Errori del connettore Mac dell'endpoint sicuro Cisco

Sommario

Introduzione

Il connettore può notificare 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 errori connettore

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

ID errore	Testo portale	Endpoint Descrizione	Risoluzione dei problemi
1	Modulo kernel non autorizzato	Estensione di sistema non autorizzata	L'esecuzione dell'estensione di sistema del connettore è stata bloccata. Aprire Protezione e Privacy System Preferences e approvare l'estensione. In alternativa, le estensioni di sistema possono essere approvate in remoto utilizzando un profilo MDM (Mobile Device Management).
2	Versione non corrispondente	Versione dell'estensione di sistema non corrispondente	Il software Connettore installato è danneggiato. Reinstallare il connettore. Nota: quando si esegue Mac Connector versione 1.14.0 e successive, alcune occorrenze dell'errore possono essere cancellate riavviando il computer.
3	Accesso al disco non concesso	Accesso completo al disco non concesso	Il connettore non può accedere ai file utente per la scansione. Aprire Preferenz sistema relative alla protezione e alla privacy e concedere l'accesso completo disco rigido per il servizio AMP. Per le versioni Mac Connector precedenti alla 1.14.0, questo processo è denominato */opt/cisco/amp/ampdaemon*. Per Mac Connector versione 1.14.0 e successive, le due applicazioni seguenti richiedono l'accesso completo al disco a seconda della versione macOS: • *AMP for Endpoints Servizio* (necessario per tutte le versioni macOS) • *AMP Security Extension* (richiesto su macOS 10.15.5 e versioni successiv Per Mac Connector versione 1.14.1 e successive, le due applicazioni seguenti richiedono l'accesso completo al disco a seconda della versione macOS: • *AMP for Endpoints Servizio* (necessario per tutte le versioni macOS) • *AMP Security Extension* (richiesto su macOS 11 e versioni successive) Ulteriori informazioni sono disponibili in questa nota tecnica.

4	Modulo kernel non caricato	Impossibile caricare l'estensione di sistema. reinstallare il connettore	Per le versioni Mac Connector precedenti alla 1.14.0 o quando viene eseguito macOS 10.14 o 10.15, questo errore indica che l'estensione di sistema del Connector è la versione corretta ed è stata approvata per l'esecuzione ma non ancora stata caricata. Per ulteriori informazioni, visitare il sito */Library/Logs/Cisco/ampdaemon.log*. Anche la disinstallazione e la reinstallazio del connettore possono risolvere il problema.
5	Utente del servizio di digitalizzazione non disponibile	Utente del servizio di digitalizzazione non disponibile	Il connettore non è riuscito a creare un utente per eseguire il processo di scans dei file. Il Connettore risolve il problema utilizzando l'utente root per eseguire la scansione dei file. 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. Se si reinstalla Connector, l'utente e il gruppo verranno nuovamente creati con la configurazio necessaria. Ulteriori informazioni sono disponibili all'indirizzo */Library/Logs/Cisco/ampdaemon.log*.
6	Riavvio frequente del servizio di analisi	Riavvio frequente del servizio di analisi	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 più file nel sistema causino l'arresto anomalo dell'algoritmo di scansione duran scansione. Il connettore continua con le scansioni nel miglior modo possibile. Se il problema non viene risolto automaticamente entro 10 minuti dall'avvio de connettore, significa che è necessario un ulteriore intervento da parte dell'uten che la capacità del connettore di eseguire le scansioni risulterà ridotta. Revisione */Library/Logs/Cisco/ampdaemon.log* e */Library/Logs/Cisco/ampscansvc.log* per ulteriori dettagli.
7	Impossibile avviare il servizio di analisi	Impossibile avviare il servizio di analisi	Impossibile avviare il processo di scansione dei file del connettore. Il connettor stato riavviato nel tentativo di risolvere il problema. La funzionalità di analisi de è disabilitata quando viene generato l'errore. Questo errore può essere attivato se si verifica un errore durante il caricament 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 file con estensione cvd per evitare questo errore. Al riavvio, il Connettore rimu 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 neces 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 vie rilevato correttamente dai controlli di integrità del file cvd del connettore. Revisione */Library/Logs/Cisco/ampdaemon.log* e */Library/Logs/Cisco/ampscansvc.log* per ulteriori dettagli.
10	Riavvio necessario per caricare il modul	Riavvio necessario per caricare le estensioni di sistema	Riavviare il sistema. Per Mac Connector versioni 1.11.1 e 1.14.0, questo errore può essere generat non è possibile caricare le estensioni di sistema. In questo caso, è possibile risolvere il problema reinstallando il connettore. Si noti che Mac Connector 1.14.1 e versioni successive potrebbe causare que errore se nel sistema sono installate troppe estensioni del sistema Network Co Filter. Se il riavvio del computer non risolve il problema, consultare le istruzion

	o del kernel o l'estensione di sistema		l'errore 13 riportate di seguito.
12	Filtro di rete non consentito	Filtro di rete non consentito	Il filtro di rete è richiesto dalla funzionalità 'Abilita correlazione flusso dispositiv criterio. Per eliminare l'errore, consentire a 'AMP for Endpoints Service' di filtra contenuto di rete nell'endpoint. Èpossibile accedere alla finestra di dialogo macOS per consentire il filtro di ret facendo clic sull'errore attivo elencato nel menu Agente e seguendo le istruzio fornite. Ulteriori informazioni, incluse le impostazioni del profilo MDM per l'autorizzazio remota dei filtri di rete, sono disponibili in questa nota tecnica.
13	Troppe estensioni del sistema di filtro del contenuto di rete	Troppe estensioni del sistema di filtro del contenuto di rete	Per Mac Connector 1.14.0, questo errore viene spesso generato a causa di ur macOS all'avvio dell'estensione di sistema del filtro del contenuto di rete. Il riav del computer eliminerà questo errore. La funzionalità 'Abilita correlazione flusso dispositivo' nel criterio richiede l'utiliz un filtro del contenuto di rete macOS di livello firewall. MacOS limita il numero filtri del contenuto di rete che è possibile eseguire. Se l'errore viene generato e non viene risolto riavviando il computer, disinstalla filtri del contenuto di rete di livello firewall non più necessari e riavviare Connec
14	Troppe estensioni del sistema di sicurezza degli endpoint	Troppe estensioni di sistema di Endpoint Security	MacOS limita il numero di estensioni di sistema di Endpoint Security che posso essere in esecuzione. Il connettore Mac richiede una delle seguenti estensioni sistema di Endpoint Security per le funzionalità 'Esegui monitoraggio copie e spostamenti file' e 'Esegui monitoraggio processo' nel criterio . Per risolvere il problema, disinstallare le estensioni di sistema di Endpoint Sec non più necessarie e riavviare il connettore.
15	L'estensione del sistema richiede l'accesso completo al disco	L'estensione del sistema richiede l'accesso completo al disco	Le estensioni di sistema macOS del connettore Mac non possono accedere ai utente per la scansione. Aprire le Preferenze di sistema relative alla protezione alla privacy e concedere l'accesso completo al disco rigido all'*estensione di protezione AMP*. In questa nota tecnica sono disponibili ulteriori dettagli, incluse le impostazioni profilo MDM per l'autorizzazione remota dell'accesso completo al disco con estensioni di sistema. Si noti che un bug su macOS 11.0.0 può causare la cancellazione spontanea dell'impostazione di accesso completo al disco al momento del riavvio, dopo c stata concessa. Questo bug è stato risolto in macOS 11.0.1.
17	Accesso Orbital	Accesso Orbitale Completo	Orbital richiede l'accesso completo al disco per accedere ai file e alle directory protetti per le query. Aprire le preferenze di sistema relative alla sicurezza e al privacy e concedere l'accesso completo al disco rigido a *Cisco Orbital.*

e
Compl
eto Al
Disco
Non
Conce
sso

Al Disco
Non
Concesso