Mise en grappe désactivée sur l'ASA esclave (RPC_SYSTEMERROR)

Contenu

Introduction

Ce document décrit comment résoudre un message d'erreur qui peut apparaître lorsque vous essayez d'ajouter une nouvelle unité ASA (Adaptive Security Appliance) esclave à un cluster ASA existant.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base en matière de regroupement
- Connaissances de base sur la configuration du clustering sur l'ASA
- Connaissance de base de la connexion SSL (Secure Socket Layer)

Components Used

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

- Logiciel ASA version 9.0 ou ultérieure
- Appareils ASA 5580 ou ASA5585-X

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

La mise en grappe vous permet de combiner plusieurs ASA physiques en une seule unité logique, ce qui augmente le débit et la redondance. Pour plus d'informations sur la mise en grappe, reportez-vous au Guide de configuration CLI de la gamme Cisco ASA, version 9.0.

Dans ce scénario, le clustering a été configuré et activé sur l'ASA maître ; sur l'ASA esclave, le clustering a été configuré mais n'est pas activé.

Problème

Lorsque vous activez la mise en grappe sur l'ASA esclave, elle est désactivée immédiatement avec un message d'erreur RPC (Remote Procedure Call). Voici un exemple du message d'erreur :

```
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.
```

Une des raisons possibles de cette erreur est une non-correspondance de la suite de chiffrement SSL entre les ASA maître et esclave. La mise en grappe nécessite au moins une suite de chiffrement SSL correspondante entre le maître et l'unité esclave à ajouter au cluster. Référez-vous à cette exigence dans le Guide de configuration CLI de la gamme Cisco ASA, 9.0 :

Les nouveaux membres du cluster doivent utiliser le même paramètre de cryptage SSL (la commande de cryptage SSL) que l'unité maître.

Dans le scénario de non-correspondance, un message syslog est enregistré :

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

Un exemple de non-correspondance est ce chiffrement sur l'ASA maître :

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

Et ce chiffrement sur l'ASA esclave à ajouter au cluster :

```
ASA2/ClusterDisabled# sh run all ssl
ssl server-version any
```

```
ssl client-version any
ssl encryption des-sha1
```

Cette incompatibilité se produit généralement lorsqu'une licence de chiffrement fort (3DES/AES) n'a pas été installée sur l'ASA esclave. La liste des suites de chiffrement sur l'ASA esclave prend par défaut **des-sha1** et n'est pas mise à jour lorsque la licence 3DES/AES est ajoutée à l'ASA esclave.

Il y a deux solutions à cette incompatibilité.

Solution 1

Sur l'ASA maître, ajoutez **des-sha1** en tant que suite de chiffrement SSL valide :

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

> **Note**: Cisco ne vous recommande pas d'activer **des-sha1** car il s'agit d'un chiffrement faible et est considéré comme vulnérable.

Solution 2

Sur l'ASA esclave, ajoutez au moins une de ces suites de chiffrement SSL : **rc4-sha1**, **aes128-sha1**, **aes256-sha1** ou **3des-sha1** :

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

Informations connexes

- Guide de configuration de l'interface de ligne de commande de la gamme Cisco ASA, 9.0
- Support et documentation techniques - Cisco Systems