

¿Por qué Trailblazer no se Inicializa?

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Background](#)

[Solución](#)

[Solución Alternativa](#)

[Resolución de problemas](#)

Introducción

Este documento describe uno de los problemas más comunes que hace que Trailblazer no se inicialice en el dispositivo de administración de seguridad (SMA).

Colaborado por Jean Orozco, Cristian Rengifo, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de administración de seguridad (SMA)
- Dispositivo de seguridad de correo electrónico (ESA)
- [Función Trailblazer introducida en AsyncOS versión 12](#)

Componentes Utilizados

Este documento es aplicable al SMA que ejecuta AsyncOS versión 12 o posterior.

The information in this document was created from the devices in a specific lab environment. Todos los dispositivos utilizados en esta documento iniciado con una configuración borrada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Trailblazer no se puede inicializar después de ejecutar el comando `trailblazerconfig enable`:

```
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.

Al verificar el estado después de habilitar el pionero, se mostrará de la siguiente manera:

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

```
trailblazer is not running
```

Normalmente, esto se debe a que la interfaz utilizada para acceder al dispositivo no se puede resolver en DNS.

Background

SMA que ejecuta la versión 11.4 o la versión más reciente 12.x puede experimentar problemas al habilitar el pionero. La salida "estado del pionero" mostrará que la función no se está ejecutando aunque previamente se habilitó con el comando "trailblazerconfig enable". Trailblazer utiliza un proxy NGINX para llegar a los servidores API y GUI y facilita la administración de los puertos al acceder al dispositivo de administración de seguridad a través de la GUI.

Nota: Asegúrese de que el servidor DNS pueda resolver el nombre de host que especificó para acceder al dispositivo. Este paso es un requisito, tal y como se establece en los requisitos previos publicados en los [detalles administrativos del artículo de la pionera](#). Esta información se menciona en la documentación de [Release Notes](#) y [User Guide](#).

Solución

Cree una entrada DNS para el nombre de host de la interfaz utilizada para acceder a la GUI del dispositivo de administración de seguridad.

Después de crear la entrada DNS, el resultado esperado será:

- Compruebe el estado del pionero.

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

```
trailblazer is not running
```

- Habilite el pionero.

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

```
trailblazer is enabled.
```

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

- Después de activar el pionero, verifique el estado de nuevo.

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

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

Solución Alternativa

- Si el servidor DNS se administra localmente, cree la entrada DNS adecuada para la interfaz utilizada para acceder a la GUI de SMA y consulte la sección de Troubleshooting.
- Si el SMA está utilizando servidores DNS raíz y/o no hay opción para crear una entrada DNS en un servidor DNS administrado localmente, como alternativa, se puede crear una entrada en Red > DNS > Editar configuración especificando en "Alternate DNS servers Overrides" el FQDN para el SMA en la sección "Dominio" y "FQDN del servidor DNS" y la dirección IP del SMA en el servidor "DNS IP Address", luego envíe y confirme los cambios. Una vez hecho esto, consulte la sección de solución de problemas.

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.e., example.com	i.e., dns.example.com	i.e., 10.0.0.3	

Nota: Esta solución alternativa sólo es posible cuando el dispositivo utiliza servidores DNS raíz. Si el dispositivo utiliza servidores DNS locales, cree una entrada DNS apropiada para el nombre de host.

Resolución de problemas

- Revise los requisitos previos descritos en el [documento de detalles administrativos del comando CLI "trailblazer" para el documento de Cisco Security Management Appliance \(SMA\)](#).
- Confirme que el pionero se esté ejecutando y después inhabilite/habilite nuevamente para reescribir el archivo de configuración del remolque en el back-end. Ver a continuación:

Revise el estado del pionero:

```
sma.local> trailblazerconfig status  
  
trailblazer is running with https on 4431 port.
```

Desactivar el pionero:

```
sma.local> trailblazerconfig disable  
  
trailblazer is disabled.
```

Confirme que se ha desactivado correctamente:

```
sma.local> trailblazerconfig status  
  
trailblazer is not running
```

Activar el dispositivo de remolque:

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

trailblazer is enabled.

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

Confirmar que el pionero se está ejecutando:

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

trailblazer is running with https on 4431 port.

Una vez que se haya completado todo lo anterior, intente acceder a través de la nueva GUI para ver si funciona.

- Si el nombre de host de la interfaz utilizada para acceder al dispositivo ya se puede resolver en DNS y/o las sugerencias anteriores no solucionaron el problema, abra un caso del TAC para resolver problemas adicionales.