Clustering auf Slave ASA deaktiviert (RPC_SYSTEMERROR)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Fehlermeldung aufgelöst werden kann, die angezeigt wird, wenn Sie versuchen, einem vorhandenen ASA-Cluster eine neue Slave Adaptive Security Appliance (ASA) hinzuzufügen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse im Clustering
- Grundkenntnisse zur Konfiguration von Clustering auf der ASA
- Grundkenntnisse des SSL-Handshake (Secure Socket Layer)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA Software Version 9.0 oder höher
- Appliances der Serie ASA 5580 oder ASA5585-X

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Durch Clustering können mehrere physische ASAs zu einer logischen Einheit zusammengefasst werden, was einen höheren Durchsatz und eine höhere Redundanz ermöglicht. Weitere Informationen zu Clustering finden Sie im Konfigurationshandbuch für die Cisco ASA-Serie, Version 9.0.

In diesem Szenario wurde das Clustering auf der Master-ASA konfiguriert und aktiviert. auf der Slave-ASA wurde Clustering konfiguriert, aber nicht aktiviert.

Problem

Wenn Sie Clustering auf der Slave-ASA aktivieren, wird es sofort mit einer RPC-Fehlermeldung (Remote Procedure Call) deaktiviert. Dies ist ein Beispiel für die Fehlermeldung:

```
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.
```

Ein möglicher Grund für diesen Fehler ist eine Diskrepanz zwischen Master und Slave-ASAs in der SSL-Verschlüsselungssuite. Beim Clustering muss mindestens eine passende SSL-Verschlüsselungssuite zwischen Master und Slave-Einheit zum Cluster hinzugefügt werden. Weitere Informationen zu dieser Anforderung finden Sie im Konfigurationshandbuch zur CLI der Cisco ASA-Serie, Version 9.0:

Neue Cluster-Mitglieder müssen dieselbe SSL-Verschlüsselungseinstellung (den SSL-Verschlüsselungsbefehl) wie die Master-Einheit verwenden.

Im Diskontszenario wird eine Syslog-Meldung protokolliert:

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

Ein Beispiel für eine Diskrepanz ist diese Verschlüsselung auf der 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
```

Diese Verschlüsselung auf der Slave-ASA wird dem Cluster hinzugefügt:

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

Diese Diskrepanz tritt häufig auf, wenn auf der ASA-Slave keine Lizenz für starke Verschlüsselung (3DES/AES) installiert wurde. Die Liste der cipher-Suites auf der Slave-ASA lautet standardmäßig **des-sha1** und wird nicht aktualisiert, wenn der Slave-ASA die 3DES/AES-Lizenz hinzugefügt wird.

Für diese Diskrepanz gibt es zwei Lösungen.

Lösung 1

Fügen Sie auf der Master-ASA **des-sha1** als gültige SSL-Verschlüsselungs-Suite hinzu:

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

> **Hinweis**: Cisco empfiehlt nicht, **des-sha1** zu aktivieren, da es sich um eine schwache Chiffre handelt und als verwundbar gilt.

Lösung 2

Fügen Sie auf der Slave-ASA mindestens eine der folgenden SSL-Verschlüsselungssuiten hinzu: **rc4-sha1**, **aes128-sha1**, **aes256-sha1** oder **3des-sha1**:

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

Zugehörige Informationen

- Konfigurationsleitfaden für die CLI der Cisco ASA-Serie 9.0
- Technischer Support und Dokumentation - Cisco Systems