Solucionar problemas de un caso de esquina del error "No se puede recuperar SBRS"

Contenido

Introducción

Este documento describe un caso de esquina encontrado para el error "No se puede recuperar SBRS" en el dispositivo de seguridad de correo electrónico (ESA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo Cisco Secure Email

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo Cisco Secure Email

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El ESA no puede recuperar la puntuación SBRS para todas las direcciones IP del remitente. La conexión a los servidores en la nube de Cisco en el puerto 443 (HTTPS) falla con errores de TLS.

Las puntuaciones de reputación de Sender Base (SBRS) son puntuaciones que se asignan a direcciones IP en función de una combinación de factores, incluidos el volumen y la reputación del correo electrónico.

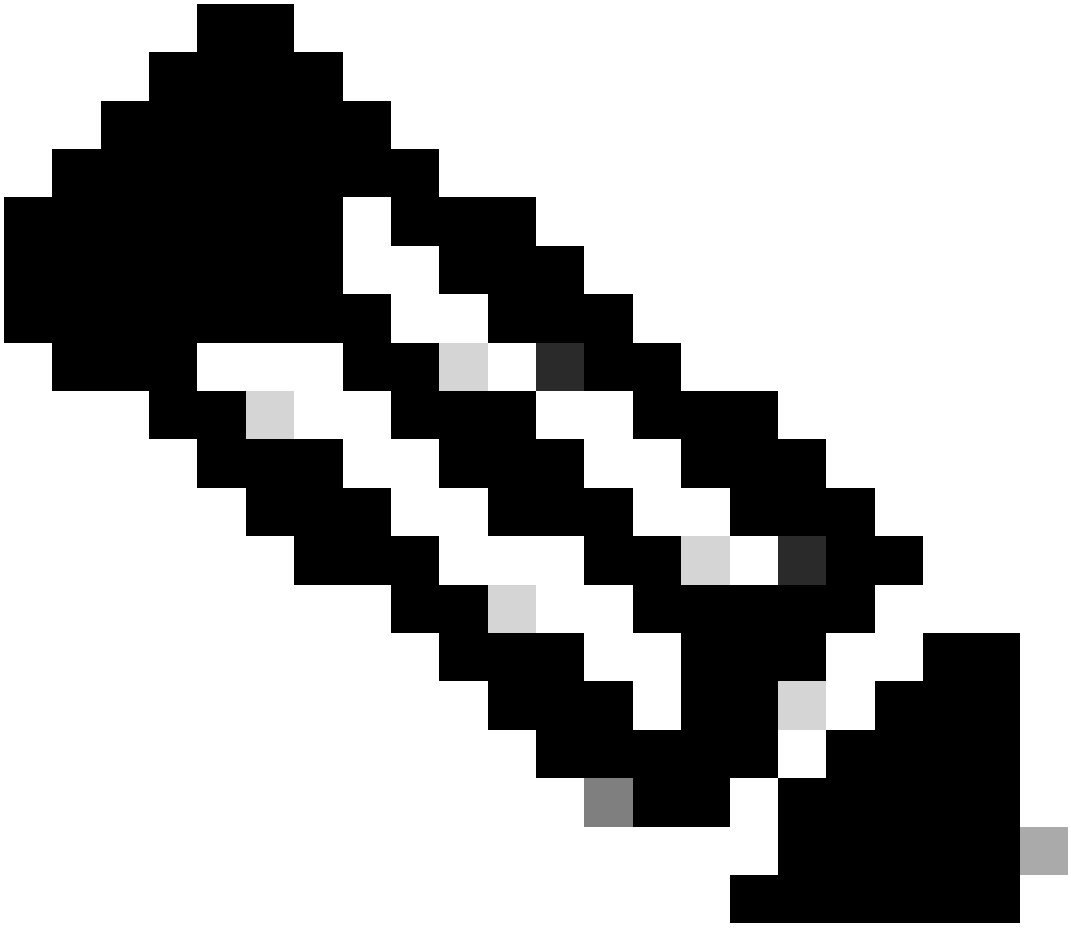
Problema

El dispositivo ESA no puede recuperar la puntuación SBRS, lo que causa retrasos en los correos electrónicos. A pesar de la conectividad exitosa con los servidores SBRS y SDR, el dispositivo no puede actualizar los componentes y el comando sdrdiagnostics muestra un estado de conexión de "No conectado" al Servicio de reputación de dominio de remitentes de Cisco.

Solución

La conectividad del servidor SBRS falla debido a un certificado interno caducado. El ESA está diseñado para renovar automáticamente este certificado. Sin embargo, en raras ocasiones, los problemas de conectividad con los servidores de actualización/descarga impiden que el ESA lo renueve automáticamente, lo que resulta en errores de TLS. El dispositivo debe conectarse a los servidores de actualización para permitir que el certificado interno se actualice:

- update-manifests.ironport.com en el puerto 443
- updates.ironport.com en el puerto 80
- downloads.ironport.com en el puerto 80



Nota: Ejecute sdrdiagnostics desde la línea de comandos. Un estado conectado confirma la conectividad.

Información Relacionada

- Guía de información de Cisco ESA Firewall
- Guía SBRS
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).