Agrupación en clústeres deshabilitada en ASA esclavo (RPC_SYSTEMERROR)

Contenido

Introducción

Este documento describe cómo resolver un mensaje de error que podría aparecer cuando intenta agregar una nueva unidad esclava de Adaptive Security Appliance (ASA) a un clúster existente de ASA.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la agrupación en clústeres
- Conocimientos básicos sobre cómo configurar el clustering en ASA
- Conocimiento básico del protocolo de enlace Secure Socket Layer (SSL)

Componentes Utilizados

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

- Software ASA versión 9.0 o posterior
- Dispositivos ASA serie 5580 o ASA5585-X

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Antecedentes

La agrupación en clústeres le permite combinar varios ASA físicos en una unidad lógica, lo que proporciona un mayor rendimiento y redundancia. Para obtener más información sobre clustering, refiérase a la Guía de Configuración CLI de Cisco ASA Series, 9.0.

En este escenario, el clustering se ha configurado y habilitado en el ASA maestro; en el ASA esclavo, el agrupamiento se ha configurado pero no se ha habilitado.

Problema

Cuando habilita la agrupación en clúster en el ASA esclavo, se inhabilita inmediatamente con un mensaje de error de llamada a procedimiento remoto (RPC). Este es un ejemplo del mensaje de error:

```
ASA2/ClusterDisabled(config)# cluster group TEST-Group
ASA2/ClusterDisabled(cfg-cluster)# enable as-slave
INFO: This unit will be enabled as a cluster slave without sanity check and confirmation.
ASA2/ClusterDisabled(cfg-cluster)# cluster_ccp_make_rpc_call failed to clnt_call. msg is
CCP_MSG_REGISTER,
ret is RPC_SYSTEMERROR
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering
or remove cluster group configuration.
```

Una razón posible para este error es una discordancia del conjunto de claves SSL entre el ASA maestro y el ASA esclavo. La agrupación en clústeres requiere que haya al menos un conjunto de cifrado SSL coincidente entre la unidad maestra y la unidad esclava para agregarlo al clúster. Refiérase a este requisito en la Guía de Configuración CLI de Cisco ASA Series, 9.0:

Los nuevos miembros del clúster deben utilizar la misma configuración de cifrado SSL (el comando de cifrado SSL) que la unidad principal.

En el escenario de discordancia, se registra un mensaje syslog :

```
%ASA-7-725014: SSL lib error. Function: SSL23_GET_SERVER_HELLO Reason: sslv3 alert handshake
failure
```

Un ejemplo de discordancia es este cifrado en el ASA maestro:

```
ASA1/master# sh run all ssl
ssl server-version any
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
```

Y este cifrado en el ASA esclavo que se agregará al clúster:

```
ASA2/ClusterDisabled# sh run all ssl
ssl server-version any
ssl client-version any
ssl encryption des-sha1
```

Esta discordancia suele producirse cuando no se ha instalado una licencia de cifrado fuerte (3DES/AES) en el ASA esclavo. La lista de los conjuntos de aplicaciones de cifrado en el ASA esclavo es **des-sha1** y no se actualiza cuando se agrega la licencia 3DES/AES al ASA esclavo.

Hay dos soluciones para esta discordancia.

Solución 1

En el ASA maestro, agregue **des-sha1** como un conjunto de cifrado SSL válido:

```
ASA1/master# configuration terminal
ASA1/master(config)# ssl encryption des-sha1
```

> Nota: Cisco no recomienda que habilite **des-sha1** porque es un cifrado débil y se considera vulnerable.

Solución 2

En el ASA esclavo, agregue al menos uno de estos conjuntos de cifrado SSL: **rc4-sha1**, **aes128-sha1**, **aes256-sha1** o **3des-sha1**:

```
ASA2/ClusterDisabled# configuration terminal
ASA2/ClusterDisabled(config)# ssl encryption rc4-sha1
```

Información Relacionada

- Guía de Configuración de Cisco ASA Series CLI, 9.0
- Soporte Técnico y Documentación - Cisco Systems