Resolver código de error de ACI F3081: certificado SAML que vence

Contenido

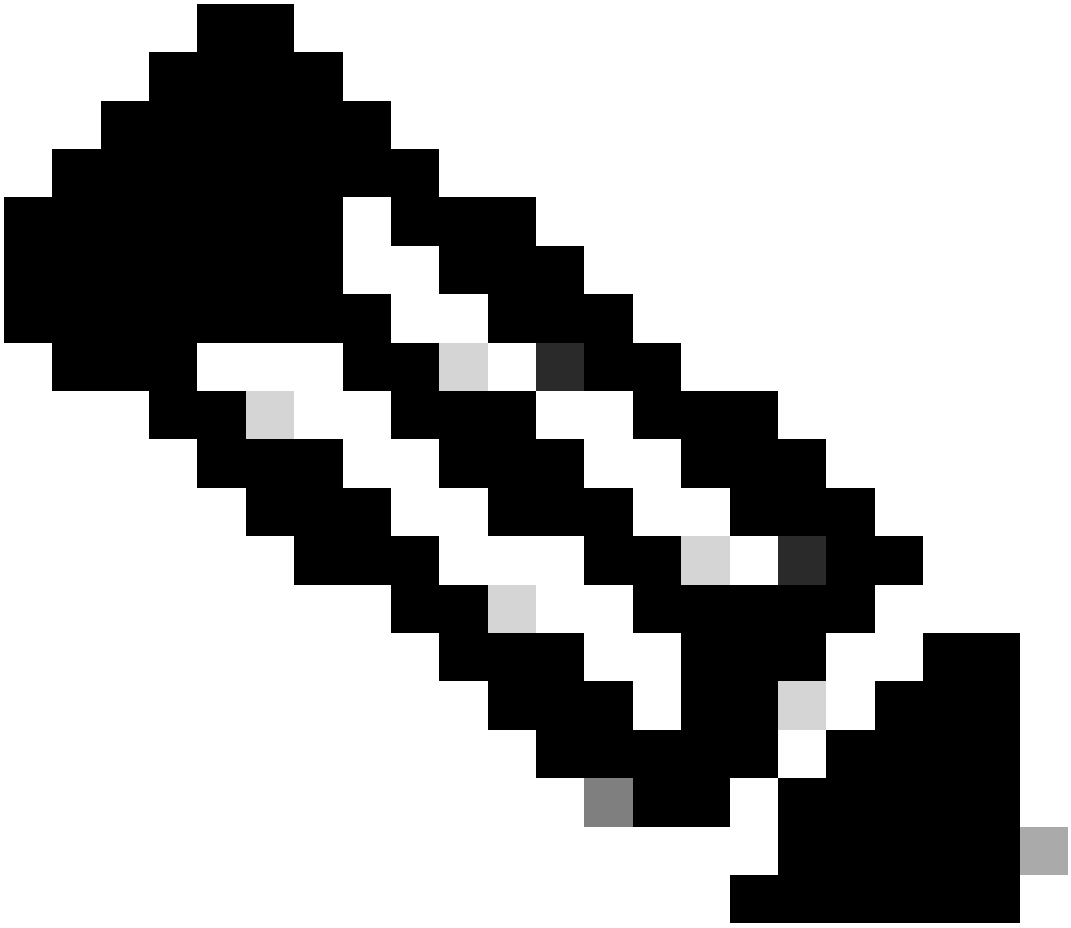
Introducción

Este documento describe ACI Fault F3081 y sus pasos de remediación.

Antecedentes

Este error ocurre cuando un certificado X.509 de SAML va a caducar en un mes en un APIC.

```
F3081: fltAaaSamlEncCertSamlEncCertExpiring
Severity: major
Explanation: This fault occurs when the SAML X.509 Certificate is going to expire in one month.
Recommended Action: If you see this fault, take the following actions:
Update SAML X.509 Certificate soon.
```



Nota: La misma ocurrencia puede ocurrir incluso sin la implementación SAML. Sin embargo, si no se utiliza SAML, no tiene ningún impacto en el sistema.

Intersight Connected ACI Fabrics

Este fallo se supervisa activamente como parte de los compromisos proactivos de ACI.

Si tiene un fabric ACI conectado a Intersight, se genera una solicitud de servicio en su nombre para indicar que se han encontrado casos de este fallo en el fabric ACI conectado a Intersight.

Inicio rápido para solucionar errores

1. Validar el estado de vencimiento del certificado X.509 de SAML, si muestra Expiring o Expired Fault, F3081 se genera.

2. Verifique si el emisor del certificado es Cisco o de terceros.

3. Si el emisor es Cisco, continúe con la regeneración del par de claves de cifrado SAML.

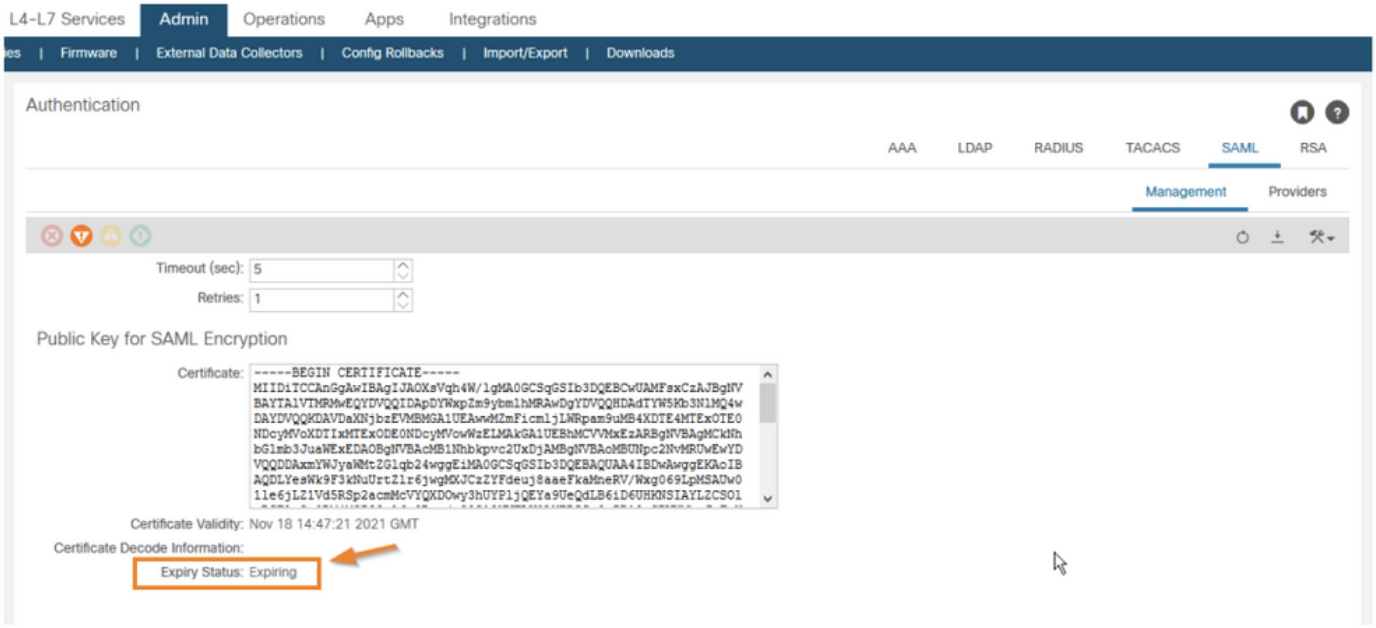
Pasos detallados para abordar la falla

Validar estado de vencimiento del certificado SAML X.509

Mediante la GUI de APIC

1. Acceda a Admin > AAA > Authentication > SAML > Management.

2. Validar el estado de caducidad del certificado SAML X.509. Expiring significa que el certificado está a punto de caducar en un mes.



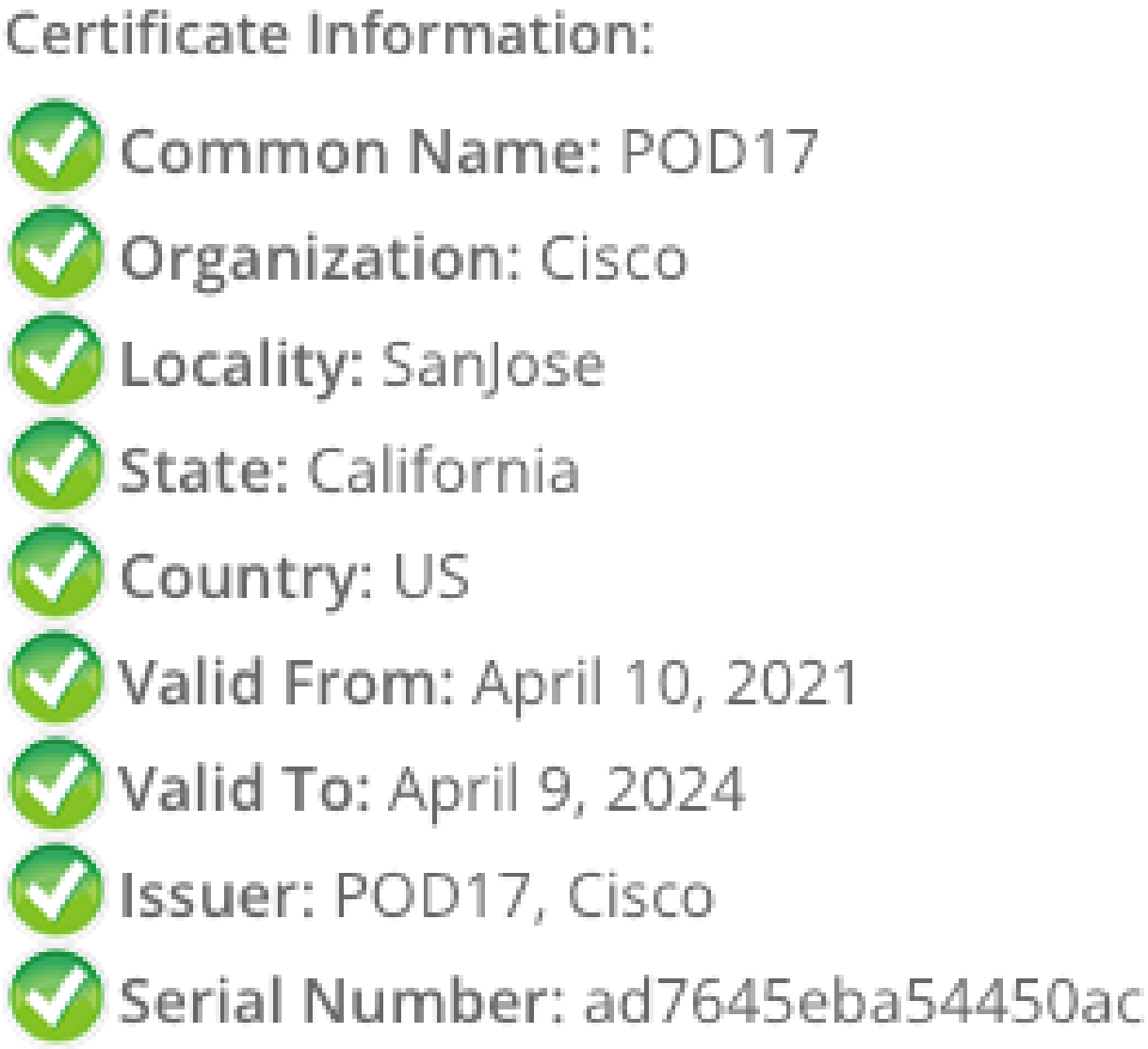
Regenere y renueve el certificado SAML X.509

Para resolver este error, puede eliminarlo regenerando y renovando el certificado y ampliando su fecha de vencimiento.

La regeneración del certificado X.509 de SAML no tiene ningún impacto.

Antes de continuar, asegúrese de comprobar de nuevo si el emisor de la autoridad de certificación (CA) del certificado es Cisco o una entidad de terceros.

Para obtener el contenido del certificado de APIC, decodifique el certificado en cualquier descodificador X.509 para obtener los parámetros del certificado:

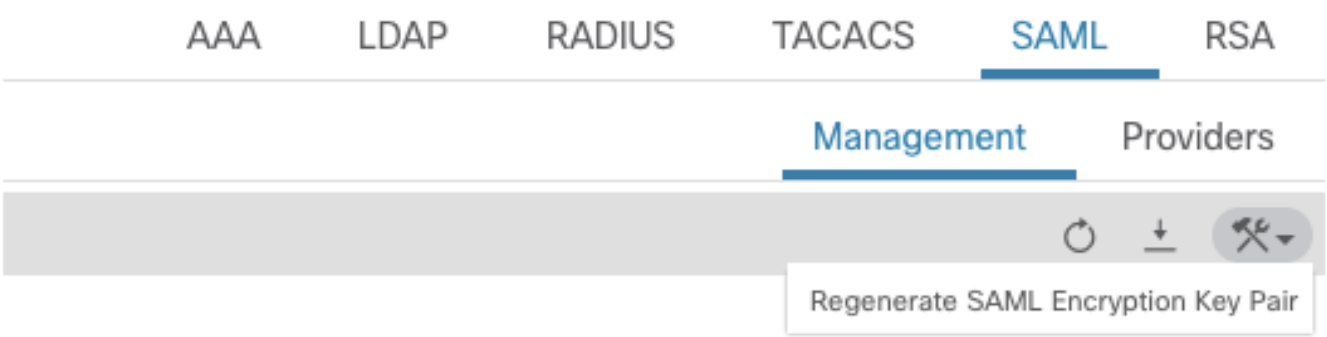


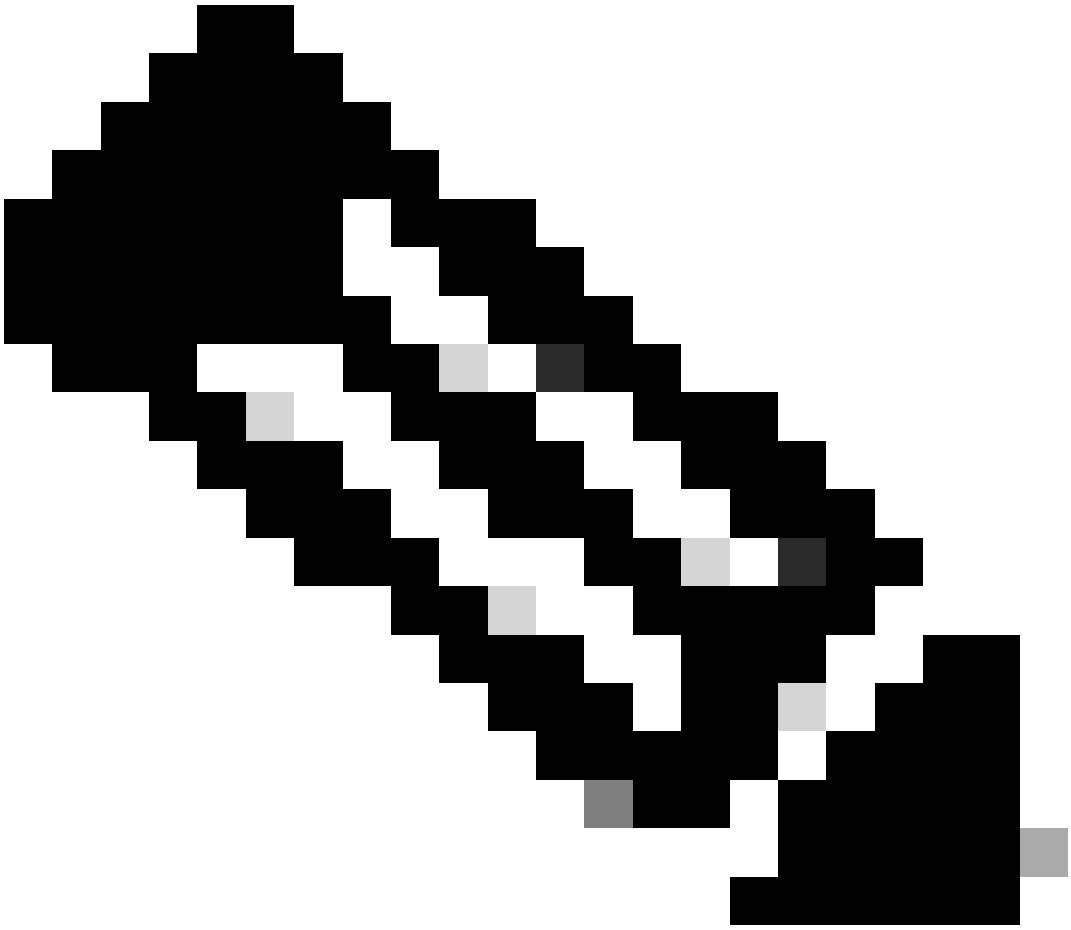
Si el certificado fue emitido por una CA de terceros, póngase en contacto con la CA para renovar el certificado X.509 de SAML.

Sin embargo, si el emisor del certificado es Cisco, puede continuar con estos pasos.

Mediante GUI de APIC

1. Acceda a Admin > AAA > Authentication > SAML > Management > Regenerate SAML Encryption Key Pair.



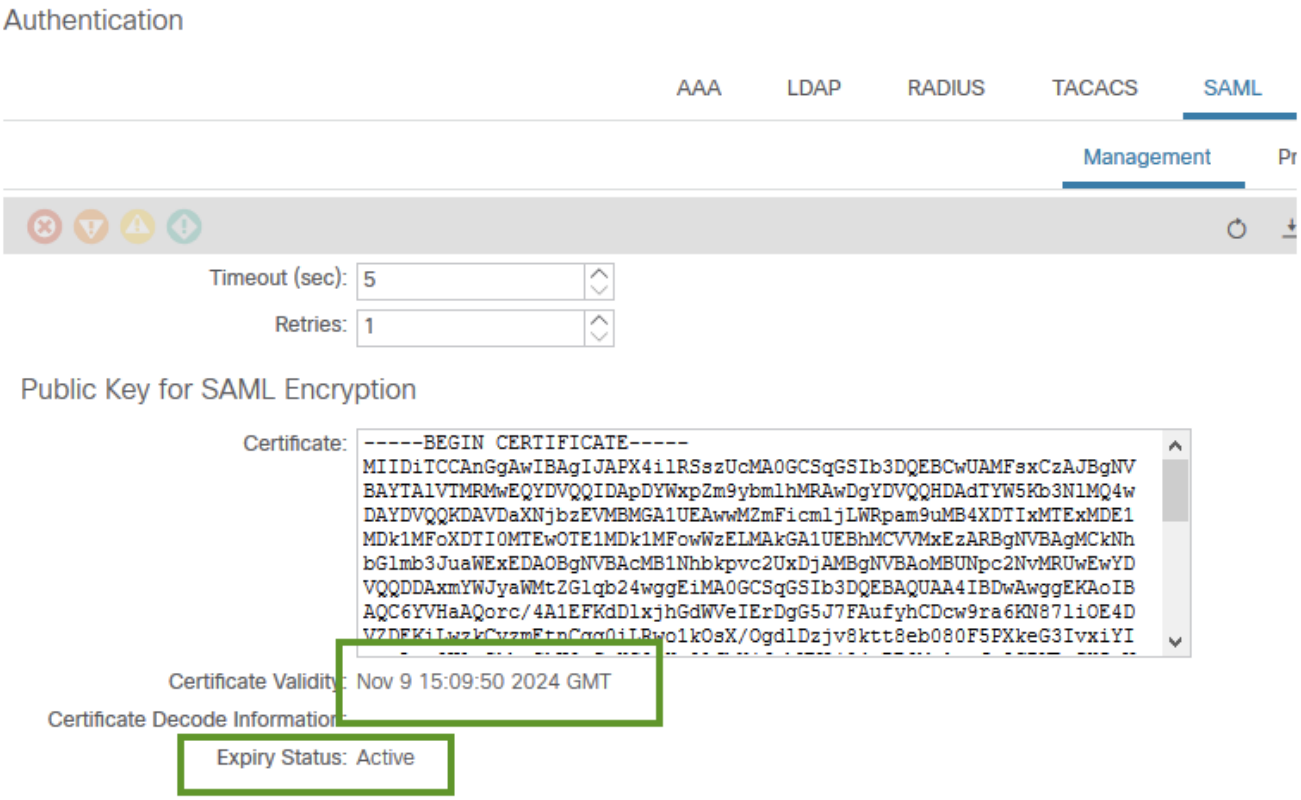


Nota: al renovar el certificado, la fecha de caducidad que aparece en Validez del certificado se amplía a una fecha que es tres años posterior a la fecha de renovación.

Validar si el estado de vencimiento cambia a Activo

Mediante la GUI de APIC

1. Acceda a Admin > AAA > Authentication > SAML > Management.



Additional Information

SAML es un formato de datos estándar abierto basado en XML que permite a los administradores acceder a un conjunto definido de aplicaciones de Cisco Collaboration sin problemas después de iniciar sesión en una de esas aplicaciones. SAML describe el intercambio de información relacionada con la seguridad entre partners empresariales de confianza. Es un protocolo de autenticación utilizado por los proveedores de servicios para autenticar a un usuario. SAML permite el intercambio de información de autenticación de seguridad entre un proveedor de identidad (IdP) y un proveedor de servicios.

El SSO de SAML utiliza el protocolo SAML 2.0 para ofrecer SSO entre dominios y entre productos para las soluciones de Cisco Collaboration. SAML 2.0 habilita el SSO en todas las aplicaciones de Cisco y permite la federación entre aplicaciones de Cisco y un IdP. SAML 2.0 también permite que los usuarios administrativos de Cisco accedan a dominios web seguros para intercambiar datos de autenticación y autorización de usuarios, entre un IdP y un Proveedor de Servicios mientras se mantienen altos niveles de seguridad. La función proporciona mecanismos seguros para utilizar credenciales comunes e información relevante en varias aplicaciones.

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).