Why Does Trailblazer Fail to Initialize?

Contents

Introduction

This document describes one of the most common problems that causes Trailblazer to fail to initialize on the Security Management Appliance (SMA).

Contributed by Jean Orozco, Cristian Rengifo, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Security Management Appliance (SMA)
- Email Security Appliance (ESA)
- Trailblazer feature introduced in AsyncOS version 12

Components Used

This document is applicable to the SMA running AsyncOS version 12 or newer.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

Trailblazer fails to initialize after running the command `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.
```

When verifying the status after trailblazer is enabled, it will show as follows:

```
ironport.example.com> trailblazerconfig status

trailblazer is not running
```

Commonly, this is caused due to the interface used to access the appliance is not resolvable in DNS.

Background

SMA running version 11.4 or newer 12.x may experience issues with enabling trailblazer. The 'trailblazer status' output will show the feature is not running even though it was previously enabled with the 'trailblazerconfig enable' command. Trailblazer uses an NGINX proxy to reach the API and GUI servers and it eases the management of the ports while accessing the Security Management Appliance via the GUI.

> **Note**: Ensure that your DNS server can resolve the hostname that you specified for accessing the appliance, this step is a requirement as stated on the prerequisites published on the Administrative details on trailblazer article. This information is mentioned on the Release Notes and User Guide documentation.

Solution

Create a DNS entry for the hostname of the interface used to access the Security Management Appliance GUI.

After creating the DNS entry, the expected result will be:

- Check trailblazer status.

```
sma.local> trailblazerconfig status

trailblazer is not running
```

- Enable trailblazer.

```
sma.local> trailblazerconfig enable

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

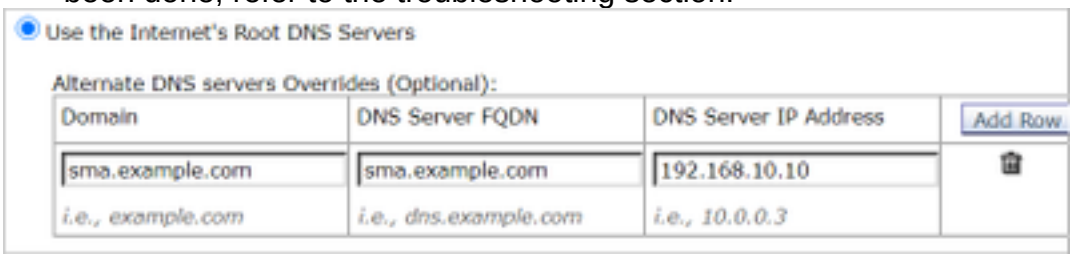
- After enabling trailblazer, check the status again.

```
sma.local> trailblazerconfig status

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

Workaround

- If the DNS server is managed locally, create the proper DNS entry for the interface used to access the SMA GUI and refer to the troubleshooting section.
- If the SMA is using root DNS servers and/or there is no option to create a DNS entry on a locally managed DNS server, as an alternative, an entry can be created in **Network** > **DNS** > **Edit Settings** by specifying in the **"Alternate DNS servers Overrides"** the FQDN for the SMA in the **"Domain"** and **"DNS Server FQDN"** section and the IP address of the SMA in the **"DNS Server IP Address"** section, then Submit and Commit the changes. Once this has been done, refer to the troubleshooting section.



> **Note**: This workaround is only possible when the appliance uses Root DNS Servers. If the appliance uses local DNS servers, please create an appropriate DNS entry for the hostname.

Troubleshooting

- Review the prerequisites described on the Administrative details on 'trailblazer' CLI command for Cisco Security Management Appliance (SMA) document.
- Confirm that trailblazer is running, then disable/enable it back in order to rewrite the trailblazer configuration file in the back-end. See below:

Review the trailblazer status:

```
sma.local> trailblazerconfig status

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

Disable trailblazer:

```
sma.local> trailblazerconfig disable

trailblazer is disabled.
```

Confirm it has been disabled properly:

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Enable trailblazer back:

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

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

Confirm trailblazer is running:

```
sma.local> trailblazerconfig status

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

After all of the above has been completed, try accessing through the new GUI to see if it works.

- If the hostname of the interface used to access the appliance is already resolvable in DNS and/or the suggestions above did not fix the issue, open a TAC case to troubleshoot further.