Probleme mit der Netzwerkverbindung der Content Security Appliance

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein Problem beheben können, das auftritt, wenn Sie keine Verbindung zur Cisco Email Security Appliance (ESA) oder zur Cisco Security Management Appliance (SMA) über das Netzwerk herstellen können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- Cisco SMA
- AsyncOS

Verwendete Komponenten

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

- Cisco ESA AsyncOS - alle Versionen
- Cisco SMA AsyncOS - alle Versionen

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.

Problem

Sie können keine Verbindung zu Ihrer ESA oder SMA über das Netzwerk herstellen. Sie versuchen, eine Verbindung über die Webschnittstelle und die CLI über Secure Shell (SSH) herzustellen, aber die Appliance scheint die Anfragen nicht zu beantworten.

> **Vorsicht**: Es ist sehr wichtig, dass Sie das System **nicht aus- und wieder einschalten**, es sei denn, Sie werden vom technischen Support von Cisco dazu aufgefordert. Wenn Sie die Appliance aus- und wieder einschalten, kann dies zu Datenbeschädigungen führen, die zu Nachrichtenverlusten, Datenbankbeschädigungen, Verlust von Protokolldaten oder Beschädigungen des Dateisystems führen können. Wenn Sie die Appliance aus- und wieder einschalten, können die Dateisysteme nicht einwandfrei deinstalliert werden. Aus diesem Grund empfiehlt Cisco, den Befehl **shutdown** oder **reboot** über die CLI oder die Option **Shutdown/Reboot** zu verwenden, die auf der Registerkarte Systemverwaltung der Appliance-GUI aufgeführt ist.

Lösung

In den meisten Fällen ist die Appliance nicht wirklich gesperrt. Es kann einfach so sein, dass es nicht möglich ist, Netzwerkanfragen wie gewohnt zu beantworten. Dieser Abschnitt enthält Richtlinien, die Sie verwenden können, um das Problem zu diagnostizieren und Ihr System möglicherweise wiederherzustellen, sodass es ausgeführt wird oder sich in einem funktionierenden Zustand befindet.

Wenn Sie die Einheit neu starten und immer noch keinen Zugriff über das Netzwerk erhalten, überprüfen Sie die Anzeigen und akustischen Codes der Einheit:

- Überprüfen Sie die Anzeigeleuchten an der Einheit. Ist irgendein Licht an?
- Sind die LEDs für die Festplatten an? Blinken sie?
- Gibt es Statuscodes auf der Vorderseite der Appliance?
- Hat die Appliance beim Start akustische Codes ausgegeben (Signaltöne)?

In vielen Fällen können Sie einfach das Netzwerkkabel austauschen oder an einen anderen Port des Switches ziehen, um das Verbindungsproblem zu beheben:

- Überprüfen Sie den Status der Anzeigeleuchten am Switch-Port, sofern diese verfügbar sind.
- Überprüfen Sie den Status der Leuchten an der Einheit. Sind sie da? Blinken sie?
- Können Sie eine direkte Verbindung zur Einheit über ein Netzwerk-Crossover-Kabel herstellen?

Ein Netzwerk-Crossover-Kabel ermöglicht Ihnen, eine direkte Verbindung zu den Ethernet-Ports

der Appliance herzustellen. Sie müssen jedoch den verbindenden Host so konfigurieren, dass er sich im gleichen Subnetz befindet wie die Schnittstelle, mit der Sie eine Verbindung herstellen. Die Verwendung eines Netzwerk-Crossover-Kabels kann bei der Diagnose von Situationen hilfreich sein, die mit Ihrem LAN zusammenhängen, z. B. wenn ein anderer Host dieselbe IP-Adresse im gleichen Subnetz hat. Überprüfen Sie, ob Ihre Appliance auf Netzwerkanforderungen reagiert:

- Antwortet Ihre Appliance nicht auf Netzwerkanfragen oder reagiert sie einfach nicht auf Serviceanfragen? Sie können einen Ping verwenden, um Folgendes zu bestimmen: Wenn Sie ein Ping an die Appliance senden können, aber kein SSH-Signal senden können, dann wissen Sie, dass sie über das Internet Control Message Protocol (ICMP) überwacht wird und der SSH-Dienst nicht reagiert oder nicht zugänglich ist.

- Haben Sie alle Netzwerkschnittstellen getestet? Überprüfen Sie, ob Sie mit dem zuvor beschriebenen Prozess eine Verbindung zu einer der anderen Schnittstellen auf der Appliance herstellen können.

Wenn Ihr System nicht auf Netzwerkanfragen reagiert und sofortiger Zugriff erforderlich ist, können Sie eine Verbindung mit dem seriellen Port auf der Geräterückseite herstellen. Dieser Port ist ein Standard-DB9-Anschluss und kann zusammen mit dem seriellen Kabel Ihres Geräts verwendet werden. Wenn Sie nicht über das serielle Kabel verfügen, das mit Ihrer Einheit geliefert wurde, müssen Sie ein Kabel erwerben, das als Nullmodemkabel konfiguriert ist.

Optional können Sie ein serielles Standardkabel mit einem Nullmodemadapter verwenden. Wenn Sie das Kabel an die Einheit anschließen, können Sie das andere Ende des Kabels an ein anderes System anschließen, z. B. einen Laptop. Sie müssen ein Terminalprogramm wie Hyperterm oder Procom verwenden. Sie müssen auch Ihr Terminalprogramm für 9600 Baud 8N1 konfigurieren. Sobald Sie Ihr Terminalprogramm starten, sollten Sie in der Lage sein, eine Verbindung herzustellen und sich anzumelden. Wenn der serielle Port nicht reagiert, sollten Sie überprüfen, ob das Kabel angeschlossen ist und das Gerät eingeschaltet ist. Wenn Sie sich immer noch nicht anmelden können, empfiehlt Cisco, sich für weitere Unterstützung an den Kundensupport zu wenden.

Netzwerkbezogene Befehle

Wenn Sie Zugriff über den seriellen Port erhalten können, geben Sie den Befehl **status detail** ein, um zu überprüfen, ob der Einheitenstatus **Online** (**Online)** anzeigt:

```
mail.example.com > status detail

Status as of:                  Mon Jan 04 12:48:31 2010 CST
Up since:                      Tue Jul 14 16:50:50 2009 CDT (173d 20h 57m 41s)
Last counter reset:            Never
System status:                 Online
Oldest Message:                24 weeks 16 hours 30 mins 48 secs
Feature - Centralized Tracking: 833 days
Feature - Centralized Reporting: 833 days
Feature - IronPort Centralized Configuration Manager: 60 days
Feature - Incoming Mail Handling: Perpetual
Feature - Centralized Spam Quarantine: 833 days
```

Hinweis: Wenn der Befehl **status detail** nicht antwortet oder einen Fehler ausgibt, wenden Sie sich an den Cisco Kundensupport.

Geben Sie den Befehl **Version** ein, um den RAID-Status zu überprüfen:

```
mail.example.com > version

Current Version
===============
Model: M660
Version: 6.5.2-101
Build Date: 2009-05-28
Install Date: 2009-07-14 17:04:32
Serial #: 002C999999-J999999
BIOS: 2.4.3I
RAID: 1.21.02-0528, 2.01.00, 1.02-014B
RAID Status: Optimal
RAID Type: 10
BMC: 1.77
```

Wenn das RAID beschädigt ist, ist es möglich, dass die Appliance einen anderen Fehler gefunden hat, der möglicherweise nicht mit dem scheinbaren Systemabsturz zusammenhängt.

> **Hinweis**: Wenn der Befehl **Version** keine Antwort gibt oder keine Daten bereitstellt, wenden Sie sich an den Cisco Kundensupport.

Geben Sie den Befehl **etherconfig** ein, um Ihre Netzwerkkonfiguration zu überprüfen:

```
mail.example.com > etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
[]> media

Ethernet interfaces:
1. Data 1 (Autoselect: <link is down>)) 00:22:19:b0:03:c4
2. Data 2 (Autoselect: <link is down>)) 00:22:19:b0:03:c6
3. Management (Autoselect: <1000baseTX full-duplex>) 00:10:18:4e:29:88

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
[]> MTU

Ethernet interfaces:
1. Data 1 default mtu 1500
2. Data 2 default mtu 1500
3. Management default mtu 1500

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
```

Aktuelle Netzwerkänderungen können sich auf die Konnektivität zur Appliance auswirken. Geben

Sie den Befehl **interface config** ein, um die Schnittstelleneinstellungen zu überprüfen:

```
mail.example.com > interfaceconfig


Currently configured interfaces:
1. Management (192.168.1.33/24 on Management: downside.hometown.net)
2. outbound_gloop_ISQ_notify (192.168.1.34/24 on Management: inside.hometown.net)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

[]>
```

Geben Sie den **diagnostischen** Befehl ein, um den gesamten netzwerkbezogenen Cache zu leeren:

```
mail.example.com > diagnostic


Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
[]> network


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> flush

Flushing LDAP cache.
Flushing DNS cache.
Flushing system ARP cache.
10.92.152.1 (10.92.152.1) deleted
10.92.152.18 (10.92.152.18) deleted

Network reset complete.

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]>
```

Hinweis: Wenn einer der netzwerkbezogenen Befehle nicht antwortet, wenden Sie sich an den Cisco Kundensupport. Wenn Sie die in diesem Dokument beschriebenen Schritte zur Fehlerbehebung durchführen und weiterhin keinen Zugriff über das Netzwerk erhalten, wenden Sie sich an den Cisco Kundensupport, um weitere Unterstützung zu erhalten.