

Risolvere i problemi relativi a un corner case dell'errore "Unable to Retrieve SBRS"

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta una richiesta ad angolo rilevata per l'errore "Unable to retrieve SBRS" (Impossibile recuperare SBRS) in Email Security Appliance (ESA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Appliance

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Email Appliance

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

L'ESA non riesce a recuperare il punteggio SBRS per tutti gli indirizzi IP dei mittenti. La connessione ai server Cisco Cloud sulla porta 443 (HTTPS) ha esito negativo con errori TLS.

I punteggi della reputazione di base del mittente (SBRS) sono punteggi assegnati agli indirizzi IP in base a una combinazione di fattori, tra cui il volume e la reputazione della posta elettronica.

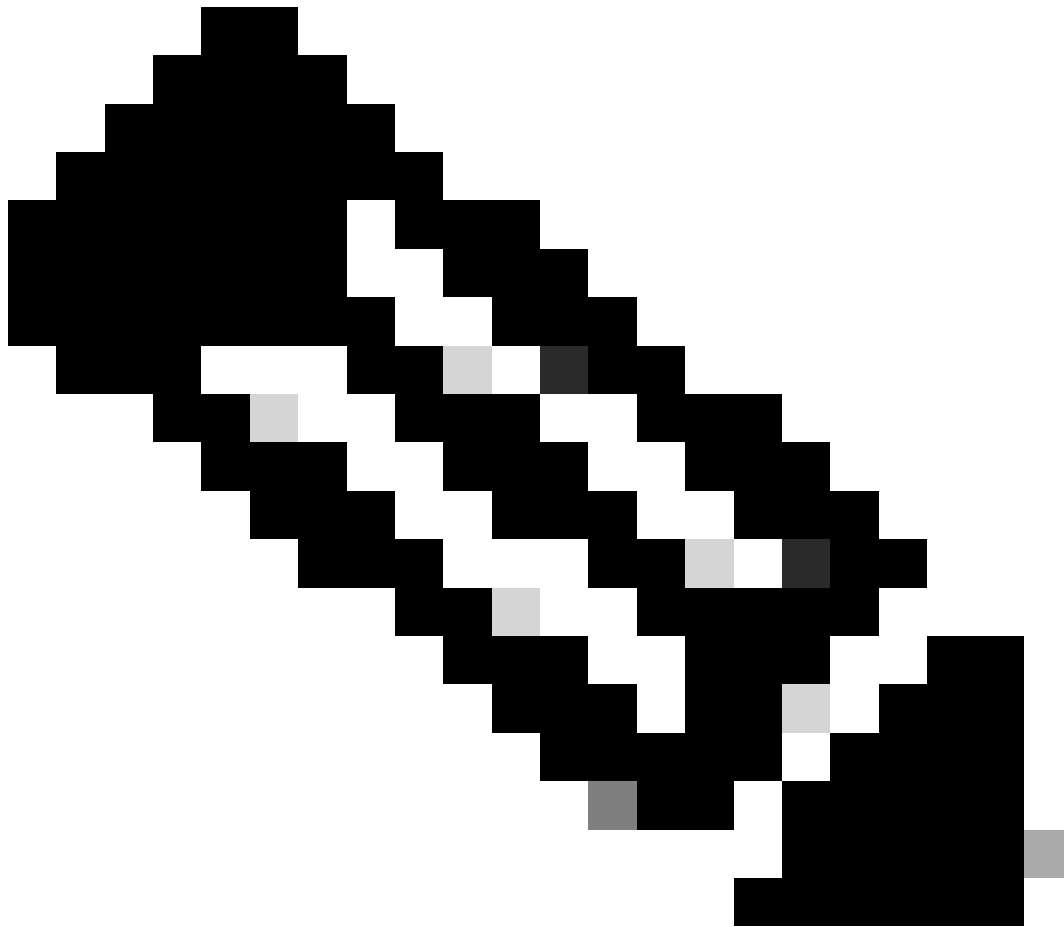
Problema

L'appliance ESA non è in grado di recuperare il punteggio SBRS, causando ritardi nella posta elettronica. Nonostante la corretta connessione ai server SBRS e SDR, l'accessorio non riesce ad aggiornare i componenti e il comando sdrdiagnostics visualizza lo stato della connessione "Non connesso" al servizio di reputazione del dominio del mittente Cisco.

Soluzione

Connettività al server SBRS non riuscita a causa di un certificato interno scaduto. L'ESA è progettata per rinnovare automaticamente il presente certificato. Tuttavia, in rari casi, problemi di connettività con i server di aggiornamento/download impediscono all'ESA di rinnovarla automaticamente, generando errori TLS. L'accessorio deve essere collegato ai server di aggiornamento per consentire l'aggiornamento del certificato interno:

- update-manifests.ironport.com sulla porta 443
- updates.ironport.com sulla porta 80
- downloads.ironport.com sulla porta 80



Nota: Eseguire sdrdiagnostics dalla riga di comando. Uno stato connesso conferma la connettività.

Informazioni correlate

- [Guida alle informazioni su Cisco ESA Firewall](#)
- [Guida SBRS](#)
- [Supporto tecnico Cisco e download](#)

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).