排除ISE管理员SAML登录失败，由于缺少域名配置，访问被拒绝

目录

问题

身份服务引擎(ISE)管理员安全断言标记语言(SAML)登录失败，在Azure Entra身份验证成功后出现“访问被拒绝”错误。虽然Azure Entra显示成功的SAML身份验证，但ISE拒绝访问管理门户。此外，证书签名请求(CSR)生成失败，并出现以下错误：

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

ISE日志显示内部HTTPS验证期间节点的FQDN和SSL握手异常的DNS解析失败：

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

系统还会显示有关过期的默认自签名证书和RESTConf由于证书不可用而回退到HTTP的重复警告。

环境

- 思科身份服务引擎(ISE)版本3.4补丁3
- 配置为SAML身份提供程序的Azure Entra（以前为Azure AD）
- 通过IP地址和FQDN访问ISE管理
- 环境从ISE 3.3升级到3.4

分辨率

1.通过运行以下命令验证当前ISE节点配置和DNS解析：

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

注意：预期结果显示成功的DNS解析返回了正确的IP地址，没有DNS错误。

2.使用ISE CLI将域名重新添加到ISE节点配置：

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

3.在ISE GUI中导航到Administration > System > Certificates > Certificates并重新生成默认自签名证书。确保新证书在Subject Alternative Name(SAN)字段中同时包含FQDN和IP地址。

4.确认重新生成的证书在SAN字段中包含节点IP地址，并且已正确绑定到管理员和门户服务。

5.测试ISE管理员SAML登录。身份验证现在应会成功，不会出现“Access Denied”（拒绝访问）错误。

原因

此问题由Cisco Bug ID CSCwm59777引起，它与ISE 3.3升级到ISE 3.4期间的IP域名处理有关。在升级过程中，会删除节点的顶级域名配置，从而阻止ISE正确解析自己的FQDN。这会导致两个相关问题：

1. DNS解析故障:ISE无法解析其自己的主机名，导致内部HTTPS调用在SAML身份验证处理期间无法进行主机名验证。
2. 证书SAN不匹配:默认管理员证书在SAN字段中不包含节点IP地址，当ISE尝试使用该IP地址作

为回退进行内部HTTPS验证时，会导致SSL握手失败。

结合这些问题可导致Azure Entra SAML身份验证成功，随后由于内部证书验证失败导致ISE访问拒绝。

相关内容

- 思科漏洞ID CSCwm59777
- 通过Azure AD的SAML SSO配置ISE管理员登录流
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。