Problemi di connettività di rete di Content Security Appliance

Sommario

Introduzione

In questo documento viene descritto come risolvere un problema che si verifica quando non è possibile connettersi a Cisco Email Security Appliance (ESA) o Cisco Security Management Appliance (SMA) tramite la rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ESA
- Cisco SMA
- AsyncOS

Componenti usati

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

- Cisco ESA AsyncOS tutte le versioni
- Cisco SMA AsyncOS tutte le versioni

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.

Problema

Non è possibile connettersi all'ESA o all'SMA tramite la rete. Si tenta di connettersi tramite l'interfaccia Web e la CLI tramite Secure Shell (SSH), ma l'accessorio non sembra rispondere alle richieste.

> **Attenzione:** È molto importante **non spegnere e riaccendere** il sistema, a meno che non sia stato consigliato dal supporto tecnico Cisco. L'accensione e lo spegnimento dell'accessorio possono causare il danneggiamento dei dati, con conseguente perdita di messaggi, danneggiamento del database, perdita di dati di registrazione o danneggiamento del file system. Quando l'accessorio viene riacceso, non è possibile smontare correttamente i file system. Per questo motivo, Cisco consiglia di usare il comando **shutdown** o **reboot** dalla CLI o l'opzione **Shutdown/Reboot** elencata nella scheda system administration della GUI dell'accessorio.

Soluzione

Nella maggior parte dei casi l'accessorio non è bloccato. Potrebbe semplicemente trovarsi in uno stato che non consente di rispondere alle richieste di rete nel modo consueto. In questa sezione vengono fornite le linee guida che è possibile utilizzare per diagnosticare il problema ed eventualmente ripristinare il sistema in modo che venga eseguito o sia in uno stato funzionante.

Se si riavvia l'accessorio correttamente ma non si riesce comunque ad accedere tramite la rete, verificare le spie e i codici acustici sull'accessorio:

- Controllare le spie dell'accessorio. Ci sono luci accese?
- Le luci dei dischi rigidi sono accese? Stanno lampeggiando?
- Sono presenti codici di stato sulla parte anteriore dell'accessorio?
- L'accessorio ha emesso codici acustici all'avvio (segnali acustici)?

In molti casi, è possibile sostituire semplicemente il cavo di rete o passare a un'altra porta dello switch per risolvere il problema di connettività:

- Controllare lo stato delle spie sulla porta dello switch, se disponibili.
- Controllare lo stato delle luci sull'accessorio. Ci sono? Stanno lampeggiando?
- Èpossibile collegarsi direttamente all'accessorio tramite un cavo crossover di rete?

Un cavo crossover di rete consente il collegamento diretto alle porte Ethernet dell'accessorio. È tuttavia necessario configurare l'host di connessione in modo che si trovi nella stessa subnet dell'interfaccia a cui ci si connette. L'utilizzo di un cavo crossover di rete può essere utile per la diagnosi di situazioni correlate alla LAN, ad esempio quando un altro host ha lo stesso indirizzo IP

nella stessa subnet. Verificare che l'accessorio risponda alle richieste di rete:

- L'appliance non risponde alle richieste di rete o semplicemente non risponde alle richieste di assistenza? Per verificare questa condizione, è possibile utilizzare il comando ping: se è possibile eseguire il ping dell'accessorio ma non del dispositivo SSH, si sa che è in ascolto tramite il protocollo ICMP (Internet Control Message Protocol) e il servizio SSH non risponde o non è accessibile.

- Sono state testate tutte le interfacce di rete? Verificare se è possibile collegarsi a una delle altre interfacce dell'accessorio utilizzando la procedura descritta in precedenza.

Se il sistema non risponde alle richieste di rete ed è necessario l'accesso immediato, è possibile collegarsi alla porta seriale situata sul retro dell'accessorio. Questa porta è un connettore DB9 standard e può essere utilizzata con il cavo seriale fornito con l'accessorio. Se il cavo seriale fornito con l'accessorio non è disponibile, è necessario acquistarne uno configurato come cavo null modem.

Se lo si desidera, è possibile utilizzare un cavo seriale standard con un adattatore per modem null. Una volta collegato il cavo all'accessorio, è possibile collegare l'altra estremità del cavo a un altro sistema, ad esempio un portatile. È necessario utilizzare un programma di terminale quale Hyperterm o Procom. È inoltre necessario configurare il programma terminale per 9600 Baud 8N1. Una volta avviato il programma terminale, sarà possibile connettersi e accedere. Se la porta seriale non risponde, verificare che il cavo sia collegato e che l'unità sia accesa. Se non è ancora possibile accedere, Cisco consiglia di contattare l'assistenza clienti per ulteriore assistenza.

Comandi relativi alla rete

Se è possibile accedere tramite la porta seriale, immettere il comando **status detail** per verificare che lo stato dell'accessorio sia **Online**:

```
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
```

Nota: Se il comando **status detail** non risponde o restituisce un errore, contattare il supporto tecnico Cisco.

Immettere il comando **Version** per verificare lo stato RAID:

```
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
```

Se il RAID è danneggiato, è possibile che l'accessorio abbia riscontrato un altro errore che potrebbe non essere correlato all'apparente blocco.

Nota: Se il comando **Version** non risponde o non fornisce dati, contattare il supporto tecnico Cisco.

Immettere il comando **etherconfig** per verificare la configurazione della rete:

```
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.
[]>
```

Le recenti modifiche alla rete possono avere un impatto sulla connettività all'accessorio. Immettere il comando **interfaceconfig** per verificare le impostazioni dell'interfaccia:

```
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.

[]>
```

Immettere il comando **diagnostic** per scaricare tutta la cache relativa alla rete:

```
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.
[]>
```

Nota: Se uno dei comandi relativi alla rete non risponde, contattare il supporto tecnico Cisco. Se si eseguono le procedure di risoluzione dei problemi descritte in questo documento e non è ancora possibile ottenere l'accesso tramite la rete, contattare il supporto tecnico Cisco per ulteriore assistenza.