Dépannage d'un cas d'angle de l'erreur " ; Impossible de récupérer SBRS" ;

Table des matières

Introduction

Ce document décrit un cas d'angle rencontré pour l'erreur « Unable to recover SBRS » sur l'appareil de sécurité de la messagerie (ESA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil de messagerie électronique sécurisé Cisco

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil de messagerie électronique sécurisé Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

ESA ne parvient pas à récupérer le score SBRS pour toutes les adresses IP des expéditeurs. La connexion aux serveurs cloud Cisco sur le port 443 (HTTPS) échoue avec des erreurs TLS.

Les SBRS (Sender Base Reputation Scores) sont des scores qui sont attribués à des adresses IP en fonction d'une combinaison de facteurs, notamment le volume d'e-mails et la réputation.

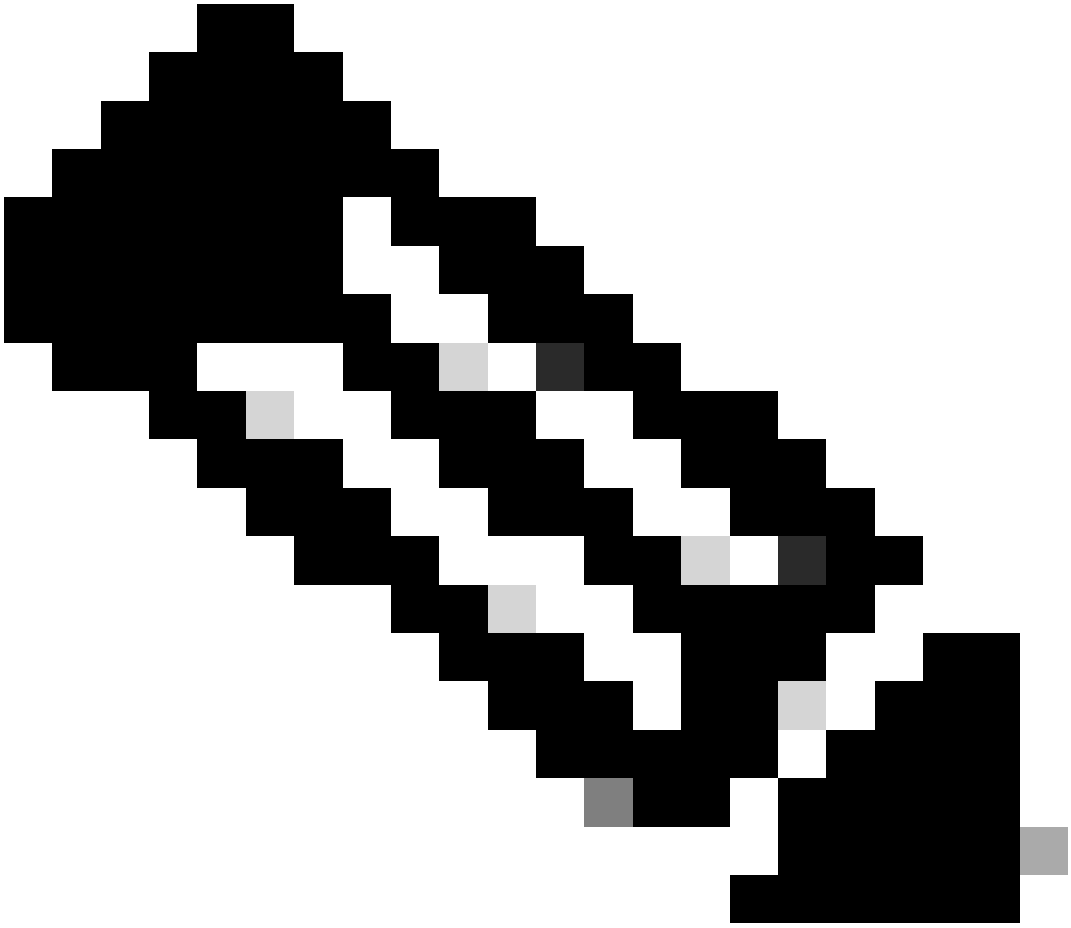
Problème

L'appliance ESA ne peut pas récupérer le score SBRS, ce qui entraîne des retards dans la transmission des e-mails. En dépit d'une connectivité réussie aux serveurs SBRS et SDR, l'appliance ne parvient pas à mettre à jour les composants et la commande sdrdiagnostics affiche l'état de connexion « Non connecté » au service de réputation de domaine de l'expéditeur Cisco.

Solution

La connectivité du serveur SBRS échoue en raison de l'expiration d'un certificat interne. L'ESA est conçu pour renouveler automatiquement ce certificat. Cependant, dans de rares cas, des problèmes de connectivité avec les serveurs de mise à jour/téléchargement empêchent l'ESA de le renouveler automatiquement, ce qui entraîne des erreurs TLS. L'appliance doit se connecter aux serveurs de mise à jour pour permettre la mise à jour du certificat interne :

- update-manifests.ironport.com sur le port 443
- updates.ironport.com sur le port 80
- downloads.ironport.com sur le port 80



Remarque : Exécutez sdrdiagnostics à partir de la ligne de commande. Un état connecté confirme la connectivité.

Informations connexes

- Guide d'information sur le pare-feu Cisco ESA
- guide SBRS
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.