Fehlerbehebung: Fehler bei der ISE-SAML-Admin-Anmeldung mit verweigertem Zugriff aufgrund einer fehlenden Konfiguration des Domänennamens

Inhalt

Problem

Die Anmeldung bei der Identity Services Engine (ISE)-Admin Security Assertion Markup Language (SAML) schlägt nach einer erfolgreichen Azure Entra-Authentifizierung mit dem Fehler "Zugriff verweigert" fehl. Obwohl Azure Entra eine erfolgreiche SAML-Authentifizierung aufweist, verweigert die ISE den Zugriff auf das Verwaltungsportal. Darüber hinaus schlägt die CSR-Generierung (Certificate Signing Request) mit dem folgenden Fehler fehl:

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

ISE-Protokolle zeigen Fehler bei der DNS-Auflösung für die FQDN- und SSL-Handshake-Ausnahmen des Knotens während der internen HTTPS-Validierung an:

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

Das System zeigt außerdem wiederholt Warnungen über abgelaufene selbstsignierte Standardzertifikate und RESTConf-Rückfälle auf HTTP an, da das Zertifikat nicht verfügbar ist.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.4 Patch 3

- Azure Entra (ehemals Azure AD), konfiguriert als SAML Identity Provider
- ISE-Management, auf das sowohl über IP-Adresse als auch FQDN zugegriffen wird
- Umgebungsaktualisierung von ISE 3.3 auf 3.4

Auflösung

1. Überprüfen Sie die aktuelle ISE-Knotenkonfiguration und die DNS-Auflösung, indem Sie die folgenden Befehle ausführen:

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


Anmerkung: Die erwarteten Ergebnisse zeigen, dass die DNS-Auflösung erfolgreich war und die richtige IP-Adresse ohne DNS-Fehler zurückgegeben wurde.

---

2. Fügen Sie den Domänennamen der ISE-Knotenkonfiguration mithilfe der ISE-CLI erneut hinzu:

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

3. Navigieren Sie in der ISE-GUI zu Administration > System > Certificates > Certificates (Verwaltung > System > Zertifikate > Zertifikate), und generieren Sie das selbstsignierte Standardzertifikat neu. Stellen Sie sicher, dass das neue Zertifikat den FQDN und die IP-Adresse im Feld "Subject Alternative Name (SAN)" (Alternativer Antragstellername) enthält.

4. Vergewissern Sie sich, dass das neu generierte Zertifikat die Knoten-IP-Adresse im SAN-Feld enthält und ordnungsgemäß an die Admin- und Portal-Services gebunden ist.

5. Testen der ISE-Admin-SAML-Anmeldung Die Authentifizierung sollte nun ohne den Fehler "Zugriff verweigert" erfolgreich sein.

Ursache

Dieses Problem wird durch die Cisco Bug-ID CSCwm59777 verursacht, die sich auf die Behandlung von IP-Domänennamen während Upgrades von ISE 3.3 auf ISE 3.4 bezieht. Während des Upgradeprozesses wird die Konfiguration des übergeordneten Domänennamen des Knotens entfernt, sodass ISE seinen eigenen FQDN nicht ordnungsgemäß auflösen kann. Dies führt zu zwei Problemen:

1. Fehler bei der DNS-Auflösung: Die ISE kann ihren eigenen Hostnamen nicht auflösen, sodass interne HTTPS-Aufrufe während der SAML-Authentifizierungsverarbeitung nicht als Hostname validiert werden können.
2. Zertifikat-SAN-Diskrepanz: Das Standard-Admin-Zertifikat enthält die Knoten-IP-Adresse nicht im SAN-Feld, was zu SSL-Handshake-Fehlern führt, wenn die ISE eine interne HTTPS-Validierung unter Verwendung der IP-Adresse als Fallback versucht.

Die Kombination dieser Probleme führt zu einer erfolgreichen Azure Entra SAML-Authentifizierung, gefolgt von einer ISE-Zugriffsverweigerung aufgrund einer fehlgeschlagenen internen Zertifikatvalidierung.

Verwandte Inhalte

- Cisco Bug-ID CSCwm59777
- Konfigurieren des ISE-Admin-Anmeldeflusses über SAML SSO mit Azure AD
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.