

Por que o Trailblazer não inicializa?

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Background](#)

[Solução](#)

[Solução](#)

[Troubleshooting](#)

Introduction

Este documento descreve um dos problemas mais comuns que faz com que o Trailblazer não inicialize no Security Management Appliance (SMA).

Contribuído por Jean Orozco, Cristian Rengifo, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Security Management Appliance (SMA)
- ESA (Email Security Appliance)
- [Recurso Trailblazer introduzido no AsyncOS versão 12](#)

Componentes Utilizados

Este documento é aplicável ao SMA que executa o AsyncOS versão 12 ou posterior.

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento iniciado com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

O Trailblazer não inicializa após executar o comando `Towblazerconfig 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.

Ao verificar o status depois que o pionazer estiver ativado, ele mostrará o seguinte:

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

```
trailblazer is not running
```

Geralmente, isso é causado porque a interface usada para acessar o dispositivo não pode ser resolvida no DNS.

Background

O SMA executando a versão 11.4 ou 12.x mais recente pode ter problemas com a habilitação do pioneiro. A saída do 'status do bandeirante' mostrará que o recurso não está em execução, mesmo que ele tenha sido anteriormente habilitado com o comando 'logging config enable'. O Trailblazer usa um proxy NGINX para acessar os servidores API e GUI e facilita o gerenciamento das portas ao acessar o Security Management Appliance via GUI.

Note: Certifique-se de que o servidor DNS possa resolver o nome de host que você especificou para acessar o dispositivo, esta etapa é um requisito conforme declarado nos pré-requisitos publicados no artigo [Detalhes administrativos sobre o pionblazer](#). Essas informações são mencionadas nas [Notas de versão](#) e na documentação [do Guia do usuário](#).

Solução

Crie uma entrada DNS para o nome de host da interface usada para acessar a GUI do Security Management Appliance.

Após criar a entrada DNS, o resultado esperado será:

- Verifique o status do pioneiro.

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

```
trailblazer is not running
```

- Habilite o pioneiro.

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

```
trailblazer is enabled.
```

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

- Depois de habilitar o pioneiro, verifique o status novamente.

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


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

Solução

- Se o servidor DNS for gerenciado localmente, crie a entrada de DNS apropriada para a interface usada para acessar a GUI do SMA e consulte a seção de solução de problemas.
- Se o SMA estiver usando servidores DNS raiz e/ou não houver opção de criar uma entrada DNS em um servidor DNS gerenciado localmente, como alternativa, uma entrada pode ser criada em Rede > DNS > Editar configurações especificando na seção "Substituições de servidores DNS alternativos" o FQDN para o SMA no "Domínio" e "DNS Server FQDN" e o IP Endereço do SMA na seção "Endereço IP do Servidor DNS" e, em seguida, Submeter e Confirmar as alterações. Depois que isso tiver sido feito, consulte a seção de solução 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>i.e., example.com</i>	<i>i.e., dns.example.com</i>	<i>i.e., 10.0.0.3</i>	

Note: Essa solução alternativa só é possível quando o dispositivo usa servidores DNS raiz. Se o dispositivo usar servidores DNS locais, crie uma entrada DNS apropriada para o nome do host.

Troubleshooting

- Reveja os pré-requisitos descritos nos [detalhes administrativos do documento CLI do 'pionblazer' para o Cisco Security Management Appliance \(SMA\)](#).
- Confirme se o pionazer está em execução e, em seguida, desative-o/ative-o novamente para reescrever o arquivo de configuração do iniciador no back-end. Veja abaixo:

Reveja o status do pioneiro:

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

Desativar pioneiro:

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

Confirme se ele foi desabilitado corretamente:

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

Ativar o pioneiro novamente:

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

```
trailblazer is enabled.
```

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

Confirme se o pioneiro está em execução:

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

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

Depois que tudo acima tiver sido concluído, tente acessar a nova GUI para ver se ela funciona.

- Se o nome de host da interface usada para acessar o dispositivo já for resolvido no DNS e/ou as sugestões acima não corrigirem o problema, abra um caso do TAC para fazer troubleshooting adicional.