Risoluzione dei problemi relativi all'accesso SAML di amministrazione di ISE: accesso negato a causa di una configurazione del nome di dominio mancante

Sommario

Problema

L'accesso SAML (Security Assertion Markup Language) dell'amministratore di Identity Services Engine (ISE) non riesce e viene visualizzato l'errore "Accesso negato" dopo la corretta autenticazione di Azure Entra. Anche se Azure Entra mostra un'autenticazione SAML riuscita, ISE nega l'accesso al portale di gestione. Inoltre, la generazione della richiesta di firma del certificato (CSR) ha esito negativo e ha restituito il seguente errore:

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

I registri ISE mostrano gli errori di risoluzione DNS per le eccezioni dell'handshake SSL e dell'FQDN del nodo durante la convalida HTTPS interna:

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

Vengono inoltre visualizzati avvisi ripetuti relativi ai certificati autofirmati predefiniti scaduti e al fallback di RESTConf al protocollo HTTP a causa della mancata disponibilità dei certificati.

Ambiente

- Patch 3 di Cisco Identity Services Engine (ISE) versione 3.4

- Azure Entra (in precedenza Azure AD) configurato come provider di identità SAML
- Gestione ISE accessibile tramite indirizzo IP e FQDN
- Ambiente aggiornato da ISE 3.3 a 3.4

Risoluzione

1. Verificare la configurazione corrente del nodo ISE e la risoluzione DNS eseguendo i seguenti comandi:

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

Nota: I risultati previsti indicano che la risoluzione DNS ha restituito l'indirizzo IP corretto senza errori DNS.

---

2. Aggiungere nuovamente il nome di dominio alla configurazione del nodo ISE utilizzando la CLI di ISE:

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

3. Passare a Amministrazione > Sistema > Certificati > Certificati nella GUI ISE e rigenerare il certificato autofirmato predefinito. Verificare che il nuovo certificato includa sia il nome di dominio completo (FQDN) che l'indirizzo IP nel campo Nome alternativo soggetto (SAN).

4. Verificare che il certificato rigenerato includa l'indirizzo IP del nodo nel campo SAN e sia correttamente associato sia al servizio Amministratore che al servizio Portale.

5. Verificare l'accesso SAML dell'amministratore ISE. L'autenticazione dovrebbe ora avere esito positivo senza l'errore "Accesso negato".

Causa

Il problema è causato dall'ID bug Cisco CSCwm59777, relativo alla gestione dei nomi di dominio IP durante gli aggiornamenti da ISE 3.3 a ISE 3.4. Durante il processo di aggiornamento, viene rimossa la configurazione del nome di dominio di primo livello del nodo, che impedisce ad ISE di risolvere correttamente il proprio FQDN. Ciò causa due problemi correlati:

1. Risoluzione DNS non riuscita: ISE non è in grado di risolvere il proprio nome host. Le chiamate HTTPS interne non riusciranno a convalidare il nome host durante l'elaborazione dell'autenticazione SAML.
2. Mancata corrispondenza SAN certificato: Il certificato di amministrazione predefinito non include l'indirizzo IP del nodo nel campo SAN, causando errori di handshake SSL quando ISE tenta la convalida HTTPS interna utilizzando l'indirizzo IP come fallback.

La combinazione di questi problemi determina la riuscita dell'autenticazione SAML di Azure Entra, seguita dal rifiuto dell'accesso ISE a causa di una convalida del certificato interno non riuscita.

Contenuto correlato

- ID bug Cisco CSCwm5977
- Configurare il flusso di accesso dell'amministratore ISE tramite SAML SSO con Azure AD
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).