Solución de problemas de inicio de sesión de SAML de administración de ISE con acceso denegado debido a una configuración de nombre de dominio faltante

Contenido

Problema

El inicio de sesión del Lenguaje de marcado de aserción de seguridad (SAML) del administrador de Identity Services Engine (ISE) falla con un error de acceso denegado después de una autenticación correcta de Azure Entra. Aunque Azure Entra muestra una autenticación SAML satisfactoria, ISE deniega el acceso al portal de administración. Además, la generación de la solicitud de firma de certificado (CSR) produce el siguiente error:

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

Los registros de ISE muestran errores de resolución de DNS para las excepciones de protocolo de enlace FQDN y SSL del nodo durante la validación HTTPS interna:

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

El sistema también muestra advertencias repetidas sobre certificados autofirmados predeterminados caducados y RESTConf que vuelve a HTTP debido a la indisponibilidad del certificado.

Entorno

- Parche 3 de Cisco Identity Services Engine (ISE) versión 3.4

- Azure Entra (anteriormente Azure AD) configurado como proveedor de identidad SAML
- Gestión de ISE a la que se accede mediante dirección IP y FQDN
- Entorno actualizado de ISE 3.3 a 3.4

Resolución

1. Verifique la configuración actual del nodo ISE y la resolución DNS ejecutando los siguientes comandos:

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

Nota: Los resultados esperados muestran una resolución de DNS correcta que devuelve la dirección IP correcta sin errores de DNS.

---

2. Vuelva a agregar el nombre de dominio a la configuración del nodo ISE mediante la CLI de ISE:

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

3. Vaya a Administration > System > Certificates > Certificates en la GUI de ISE y regenere el certificado autofirmado predeterminado. Asegúrese de que el nuevo certificado incluye el FQDN y la dirección IP en el campo Nombre alternativo del sujeto (SAN).

4. Confirme que el certificado regenerado incluye la dirección IP del nodo en el campo SAN y que está enlazado correctamente a los servicios de administración y de portal.

5. Pruebe el inicio de sesión SAML de administración de ISE. La autenticación debería realizarse ahora sin el error "Acceso denegado".

Causa

Este problema es causado por el Id. de bug Cisco CSCwm59777, que se relaciona con la gestión de nombres de dominio IP durante las actualizaciones de ISE 3.3 a ISE 3.4. Durante el proceso de actualización, se elimina la configuración de nombres de dominio de nivel superior del nodo, lo que impide que ISE resuelva correctamente su propio FQDN. Esto causa dos problemas relacionados:

1. Error de resolución DNS: ISE no puede resolver su propio nombre de host, lo que hace que las llamadas HTTPS internas no puedan validar el nombre de host durante el procesamiento de autenticación SAML.
2. Discordancia de SAN de certificado: El certificado de administración predeterminado no incluye la dirección IP del nodo en el campo SAN, lo que provoca errores de protocolo de enlace SSL cuando ISE intenta la validación HTTPS interna utilizando la dirección IP como reserva.

La combinación de estos problemas da como resultado una autenticación SAML de Azure Entra satisfactoria seguida de una denegación de acceso a ISE debido a una validación de certificado interno errónea.

Contenido relacionado

- ID de bug de Cisco CSCwm59777
- Configuración del flujo de inicio de sesión de administración de ISE mediante SSO de SAML con Azure AD
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).