由於缺少域名配置，ISE管理員SAML登入失敗，訪問被拒絕

目錄

問題

身份服務引擎(ISE)管理員安全斷言標籤語言(SAML)登入失敗，在成功的Azure Entra身份驗證後出現「訪問被拒絕」錯誤。儘管Azure Entra顯示成功的SAML身份驗證，但ISE拒絕訪問管理門戶。此外，生成證書簽名請求(CSR)失敗，並出現以下錯誤：

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

ISE日誌在內部HTTPS驗證期間顯示節點FQDN和SSL握手異常的DNS解析失敗：

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

系統還會顯示有關過期預設自簽名證書和RESTConf由於證書不可用而回退到HTTP的重複警告。

環境

- 思科身分識別服務引擎(ISE)版本3.4補丁3
- 配置為SAML標識提供程式的Azure Entra（以前為Azure AD）
- 通過IP地址和FQDN訪問ISE管理
- 環境從ISE 3.3升級到3.4

解析

1.通過運行以下命令驗證當前ISE節點配置和DNS解析：

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

附註：預期結果顯示成功的DNS解析返回正確的IP地址，且沒有DNS錯誤。

2.使用ISE CLI將域名重新新增到ISE節點配置中：

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

3.在ISE GUI中導航到Administration > System > Certificates > Certificates，然後重新生成預設自簽名證書。確保新證書在Subject Alternative Name(SAN)欄位中同時包含FQDN和IP地址。

4.確認重新生成的證書在SAN欄位中包含節點IP地址，並且已正確繫結到管理員和門戶服務。

5.測試ISE管理員SAML登入。現在，身份驗證應會成功，而不會出現「Access Denied」（拒絕訪問）錯誤。

原因

此問題由Cisco Bug ID CSCwm5977引起，它涉及從ISE 3.3升級到ISE 3.4期間的IP域名處理。在升級過程中，刪除節點的頂級域名配置，從而阻止ISE正確解析自己的FQDN。這會導致兩個相關問題：

1. DNS解析失敗:ISE無法解析其自己的主機名，導致內部HTTPS呼叫在SAML身份驗證處理期間無法進行主機名驗證。
2. 證書SAN不匹配:預設管理證書在SAN欄位中不包含節點IP地址，當ISE嘗試使用該IP地址作為

回退的內部HTTPS驗證時，會導致SSL握手失敗。

由於內部證書驗證失敗，這些問題的組合導致成功的Azure Entra SAML身份驗證後是ISE訪問拒絕。

相關內容

- Cisco錯誤ID CSCwm59777
- 通過Azure AD的SAML SSO配置ISE管理員登入流
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。