# Pourquoi Trailblazer ne parvient-il pas à s'initialiser ?

## Contenu



## Introduction

Ce document décrit l'un des problèmes les plus courants qui empêche Trailblazer de s'initialiser sur l'appliance de gestion de la sécurité (SMA).

Contribution de Jean Orozco, Cristian Rengifo, Ingénieurs du TAC Cisco.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de gestion de la sécurité (SMA)
- Dispositif de sécurité de la messagerie (ESA)
- Fonction Trailblazer introduite dans AsyncOS version 12

### Components Used

Ce document s'applique au SMA exécutant AsyncOS version 12 ou ultérieure.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans cette document démarré avec une configuration effacée (par défaut).Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Problème

Trailblazer ne parvient pas à s'initialiser après avoir exécuté la commande semi-blazerconfig

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.
```

Lors de la vérification de l'état après l'activation du semi-azer, il s'affiche comme suit :

```
ironport.example.com> trailblazerconfig status

trailblazer is not running
```

Généralement, cela est dû au fait que l'interface utilisée pour accéder à l'appliance n'est pas résolvable dans DNS.

### Fond

SMA version 11.4 ou ultérieure 12.x peut rencontrer des problèmes lors de l'activation du semi-azer. Le résultat de l'état du semi-azer indique que la fonctionnalité n'est pas en cours d'exécution, même si elle a été précédemment activée avec la commande 'trailblazerconfig enable'. Trailblazer utilise un proxy NGINX pour atteindre les serveurs API et GUI et facilite la gestion des ports tout en accédant à l'appliance de gestion de la sécurité via l'interface utilisateur graphique.

> Remarque: Assurez-vous que votre serveur DNS peut résoudre le nom d'hôte que vous avez spécifié pour l'accès à l'appliance. Cette étape est une condition requise, comme indiqué sur les conditions préalables publiées dans les détails administratifs de l'article sur le précurseur. Ces informations sont mentionnées dans la documentation Release Notes et User Guide.

## Solution

Créez une entrée DNS pour le nom d'hôte de l'interface utilisée pour accéder à l'interface utilisateur graphique de l'appliance de gestion de la sécurité.

Après avoir créé l'entrée DNS, le résultat attendu sera :

- Vérifiez l'état du semi-conducteur.

```
sma.local> trailblazerconfig status

trailblazer is not running
```

- Activez le précurseur.

```
sma.local> trailblazerconfig enable

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

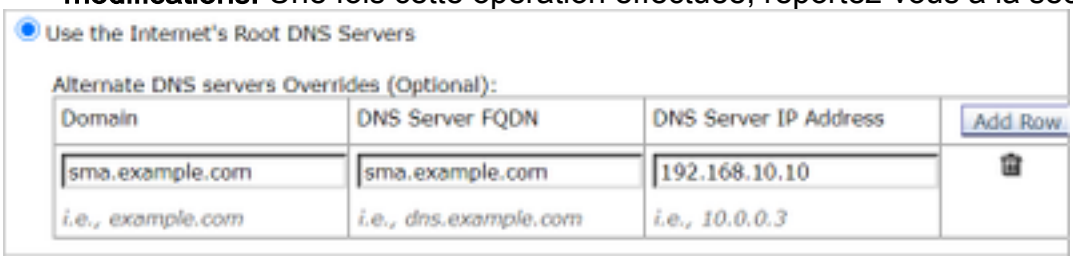
- Après avoir activé le semi-conducteur, vérifiez à nouveau l'état.

```
sma.local> trailblazerconfig status

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

## Solution de contournement

- Si le serveur DNS est géré localement, créez l'entrée DNS appropriée pour l'interface utilisée pour accéder à l'interface utilisateur graphique SMA et reportez-vous à la section de dépannage.
- Si la SMA utilise des serveurs DNS racine et/ou qu'il n'y a aucune option pour créer une entrée DNS sur un serveur DNS géré localement, comme alternative, une entrée peut être créée dans **Network > DNS > Edit Settings** en spécifiant dans la **« Remplace les serveurs DNS alternatifs »** le FQDN pour la SMA dans la section **« Domain » et « DNS Server FQDN » et l'adresse IP dans la section « Adresse IP du serveur DNS », puis envoyez et validez les modifications.** Une fois cette opération effectuée, reportez-vous à la section dépannage.




> Remarque: Cette solution de contournement n'est possible que lorsque l'appliance utilise des serveurs DNS racine. Si l'appliance utilise des serveurs DNS locaux, créez une entrée DNS appropriée pour le nom d'hôte.

## Dépannage

- Examinez les conditions préalables décrites dans le document Administrative Details on 'trailblazer' CLI command for Cisco Security Management Appliance (SMA).
- Vérifiez que le semi-conducteur est en cours d'exécution, puis désactivez/activez-le à nouveau afin de réécrire le fichier de configuration du semi-conducteur dans le serveur principal. Voir ci-dessous :

Vérifiez l'état du semi-conducteur :

```
sma.local> trailblazerconfig status

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

Désactiver le précurseur :

```
sma.local> trailblazerconfig disable

trailblazer is disabled.
```

Confirmez qu'il a été désactivé correctement :

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Activez le routage du semi-conducteur :

```
sma.local> trailblazerconfig enable

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

Confirmer que le semi-azer est en cours d'exécution :

```
sma.local> trailblazerconfig status

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

Une fois que tous les éléments ci-dessus sont terminés, essayez d'accéder à l'interface utilisateur graphique pour voir s'il fonctionne.

- Si le nom d'hôte de l'interface utilisée pour accéder à l'appliance est déjà résolvable dans DNS et/ou si les suggestions ci-dessus n'ont pas résolu le problème, ouvrez un dossier TAC pour le dépanner ultérieurement.