

Solucionar um problema de canto do erro "Não foi possível recuperar SBRS"

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve um caso de canto encontrado para o erro "Não é possível recuperar SBRS" no Email Security Appliance (ESA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Email Appliance

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Email Appliance

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O ESA não consegue recuperar a pontuação SBRS para todos os endereços IP do remetente. A conexão com os servidores em nuvem da Cisco na porta 443 (HTTPS) falha com erros TLS.

As Pontuações de Reputação Básicas do Remetente (SBRS) são pontuações atribuídas aos endereços IP com base em uma combinação de fatores, incluindo volume de e-mail e reputação.

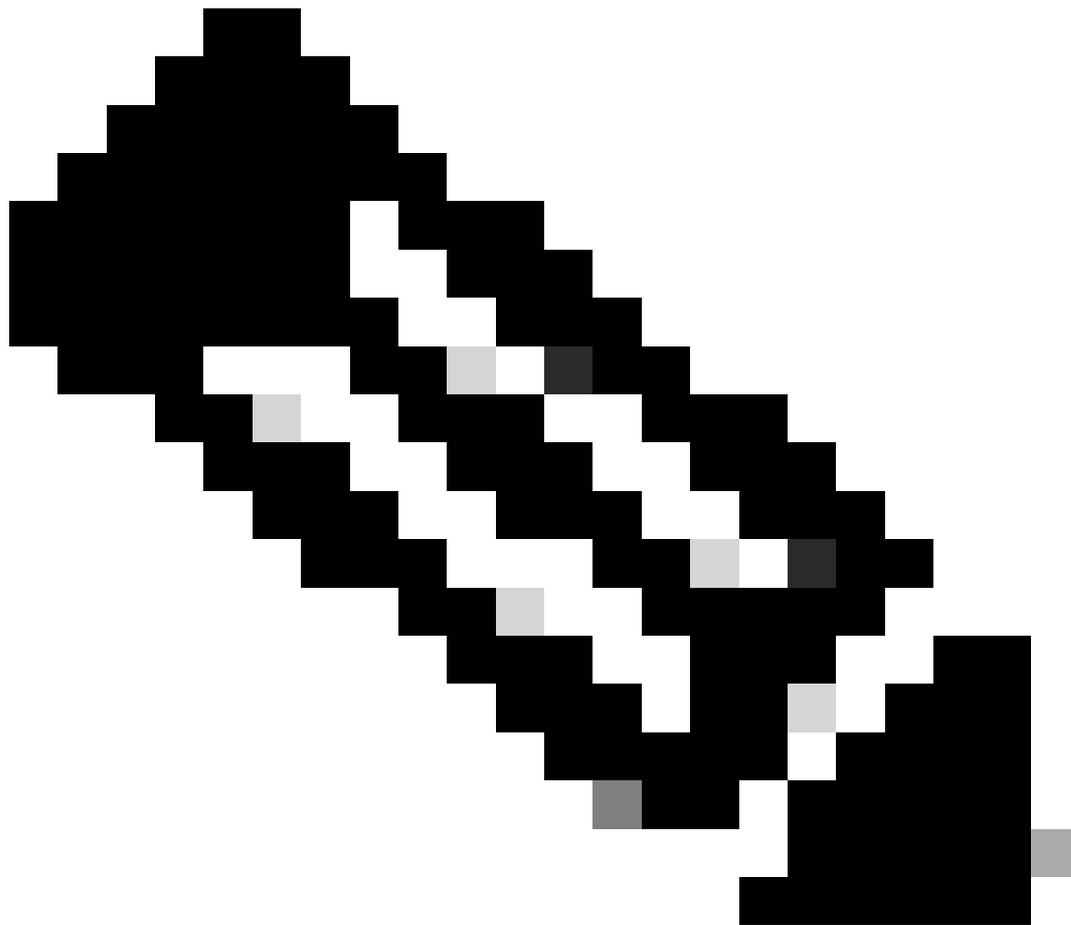
Problema

O dispositivo ESA não consegue recuperar a pontuação SBRS, causando atrasos de e-mail. Apesar da conectividade bem-sucedida com os servidores SBRS e SDR, o dispositivo não atualiza os componentes e o comando sdrdiagnostics exibe um status de conexão de "Não conectado" com o Cisco Sender Domain Reputation Service.

Solução

Falha na conectividade do servidor SBRS devido a um certificado interno expirado. O ESA foi projetado para renovar automaticamente este certificado. No entanto, em casos raros, problemas de conectividade com servidores de atualização/download impedem que o ESA o renove automaticamente, resultando em erros de TLS. O equipamento deve se conectar aos servidores de atualização para permitir que o certificado interno seja atualizado:

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



Note: Execute o `sdrdiagnostics` na linha de comando. Um estado conectado confirma a conectividade.

Informações Relacionadas

- [Guia de informações do firewall Cisco ESA](#)
- [Guia SBRS](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.