

Resolver código de falha da ACI F3081: Expirando certificado SAML

Contents

[Introdução](#)

[Informações de Apoio](#)

[Malhas da Intersight Connected ACI](#)

[Início rápido para solucionar falha](#)

[Etapas detalhadas para solucionar a falha](#)

[Validar Status de Expiração do Certificado X.509 do SAML](#)

[Regenerar e Renovar o Certificado X.509 SAML](#)

[Validar se o status de expiração for alterado para Ativo](#)

[Informações adicionais](#)

Introdução

Este documento descreve a falha F3081 da ACI e suas etapas de correção.

Informações de Apoio

Essa falha ocorre quando um certificado SAML X.509 expirará em um mês em um 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.



Observação: a mesma ocorrência pode ocorrer mesmo sem a implementação SAML. No entanto, se o SAML não estiver sendo usado, ele não terá nenhum impacto no sistema.

Malhas da Intersight Connected ACI

Essa falha é monitorada ativamente como parte dos [contratos de ACI proativos](#).

Se você tiver uma estrutura da ACI conectada à Intersight, uma solicitação de serviço será gerada em seu nome para indicar que instâncias dessa falha foram encontradas na estrutura da ACI conectada à Intersight.

Início rápido para solucionar falha

1. Valide o status Vencimento do certificado SAML X.509 se ele mostrar Falha expirando ou expirada, F3081 é gerado.
2. Verifique se o Emissor do Certificado é da Cisco ou de Terceiros.

3. Se o Emissor for a Cisco, continue com a regeneração do Par de chaves de criptografia SAML.

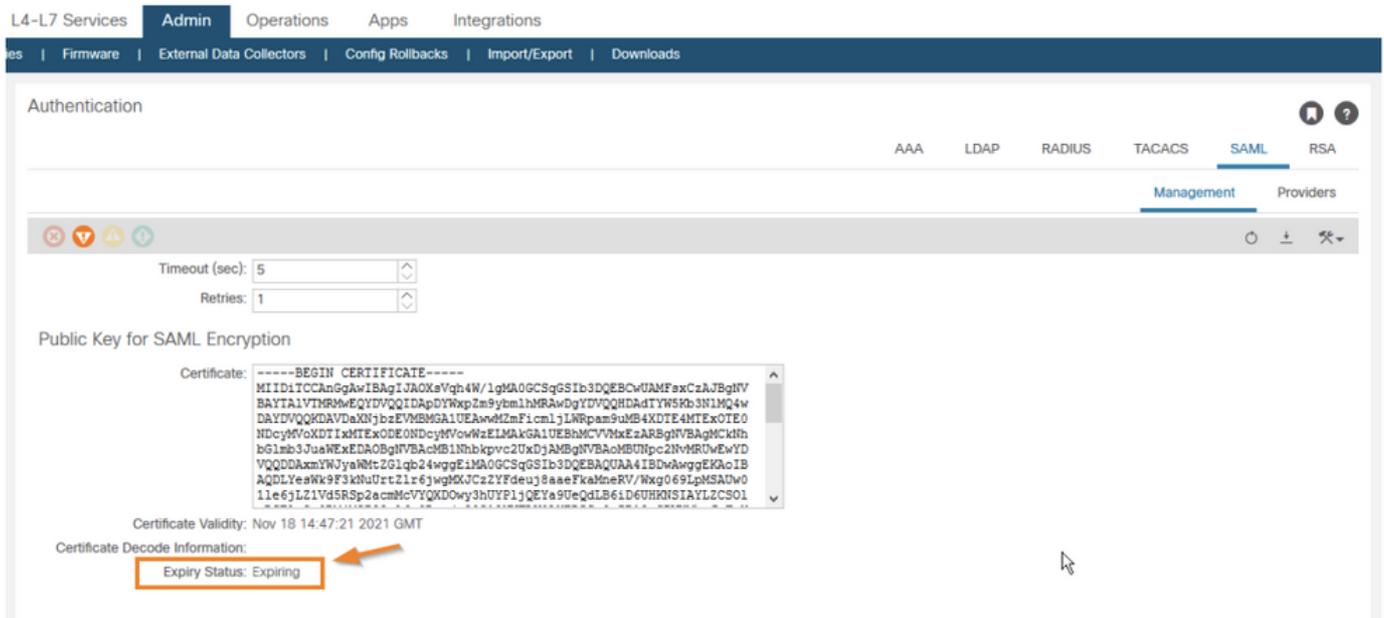
Etapas detalhadas para solucionar a falha

Validar Status de Expiração do Certificado X.509 do SAML

Através da GUI do APIC

1. Navegue até Admin > AAA > Authentication > SAML > Management.

2. Validar o status de Expiração do Certificado SAML X.509. Expiring significa que o certificado está prestes a expirar em um mês.



Regenerar e Renovar o Certificado X.509 SAML

Para resolver essa falha, você pode limpá-la regenerando e renovando o certificado e estendendo sua data de expiração.

Regenerar o certificado SAML X.509 não tem nenhum impacto.

Antes de continuar, verifique se o emissor da autoridade de certificação (CA) para o certificado é a Cisco ou uma entidade de terceiros.

Para obter o conteúdo do certificado do APIC, decodifique o certificado em qualquer decodificador X.509 para obter os parâmetros do certificado:

Certificate Information:

- ✓ Common Name: POD17
- ✓ Organization: Cisco
- ✓ Locality: Sanjose
- ✓ State: California
- ✓ Country: US
- ✓ Valid From: April 10, 2021
- ✓ Valid To: April 9, 2024
- ✓ Issuer: POD17, Cisco
- ✓ Serial Number: ad7645eba54450ac

Se o certificado tiver sido emitido por uma CA de terceiros, entre em contato com a CA para renovar seu certificado SAML X.509.

No entanto, se o emissor do certificado for a Cisco, você poderá prosseguir com estas etapas.

Via GUI do APIC

1. Navegue até Admin > AAA > Authentication > SAML > Management > Regenerate SAML Encryption Key Pair.

AAA

LDAP

RADIUS

TACACS

SAML

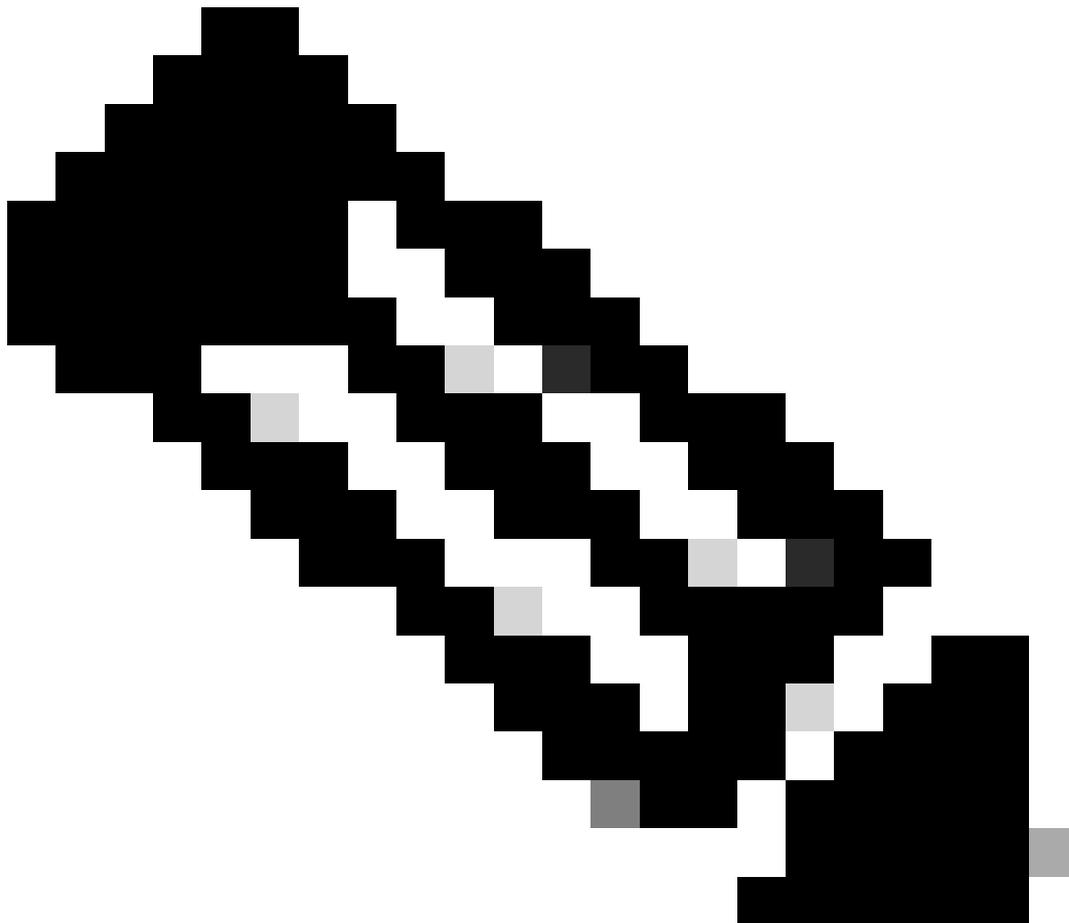
RSA

Management

Providers



Regenerate SAML Encryption Key Pair



Observação: ao renovar o certificado, a data de expiração exibida na Validade do certificado é estendida para uma data que é três anos após a data de renovação.

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.