Fehlerbehebung bei SEG"API-Server nicht gestartet oder nicht erreichbar"

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für den Fehler "Entweder der API-Server wurde nicht gestartet oder ist nicht erreichbar" in der Secure Email Gateway (SEG)-Benutzeroberfläche der nächsten Generation beschrieben.

Voraussetzungen

Beginnend mit AsyncOS 11.4 und fortführend mit AsyncOS 12.x für Security Management Appliance (SMA), wurde die Web-Benutzeroberfläche (UI) umgestaltet und die interne Datenverarbeitung durchgeführt.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Secure Email Gateway (SEG)
- Security Management Appliance (SMA)
- Zugriff auf die Web-Benutzeroberfläche

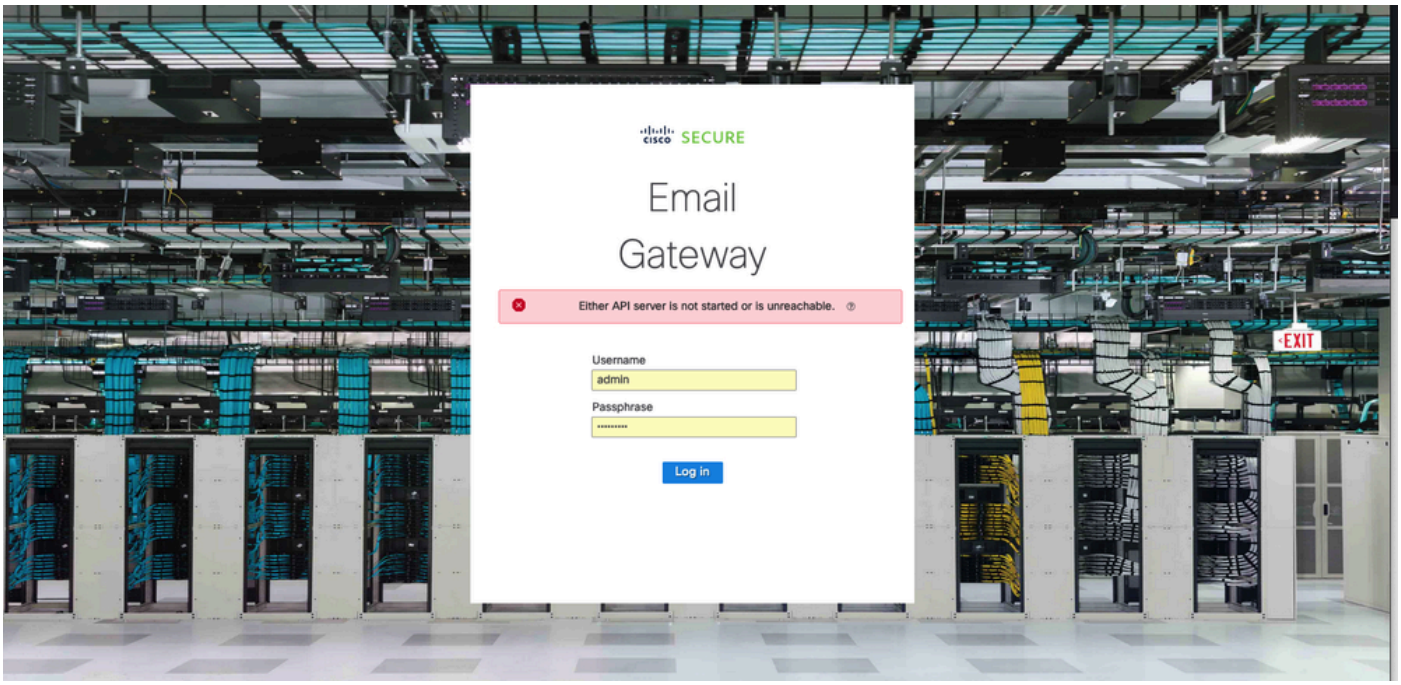
Verwendete Komponenten

- SEG auf Version 11.4 oder höher
- SMA auf Version 12.x oder höheren Versionen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Es konnte nicht auf die Webschnittstelle der nächsten Generation zugegriffen werden. Es wird folgender Fehler angezeigt: "Entweder der API-Server wurde nicht gestartet oder ist nicht erreichbar".



Lösung

Schritt 1: Überprüfen Sie, ob die HTTPS-Funktion der AsyncOS-API in der Verwaltungs-IP-Adresse des sicheren E-Mail-Gateways/der Sicherheitsverwaltungs-Appliance aktiviert ist.

Hinweis: Wenden Sie sich für Cisco Secure Email Cloud Gateway an das TAC, um die IP-Konfiguration zu überprüfen.

<#root>

```
sma.local> interfaceconfig
Currently configured interfaces:
1. Management (10.31.124.134/26 on Management: esa14.mexesa.com)

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

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
```

```
[Management]>

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 192.168.1.2 ):
[10.31.124.134]>

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[0xffffffc0]>

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:
1. Management
[1]>

Hostname:
[sma.local]>

Do you want to configure custom SMTP Helo to use in the SMTP conversation? [N]>

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?
[22]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable Cluster Communication Service on this interface? [N]>

Do you want to enable HTTP on this interface? [Y]>

Which port do you want to use for HTTP?
[80]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?
[443]>

Do you want to enable Spam Quarantine HTTP on this interface? [N]>

Do you want to enable Spam Quarantine HTTPS on this interface? [N]>

Do you want to enable AsyncOS API HTTP on this interface? [N]>

Do you want to enable AsyncOS API HTTPS on this interface? [N]> Y
```

Schritt 2: Konfiguration des Hostnamens bestätigen

Stellen Sie sicher, dass der Appliance-Hostname in keiner anderen Konfiguration oder Appliance verwendet wird, führen Sie den Befehl sethostname aus, um ihn zu überprüfen, oder ändern Sie ggf. die Konfiguration.

<#root>

```
sma.local>
sethostname
[sma.local]>
```

Schritt 3: Überprüfung des Netzwerkzugriffs

Für die Benutzeroberfläche der nächsten Generation ist erforderlich, um Trailblazer und Port 443 zuzulassen.

Führen Sie den Befehl trailblazerconfig status aus.

<#root>

```
sma.local>
trailblazerconfig status

trailblazer is not running
sma.local>
trailblazerconfig enable

trailblazer is enabled.
```

Schritt 4: Zugriff auf die Benutzeroberfläche der nächsten Generation

Zugriff auf die Webschnittstelle der nächsten Generation

Wenn das Problem weiterhin besteht, wenden Sie sich an das Cisco TAC.

Zugehörige Informationen

- Deaktivieren/Aktivieren eines neuen GUI-Banners auf Security Management Appliances
- Verwaltungsdetails des CLI-Befehls "trailblazer" für die Cisco Security Management Appliance (SMA)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.