Dépannage de l'échec d'appairage haute disponibilité en raison d'une incompatibilité de clé d'authentification dans EPN

Table des matières

Introduction

Ce document décrit comment résoudre l'erreur de non-correspondance de clé d'authentification lors de la configuration de l'appairage haute disponibilité entre les serveurs EPNM principal et secondaire.

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- gestionnaire de réseau programmable évolué (EPNM)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

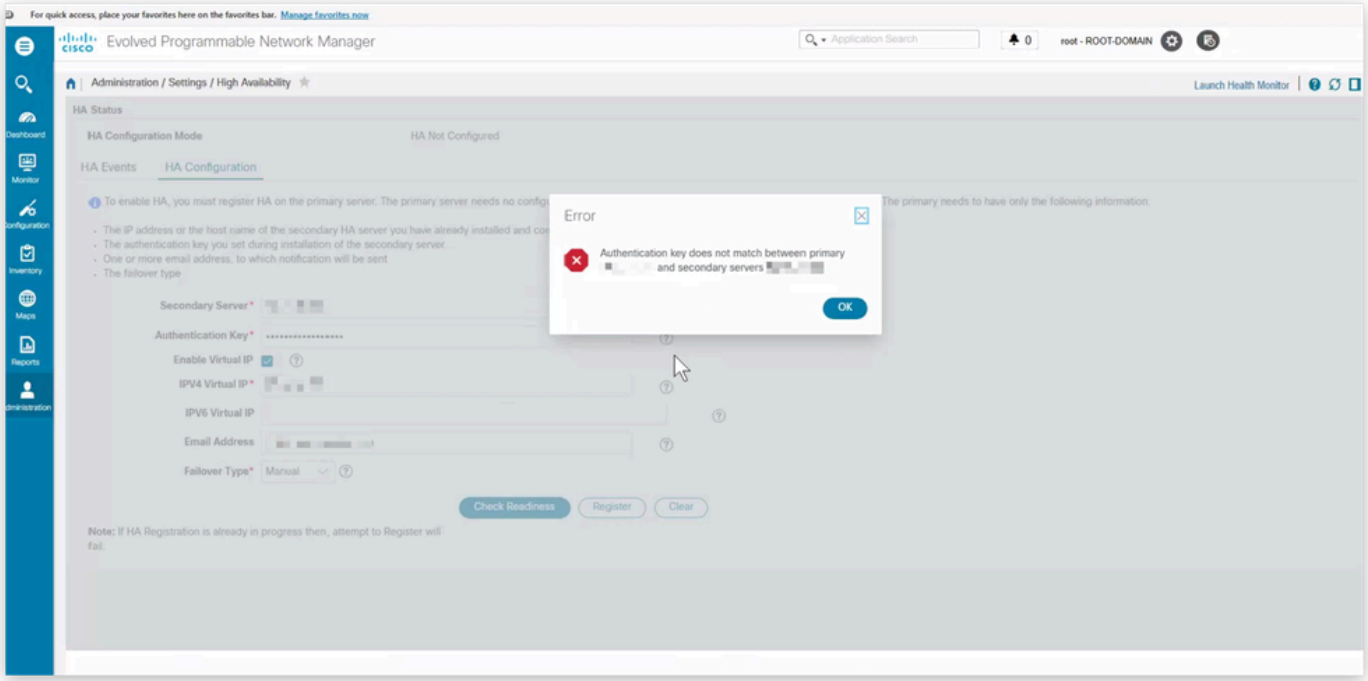
- Logiciel EPNM version 8.x

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.

Énoncé du problème

Les tentatives de configuration de l'appairage haute disponibilité (HA) entre les serveurs Cisco EPNM (Evolved Programmable Network Manager) principal et secondaire échouent. Un message d'erreur indique que la clé haute disponibilité ne correspond pas entre les serveurs principal et secondaire. La réinitialisation de la clé haute disponibilité secondaire et la nouvelle tentative du processus d'appairage ne résolvent pas le problème.

- Message d'erreur : "La clé d'authentification ne correspond pas entre le serveur principal <IP primaire> et le serveur secondaire <IP secondaire>"
- Une défaillance se produit lors de la configuration HA entre les noeuds EPNM principal et secondaire
- Les tentatives de réinitialisation de la clé haute disponibilité sur le serveur secondaire ont échoué



Environnement

- Technologie : Services de gestion de réseau (NMS)
- Produit : Gestionnaire de réseau programmable évolué Cisco
- Version du logiciel: 8.1.0
- Serveurs EPNM principaux et secondaires configurés pour la haute disponibilité
- Action récente : Tentative de réinitialisation de la clé haute disponibilité sur le serveur secondaire et rétablissement de l'appairage haute disponibilité
- Erreur observée : "La clé d'authentification ne correspond pas entre le serveur principal <IP primaire> et le serveur secondaire <IP secondaire>"

Résolution

1. Modifier la clé d'authentification haute disponibilité sur les deux serveurs

Mettez à jour la clé d'authentification HA sur les serveurs EPNM principal et secondaire pour vous assurer qu'ils correspondent.

Exécutez la commande sur chaque serveur (remplacez `<newkey>` par la clé d'authentification souhaitée) :

<#root>

ncs ha authkey

Exemple :

<#root>

epnm/admin#

ncs ha authkey HAAuthKey123

```
Going to update Secondary authentication key
Successfully updated Secondary authentication key in standalone server
epnm/admin#
```

2. Certificats de tofu clairs

Pour éliminer les incohérences potentielles entre les certificats, effacez les certificats Tofu associés au processus de jumelage HA sur les deux serveurs.

Sur le serveur principal :

Répertoriez les certificats Tofu existants :

<#root>

ncs certvalidation tofu-certs listcerts

Si vous voyez une entrée pour l'adresse IP du serveur secondaire, supprimez-la avec :

<#root>

ncs certvalidation tofu-certs deletecert host

_8082

Sur le serveur secondaire :

Répertoriez les certificats Tofu existants :

<#root>

ncs certvalidation tofu-certs listcerts

Si vous voyez une entrée pour l'adresse IP du serveur principal, supprimez-la avec :

<#root>

ncs certvalidation tofu-certs deletecert host

_8082

3. Redémarrez les services NCS sur le serveur principal

Après avoir mis à jour la clé haute disponibilité et effacé les certificats Tofu appropriés, redémarrez les services NCS sur le serveur principal pour appliquer les modifications.

Remarque : cette étape a un impact sur le service ; l'accès à l'application n'est pas disponible pendant le redémarrage du serveur principal.

Arrêtez les services NCS :

<#root>

ncs stop verbose

```
epnm/admin#
epnm/admin# ncs status
Health Monitor Server is running. ( [Role] Primary [State] HA not Configured )
Database server is running
Distributed Cache Service is running.
Messaging Service is running.
FTP Service is disabled
TFTP Service is disabled
NMS Server is running.
LCM Monitor is running.
SAM Daemon is running ...
DA Daemon is running ...
Compliance engine is running
epnm/admin#
epnm/admin#
epnm/admin#
epnm/admin# ncs stop verbose
```

- Attendez que tous les services soient arrêtés et vérifiez leur état à l'aide de la commande suivante :
  <#root>

  ncs status

- Démarrez tous les services à l'aide de la commande :
  <#root>

  ncs start verbose

- Patientez jusqu'à ce que tous les services soient démarrés et vérifiez à nouveau l'état à l'aide de la commande :
  <#root>

  ncs status

4. Réessayer la configuration haute disponibilité via l'interface graphique du serveur principal

Une fois que le serveur principal a redémarré, poursuivez le workflow de configuration de haute disponibilité normal à l'aide de l'interface graphique utilisateur (GUI) du serveur principal.

Motif

La cause sous-jacente de l'échec de l'appairage haute disponibilité est une non-correspondance dans la clé d'authentification haute disponibilité entre les serveurs Cisco EPNM principal et secondaire. L'erreur suivante se produit : "Authentication key does not match between primary <IP> and secondary servers <Secondary IP>". Des incohérences de certificats supplémentaires (certificats Tofu) peuvent également empêcher la réussite de l'établissement de la haute disponibilité.

Informations connexes

- Réinitialiser la clé d'authentification HA
- Procédure de redémarrage du service Cisco EPNM (vidéo)
- Assistance technique de Cisco et téléchargements

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.