Pourquoi l'initialisation de Trailblazer échoue-t-elle ?

Table des matières

Introduction

Ce document décrit l'un des problèmes les plus courants qui entraînent l'échec de l'initialisation de Trailblazer sur le dispositif de gestion de la sécurité (SMA).

Contribution de Jean Orozco, Cristian Rengifo, Ingénieurs du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

L'initialisation de Trailblazer échoue après l'exécution de la commande trailblazerconfig enable :

```
<#root>

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 de trailblazer, il s'affiche comme suit :

```
<#root>

ironport.example.com>

trailblazerconfig status


trailblazer is not running
```

Généralement, cela est dû au fait que l'interface utilisée pour accéder à l'appliance ne peut pas être résolue dans DNS.

Fond

SMA exécutant la version 11.4 ou une version plus récente 12.x peut rencontrer des problèmes avec l'activation de trailblazer. Le résultat « trailblazer status » indique que la fonctionnalité n'est pas en cours d'exécution alors qu'elle était 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 accéder à l'appliance. Cette étape est obligatoire, comme indiqué dans les conditions préalables publiées dans l'article Détails d'administration sur le pionnier. Ces informations sont mentionnées dans les notes de version et dans la documentation du Guide de l'utilisateur.

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.

Une fois l'entrée DNS créée, le résultat attendu est le suivant :

- Vérifiez l'état des pionniers.

```
<#root>
```

```
sma.local>
trailblazerconfig status


trailblazer is not running
```

- Activez le pionnier.

```
<#root>
sma.local>
trailblazerconfig enable


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

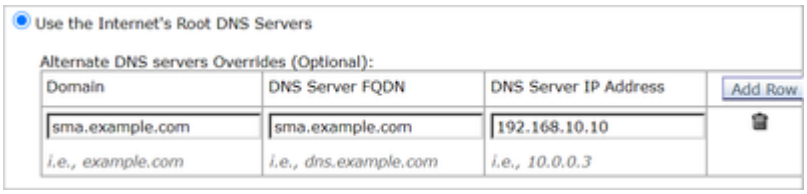
- Après avoir activé trailblazer, vérifiez à nouveau l'état.

```
<#root>
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 le SMA utilise des serveurs DNS racine et/ou s'il n'y a pas d'option pour créer une entrée DNS sur un serveur DNS géré localement, comme alternative, une entrée peut être créée dans Réseau > DNS > Modifier les paramètres en spécifiant dans "Les serveurs DNS alternatifs remplacent" le FQDN pour le SMA dans la section "Domaine" et "DNS Server FQDN" et l'adresse IP du SMA dans la section "Adresse IP du serveur DNS", puis Soumettre et valider les modifications. Une fois cette opération effectuée, reportez-vous à la section consacrée au 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

- Passez en revue les conditions préalables décrites dans le document Détails administratifs sur la commande CLI « trailblazer » pour Cisco Security Management Appliance (SMA).
- Confirmez que trailblazer est en cours d'exécution, puis désactivez/réactivez-le afin de réécrire le fichier de configuration de trailblazer dans le back-end. Voir ci-dessous :

Vérifiez l'état du pionnier :

```
<#root>

sma.local>

trailblazerconfig status


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

Désactiver le pionnier :

```
<#root>

sma.local>

trailblazerconfig disable


trailblazer is disabled.
```

Vérifiez qu'elle a été désactivée correctement :

```
<#root>

sma.local>

trailblazerconfig status
```

```
trailblazer is not running
```

Activer le retour du pionnier :

```
<#root>

sma.local>

trailblazerconfig enable
```

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

Confirmez que le pionnier est en cours :

```
<#root>

sma.local>

trailblazerconfig status
```

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

Une fois que toutes les étapes ci-dessus sont terminées, essayez d'accéder à via la nouvelle interface utilisateur graphique pour voir si cela fonctionne.

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.