure Endpoint Linux Connector OS
18	Il monitoraggio degli eventi del connettore è sovraccarico	Questo errore viene generato quando il connettore è sottoposto a un carico elevato a causa di un numero eccessivo di eventi di sistema. La protezione del sistema è limitata e il connettore esegue il monitoraggio di un set ridotto di eventi critici del sistema fino a ridurre l'attività complessiva del sistema. Questo errore potrebbe indicare un'attività di sistema dannosa o applicazioni molto attive nel sistema. Se un'applicazione attiva è benigna e considerata attendibile dall'utente, può essere aggiunta a un set di esclusione di processo per ridurre il carico di monitoraggio sul connettore. Questa azione può essere sufficiente per eliminare il guasto. Se nessun processo innocuo provoca un carico di lavoro elevato, è necessaria un'indagine per determinare se l'aumento dell'attività è dovuto a un processo dannoso. Se il connettore è sottoposto a brevi periodi di carico elevato, è possibile che questo errore si risolva da solo. Se l'errore viene generato frequentemente, non esistono processi innocui

		che causano un carico elevato e non sono stati rilevati processi dannosi, è necessario eseguire nuovamente il provisioning del sistema per gestire carichi più pesanti.
19	Il criterio SELinux è mancante o disabilitato	Questo errore viene generato quando il criterio Secure Enterprise Linux (SELinux) del sistema impedisce al connettore di monitorare l'attività del sistema. Se SELinux è abilitato e in modalità di applicazione, il connettore richiede questa regola nella policy SELinux: `allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };` Sui sistemi basati su Red Hat, tra cui RHEL 7 e Oracle Linux 7, questa regola non è presente nel criterio SELinux predefinito. Durante un'installazione o un aggiornamento, il connettore tenta di aggiungere questa regola tramite l'installazione di un SELinux Policy Module denominato `cisco-secure-bpf`. Se `cisco-secure-bpf` non riesce a eseguire l'installazione e il caricamento oppure è disattivato, l'errore viene generato. Per risolvere il problema, reinstallare o aggiornare il Connettore in modo da attivare l'installazione di cisco-secure-bpf oppure aggiungere manualmente la regola al criterio SELinux esistente e riavviare il Connettore. Per istruzioni più dettagliate sulla modifica della policy SELinux per risolvere il problema, vedere SELinux Policy Fault.

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).