

ドメイン名設定の欠落が原因でアクセスが拒否された場合のISE Admin SAMLログインのトラブルシューティング

内容

お問い合わせ内容

Azure Entraの認証に成功すると、Identity Services Engine (ISE)のSecurity Assertion Markup Language (SAML)へのログインが失敗し、「アクセス拒否」エラーが表示されます。Azure EntraはSAML認証の成功を示しますが、ISEは管理ポータルへのアクセスを拒否します。また、証明書署名要求(CSR)の生成が失敗し、次のエラーが表示されます。

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

ISEログには、内部HTTPS検証中のノードのFQDNおよびSSLハンドシェイクの例外に対するDNS解決エラーが示されます。

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

また、デフォルトの自己署名証明書の有効期限が切れたこと、および証明書が使用できないためにRESTConfがHTTPにフォールバックすることについて、繰り返し警告が表示されます。

環境

- Cisco Identity Services Engine(ISE)バージョン3.4パッチ3
- SAML IDプロバイダーとして構成されたAzure Entra (以前のAzure AD)
- IPアドレスとFQDNの両方を介してアクセスされるISE管理

- ISE 3.3から3.4への環境アップグレード

解決策

1. 次のコマンドを実行して、現在のISEノード設定とDNS解決を確認します。

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



注:DNS解決が成功し、正しいIPアドレスが返され、DNSエラーが発生していないことが予期される結果として示されます。

2. ISE CLIを使用して、ドメイン名をISEノード設定に再度追加します。

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

3. ISE GUIでAdministration > System > Certificates > Certificatesの順に移動し、デフォルトの自己署名証明書を再生成します。新しい証明書のSubject Alternative Name(SAN)フィールドにFQDNとIPアドレスの両方が含まれていることを確認します。

4. 再生成された証明書のSANフィールドにノードのIPアドレスが含まれており、管理者サービスとポータルサービスの両方に正しくバインドされていることを確認します。

5. ISE管理SAMLログインをテストします。これで、「Access Denied」エラーなしで認証が成功するはずです。

原因

この問題は、ISE 3.3からISE 3.4へのアップグレード中のIPドメイン名の処理に関連する[Cisco Bug ID CSCwm59777](#)が原因で発生します。アップグレードプロセス中に、ノードのトップレベ

ルドメイン名の設定が削除され、ISEはそれ自体のFQDNを正しく解決できなくなります。これにより、次の2つの関連する問題が発生します。

1. DNS解決の失敗: ISEが自身のホスト名を解決できないため、内部HTTPSコールがSAML認証処理中にホスト名の検証に失敗します。
2. 証明書SANの不一致: デフォルトの管理証明書のSANフィールドにノードのIPアドレスが含まれていないため、ISEがIPアドレスをフォールバックとして使用して内部HTTPS検証を試行すると、SSLハンドシェイクが失敗します。

これらの問題の組み合わせにより、内部証明書の検証に失敗したため、Azure Entry SAML認証が成功した後、ISEアクセスが拒否されます。

関連コンテンツ

- [Cisco Bug ID CSCwm59777](#)
- [Azure ADを使用したSAML SSOによるISE管理者ログインフローの設定](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。