Troubleshooting de Falha de Logon SAML de Administrador do ISE com Acesso Negado Devido à Ausência de Configuração de Nome de Domínio

Contents

Problema

O logon SAML (Security Assertion Markup Language) do administrador do Identity Services Engine (ISE) falha com um erro "Acesso Negado" após uma autenticação do Azure Entra bem-sucedida. Embora o Azure Entra mostre uma autenticação SAML bem-sucedida, o ISE nega o acesso ao portal de gerenciamento. Além disso, a geração de CSR (Certificate Signing Request, Solicitação de assinatura de certificado) falha com o seguinte erro:

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

Os logs do ISE mostram falhas de resolução DNS para as exceções de handshake FQDN e SSL do nó durante a validação interna de HTTPS:

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

O sistema também exibe avisos repetidos sobre certificados padrão autoassinados expirados e RESTConf retornando para HTTP devido à indisponibilidade do certificado.

Ambiente

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

- Azure Entra (antigo Azure AD) configurado como Provedor de Identidade SAML
- Gerenciamento ISE acessado via endereço IP e FQDN
- Ambiente atualizado do ISE 3.3 para 3.4

Resolução

1. Verifique a configuração atual do nó ISE e a resolução DNS executando os seguintes comandos:

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


Note: Os resultados esperados mostram resolução de DNS bem-sucedida retornando o endereço IP correto sem erros de DNS.

---

2. Adicione novamente o nome de domínio à configuração do nó do ISE usando a CLI do ISE:

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

3. Navegue até Administration > System > Certificates > Certificates na GUI do ISE e gere novamente o certificado autoassinado padrão. Certifique-se de que o novo certificado inclua o FQDN e o endereço IP no campo Nome alternativo do assunto (SAN).

4. Confirme se o certificado gerado novamente inclui o endereço IP do nó no campo SAN e se está adequadamente associado aos serviços de administrador e portal.

5. Teste o login SAML do administrador do ISE. A autenticação deve agora ser bem-sucedida sem o erro "Acesso negado".

Causa

Esse problema é causado pela ID de bug Cisco CSCwm59777, que se relaciona ao tratamento de nome de domínio IP durante atualizações do ISE 3.3 para o ISE 3.4. Durante o processo de atualização, a configuração de nome de domínio de nível superior do nó é removida, impedindo que o ISE resolva adequadamente seu próprio FQDN. Isso causa dois problemas relacionados:

1. Falha na resolução DNS: O ISE não pode resolver seu próprio nome de host, fazendo com que as chamadas HTTPS internas falhem na validação do nome de host durante o processamento de autenticação SAML.
2. Incompatibilidade de SAN de Certificado: O certificado padrão do administrador não inclui o endereço IP do nó no campo SAN, causando falhas de handshake SSL quando o ISE tenta a validação HTTPS interna usando o endereço IP como fallback.

A combinação desses problemas resulta na autenticação bem-sucedida do Azure Entra SAML seguida pela negação de acesso do ISE devido à falha na validação do certificado interno.

Conteúdo relacionado

- ID de bug Cisco CSCwm59777
- Configurar o Fluxo de Logon do Administrador do ISE via SAML SSO com o Azure AD
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.