Errori del connettore Linux dell'endpoint sicuro Cisco

Sommario

Introduzione

Il connettore Cisco Secure Endpoint Linux può notificare un evento Generato da errori 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 errori connettore Linux endpoint sicuro

Nella tabella seguente vengono descritti gli errori e i passaggi diagnostici corrispondenti.

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 risolve il problema utilizzando l'utente root p eseguire la scansione dei file. Ciò si discosta dalla progettazione prevista e 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. Se si reinstalla il connettore, l'utente e il gruppo verranno ricreati con la configurazione necessaria. Ulteriori informazioni sono disponibili all'indirizzo */var/log/cisco/ampdaemon.log*. Se il cliente limita la creazione dei gruppi di utenti tramite le impostazioni in **/etc/login.defs**, è necessario modificare temporaneamente questo file duran l'esecuzione del programma di installazione per consentire la creazione dell'utente e del gruppo. A tale scopo, è possibile modificare **usergroups_en** no a yes.
6	Riavvio frequente del servizio di analisi	Questo errore può essere generato nei connettori Linux 1.15.1 e versioni successive se un altro programma ha modificato una delle autorizzazioni di directory del connettore (ad esempio /opt/cisco o una directory figlio). Per risolvere questo problema, è necessario ripristinare l'autorizzazione predefi della directory modificata, ad esempio 0755), assicurarsi che nessun progra futuro modifichi la directory /opt/cisco (o eventuali directory figlio) e riavviare servizio connettore. 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 ch uno o più file nel sistema causino l'arresto anomalo dell'algoritmo di scansio durante la scansione. Il connettore continua con le scansioni nel miglior mo 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 ch capacità del connettore di eseguire scansioni risulterà 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 connet è stato riavviato nel tentativo di eliminare il problema. La funzionalità di anal file è disabilitata quando viene generato l'errore. Questo errore può essere attivato se si verifica un errore durante il caricame di un file di definizione dei virus (file con estensione cvd) appena installato. connettore esegue una serie di controlli di integrità e stabilità prima di attiva nuovi file con estensione cvd per evitare questo errore. Al riavvio il connetto rimuoverà tutti i file .cvd non validi in modo che il connettore possa riprende 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 aggiornamento con estensione cvd, significa che un file cvd non valido non rilevato correttamente dai controlli di integrità del file cvd del connettore.
8	Impossibile avviare il monitoraggio del file system in tempo reale	Questo errore può essere attivato nei connettori Linux se la memoria dispor del computer è insufficiente e il servizio scanner non è in grado di avviarsi. I requisiti minimi di sistema su Linux, consultare la "Guida per l'utente di Secu 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*. 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 so disponibili nel connettore quando viene generato l'errore. Questo errore vien 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, il problema potrebbe 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 parti installati nel sistema. Per informazioni dettagliate o per disattivare il monitoraggio dei file nelle impostazioni dei criteri del connettore, vedere */var/log/messages*. L'errore può anche essere causato quando si esegue una versione del kern non supportata dal connettore. In questo caso può essere cancellato creand modulo del kernel ampfsm personalizzato per il kernel del sistema in esecu corrente (applicabile al connettore Linux versione 1.16.0 e successive). Per ulteriori informazioni sulla creazione di moduli kernel personalizzati, vedere: Creazione di moduli kernel per i connettori Linux di Cisco Secure Endpoint
9	Impossibile avviare Monitoraggio rete in tempo reale	Il modulo del kernel che fornisce il monitoraggio in tempo reale dell'attività d non è stato caricato e nel criterio del connettore è abilitato "Abilita correlazio flusso dispositivo". Questa funzione di monitoraggio non è disponibile nel connettore quando viene generato l'errore. Questo errore viene generato qu il connettore Secure Endpoint non è in grado di caricare il modulo kernel sottostante necessario per il monitoraggio dell'attività del file system.

11	Manca il pacchetto di sviluppo del kernel richiesto	UEFI Secure Boot deve essere disabilitato sul sistema. Se l'avvio protetto è disabilitato, il problema potrebbe 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 parti installati nel sistema. Per informazioni dettagliate o per disattivare il monitoraggio dei file nelle impostazioni dei criteri del connettore, vedere */var/log/messages*. L'errore può anche essere causato quando si esegue una versione del kern non supportata dal connettore. In questo caso può essere cancellato creand modulo del kernel ampfsm personalizzato per il kernel del sistema in esecu corrente (applicabile al connettore Linux versione 1.16.0 e successive). Per ulteriori informazioni sulla creazione di moduli kernel personalizzati, vedere: Creazione di moduli kernel per i connettori Linux di Cisco Secure Endpoint Per le distribuzioni basate su Red Hat, manca il pacchetto di sviluppo del ke necessario per il monitoraggio in tempo reale del file system e dell'attività di e nel criterio del connettore è abilitato "Controlla copie e spostamenti file" o "Abilita correlazione flusso dispositivo". Questo errore viene generato quand connettore dell'endpoint sicuro non è in grado di compilare e caricare il mod 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 n criterio per eliminare l'errore. (Applicabile solo ai connettori Linux versione 1 e successive). Per Oracle Linux UEK 6 e versioni successive, per queste funzioni è richies package kernel-uek-devel. Installare il pacchetto kernel-uek-devel per il kern attualmente in esecuzione e riavviare il connettore oppure disattivare queste funzionalità nel criterio per eliminare l'errore. (Applicabile solo ai connettori l versione 1.18.0 e successive). Per le distribuzioni basate su Debian, il pacchetto linux-headers è richiesto queste funzioni. Installare il pacchetto linux-headers per il kernel attualment esecuzione e riavviare il connettore, o disabilitare queste funzionalità nel cri per cancellare questo errore. (Applicabile al connettore Linux versione 1.15. 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 Secure Endpoint Linux Connector OS