Clustering Disabled on Slave ASA (RPC_SYSTEMERROR)

Contents

Introduction

This document describes how to resolve an error message that might appear when you attempt to add a new slave Adaptive Security Appliance (ASA) unit to an existing cluster of ASAs.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of clustering
- Basic knowledge of how to configure clustering on the ASA
- Basic knowledge of the Secure Socket Layer (SSL) handshake

Components Used

The information in this document is based on these software and hardware versions:

- ASA software version 9.0 or later
- ASA 5580 or ASA5585-X series appliances

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

Refer to Cisco Technical Tips Conventions for information on document conventions.

Background Information

Clustering lets you combine multiple physical ASAs into one logical unit, which provides increased throughput and redundancy. For more information on clustering, refer to the Cisco ASA Series CLI Configuration Guide, 9.0.

In this scenario, clustering has been configured and enabled on the master ASA; on the slave ASA, clustering has been configured but not enabled.

Problem

When you enable clustering on the slave ASA, it is disabled immediately with a remote procedure call (RPC) error message. This is an example of the error message:

```
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.
```

One possible reason for this error is an SSL cipher suite mismatch between the master and the slave ASAs. Clustering requires that there be at least one matching SSL cipher suite between the master and the slave unit to be added to the cluster. Refer to this requirement in the Cisco ASA Series CLI Configuration Guide, 9.0:

New cluster members must use the same SSL encryption setting (the SSL encryption command) as the master unit.

In the mismatch scenario, a syslog message is logged :

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

An example of a mismatch is this encryption on the master ASA:

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

And this encryption on the slave ASA to be added to the cluster:

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

This mismatch commonly occurs when a strong encryption (3DES/AES) license has not been installed on the slave ASA. The list of cipher suites on the slave ASA defaults to **des-sha1** and is not updated when the 3DES/AES license is added to the slave ASA.

There are two solutions for this mismatch.

Solution 1

On the master ASA, add **des-sha1** as a valid SSL cipher suite:

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

> **Note**: Cisco does not recommend that you enable **des-sha1** because it is a weak cipher and is considered vulnerable.

Solution 2

On the slave ASA, add at least one of these SSL cipher suites: **rc4-sha1**, **aes128-sha1**, **aes256-sha1**, or **3des-sha1**:

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

Related Information

- **Cisco ASA Series CLI Configuration Guide, 9.0**
- **Technical Support & Documentation - Cisco Systems**