Clustering disabilitato su ASA slave (RPC_SYSTEMERROR)

Sommario

Introduzione

In questo documento viene descritto come risolvere un messaggio di errore che potrebbe essere visualizzato quando si tenta di aggiungere una nuova unità ASA (Adaptive Security Appliance) slave a un cluster esistente di appliance ASA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di clustering
- Conoscenze base di come configurare il clustering sull'appliance ASA
- Conoscenze base dell'handshake SSL (Secure Sockets Layer)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software ASA versione 9.0 o successive
- Appliance ASA serie 5580 o ASA serie 5585-X

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Il clustering consente di combinare più appliance ASA fisiche in un'unica unità logica, aumentando la velocità di trasmissione e la ridondanza. Per ulteriori informazioni sul clustering, consultare la Cisco ASA Series CLI Configuration Guide, 9.0.

In questo scenario, il clustering è stato configurato e abilitato sull'appliance ASA master; sull'appliance ASA slave, il clustering è stato configurato ma non abilitato.

Problema

Quando si abilita il clustering sull'appliance ASA slave, questa viene disabilitata immediatamente con un messaggio di errore RPC (Remote Procedure Call). Questo è un esempio del messaggio di errore:

```
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 possibile causa è una mancata corrispondenza della suite di cifratura SSL tra l'appliance ASA master e quella slave. Il clustering richiede che tra il master e l'unità slave da aggiungere al cluster sia presente almeno una suite di cifratura SSL corrispondente. Fare riferimento a questo requisito nella Cisco ASA Series CLI Configuration Guide, 9.0:

I nuovi membri del cluster devono utilizzare la stessa impostazione di crittografia SSL (comando di crittografia SSL) dell'unità master.

Nello scenario di mancata corrispondenza, viene registrato un messaggio syslog:

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

Un esempio di mancata corrispondenza è la seguente crittografia sull'appliance ASA master:

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

E questa crittografia sull'appliance ASA slave da aggiungere al cluster:

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

Questa mancata corrispondenza si verifica in genere quando non è stata installata una licenza di crittografia avanzata (3DES/AES) sull'appliance ASA slave. Per impostazione predefinita, l'elenco delle suite di cifratura sull'appliance ASA slave è **des-sha1** e non viene aggiornato quando si aggiunge la licenza 3DES/AES all'appliance ASA slave.

Esistono due soluzioni per questa mancata corrispondenza.

Soluzione 1

Sull'appliance ASA master, aggiungere **des-sha1** come suite di cifratura SSL valida:

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

> **Nota:** Cisco sconsiglia di abilitare **des-sha1** perché è una cifratura debole ed è considerata vulnerabile.

Soluzione 2

Sull'appliance ASA slave, aggiungere almeno una delle seguenti suite di cifratura SSL: **rc4-sha1**, **aes128-sha1**, **aes256-sha1** o **3des-sha1**:

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

Informazioni correlate

- Cisco ASA Series CLI Configuration Guide, 9.0
- Documentazione e supporto tecnico – Cisco Systems