Dépannage de la connexion SAML d'administration ISE échoue avec accès refusé en raison d'une configuration de nom de domaine manquante

Table des matières

Problème

La connexion SAML (Security Assertion Markup Language) de l'administrateur Identity Services Engine (ISE) échoue avec une erreur « Accès refusé » après une authentification Azure Entra réussie. Bien qu'Azure Entra affiche une authentification SAML réussie, ISE refuse l'accès au portail de gestion. En outre, la génération de la demande de signature de certificat (CSR) échoue avec l'erreur suivante :

```
cpm.admin.caservice.utils.CAUtil -::admin::addLocalCert:- Error occurred managing certificates :::-CSRF
```

Les journaux ISE affichent les échecs de résolution DNS pour les exceptions FQDN et de connexion SSL du noeud pendant la validation HTTPS interne :

```
SSLHandshakeException: No subject alternative names matching IP address 10.X.X.X found
```

Le système affiche également des avertissements répétés concernant les certificats auto-signés par défaut expirés et RESTConf revenant à HTTP en raison de l'indisponibilité du certificat.

Environnement

- Cisco Identity Services Engine (ISE) version 3.4, correctif 3

- Azure Entra (anciennement Azure AD) configuré comme fournisseur d'identité SAML
- Gestion ISE accessible via l'adresse IP et le nom de domaine complet
- Environnement mis à niveau de la version ISE 3.3 à la version 3.4

Résolution

1. Vérifiez la configuration actuelle du noeud ISE et la résolution DNS en exécutant les commandes suivantes :

```
show running-config | include domain
nslookup xxxxxxxxxx.internal
ping xxxxxxxxxx.internal
```


Remarque : Les résultats attendus indiquent une résolution DNS réussie renvoyant l'adresse IP correcte sans erreurs DNS.

---

2. Ajoutez à nouveau le nom de domaine à la configuration du noeud ISE à l'aide de l'interface de ligne de commande ISE :

```
device# config t
device(config)# ip domain-name xxxxxxxxxx.internal
```

3. Accédez à Administration > System > Certificates > Certificates dans l'interface utilisateur graphique ISE et régénérez le certificat auto-signé par défaut. Assurez-vous que le nouveau certificat inclut à la fois le nom de domaine complet et l'adresse IP dans le champ Autre nom du sujet (SAN).

4. Vérifiez que le certificat régénéré inclut l'adresse IP du noeud dans le champ SAN et qu'il est correctement lié aux services Admin et Portal.

5. Testez la connexion SAML de l'administrateur ISE. L'authentification doit maintenant réussir sans l'erreur « Accès refusé ».

Motif

Ce problème est causé par l'ID de bogue Cisco CSCwm59777, qui concerne la gestion des noms de domaine IP pendant les mises à niveau d'ISE 3.3 à ISE 3.4. Pendant le processus de mise à niveau, la configuration du nom de domaine de niveau supérieur du noeud est supprimée, empêchant ISE de résoudre correctement son propre nom de domaine complet. Cela entraîne deux problèmes connexes :

1. Échec de la résolution DNS : ISE ne peut pas résoudre son propre nom d'hôte, ce qui entraîne l'échec de la validation du nom d'hôte lors du traitement d'authentification SAML.
2. Non-concordance du SAN du certificat : Le certificat d'administration par défaut n'inclut pas l'adresse IP du noeud dans le champ SAN, ce qui entraîne des échecs de connexion SSL lorsque ISE tente une validation HTTPS interne en utilisant l'adresse IP comme secours.

La combinaison de ces problèmes entraîne une authentification Azure Entra SAML réussie suivie d'un refus d'accès ISE en raison d'un échec de la validation du certificat interne.

Autres informations utiles

- ID de bogue Cisco CSCwm59777
- Configurer le flux de connexion de l'administrateur ISE via SAML SSO avec Azure AD
- 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.