

Waarom kan Trailblazer niet initialiseren?

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Achtergrond](#)

[Oplossing](#)

[Werken](#)

[Probleemoplossing](#)

Inleiding

Dit document beschrijft een van de meest voorkomende problemen waardoor Trailblazer niet op de Security Management-applicatie (SMA) initialiseert.

Bijgedragen door Jean Orozco, Cristian Rengifo, Cisco TAC Engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Security Management-applicatie (SMA)
- E-mail security applicatie (ESR)
- [Gebruikershandleiding trailblazer geïntroduceerd in AsyncOS versie 12](#)

Gebruikte componenten

Dit document is van toepassing op de SMA met AsyncOS versie 12 of nieuwer.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle in dit apparaat gebruikte apparaten Het document is gestart met een gewist (standaard) configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

Trailblazer formatteert niet na het in werking stellen van het commando trailblazerfig, om:

```
ironport.example.com> trailblazerconfig status
```

```
trailblazer is not running
ironport.example.com> trailblazerconfig enable
```

```
trailblazer is enabled.
```

To access the Next Generation web interface, use the port 4431 for HTTPS.

Wanneer u na het inschakelen van de trailblazer de status controleert, ziet deze er als volgt uit:

```
ironport.example.com> trailblazerconfig status
```

```
trailblazer is not running
```

Dit wordt meestal veroorzaakt doordat de interface die wordt gebruikt om het apparaat te benaderen, niet kan worden opgelost in DNS.

Achtergrond

Een SMA-actieve versie 11.4 of nieuwer 12.x kan problemen ondervinden bij het inschakelen van een trainer. De 'trailblazer status' output zal tonen dat de eigenschap niet draait, alhoewel het eerder werd geactiveerd met het 'trailblazereconferentie' bevel. Trailblazer gebruikt een NGINX-proxy om de API- en GUI-servers te bereiken en het vergemakkelijkt het beheer van de poorten bij het verkrijgen van toegang tot de Security Management-applicatie via de GUI.

Opmerking: Zorg ervoor dat uw DNS-server de hostname die u hebt opgegeven voor het verkrijgen van toegang tot het apparaat, kan oplossen. Deze stap is een vereiste zoals aangegeven op de vereisten die zijn gepubliceerd in het artikel [Administrator-details op trailblazer](#). Deze informatie wordt vermeld in de documentatie [bij de Releaseopmerkingen](#) en de [gebruikersgids](#).

Oplossing

Maak een DNS ingang voor de hostnaam van de interface die wordt gebruikt om toegang te krijgen tot de Security Management-applicatie GUI.

Na het maken van de DNS-unit zal het verwachte resultaat zijn:

- Controleer de verkeningsstatus.

```
sma.local> trailblazerconfig status
```

```
trailblazer is not running
```

- Trailblazer inschakelen.

```
sma.local> trailblazerconfig enable
```

```
trailblazer is enabled.
```

To access the Next Generation web interface, use the port 4431 for HTTPS.

- Controleer de status na het inschakelen van de trailblazer.

```
sma.local> trailblazerconfig status
```

trailblazer is running with https on port 4431.

Werken

- Als de DNS-server lokaal wordt beheerd, maakt u de juiste DNS-ingang voor de interface die wordt gebruikt om de SMA GUI te bereiken en raadpleegt u het gedeelte Problemen oplossen.
- Als SMA root DNS-servers gebruikt en/of er geen optie is om een DNS-ingang op een lokaal beheerde DNS-server te maken, als alternatief kan er een directory worden gecreëerd in **Network > DNS > Instellingen bewerken** door "**Alternatieve DNS-servers overrides**" te specificeren op de FQDN voor het SMA in het "**Domain**"- en "**DNS-FQDN**"-adres en het **IP-adres van het SMA in het gedeelte "DNS Server IP Address" (DNS server-adres)** en dien de **wijzigingen in en beveel deze**. Als dit eenmaal is gedaan, raadpleegt u het gedeelte Problemen oplossen.

Use the Internet's Root DNS Servers

Alternate DNS servers Overrides (Optional):

Domain	DNS Server FQDN	DNS Server IP Address	Add Row
sma.example.com	sma.example.com	192.168.10.10	
<i>i.e., example.com</i>	<i>i.e., dns.example.com</i>	<i>i.e., 10.0.0.3</i>	

Opmerking: Deze tijdelijke oplossing is alleen mogelijk wanneer het apparaat Root DNS-servers gebruikt. Als het apparaat lokale DNS-servers gebruikt, maakt u een geschikte DNS-ingang voor de hostnaam.

Probleemoplossing

- Bekijk de vereisten die op de [administratieve details](#) in [het CLI-opdracht voor Cisco Security Management Appliance \(SMA\)](#) document worden beschreven.
- Bevestig dat de verkenner actief is en schakelt u deze vervolgens uit/weer in om het configuratiebestand van de trailblazer in het achterste gedeelte te herschrijven. Zie hieronder:

Bekijk de trainingsstatus:

```
sma.local> trailblazerconfig status
```

```
trailblazer is running with https on 4431 port.
```

Trailblazer uitschakelen:

```
sma.local> trailblazerconfig disable
```

```
trailblazer is disabled.
```

Bevestig dat het kinderslot goed is uitgeschakeld:

```
sma.local> trailblazerconfig status
```

trailblazer is not running

Trailblazer terug inschakelen:

```
sma.local> trailblazerconfig enable
```

trailblazer is enabled.

To access the Next Generation web interface, use the port 4431 for HTTPS.

Bevestig dat er een verkenner is:

```
sma.local> trailblazerconfig status
```

trailblazer is running with https on 4431 port.

Probeer, nadat al het bovenstaande is voltooid, toegang te krijgen tot de nieuwe GUI om te zien of het werkt.

- Als de hostnaam van de interface die wordt gebruikt om het apparaat te bereiken, al kan worden opgelost in DNS en/of als de bovenstaande suggesties de probleem niet hebben opgelost, opent u een TAC-case om de oplossing verder te ondersteunen.