

ACI障害コードF3081: Expiring SAML Certificateの解決

内容

[はじめに](#)

[背景説明](#)

[Intersight接続ACIファブリック](#)

[迅速な問題解決](#)

[障害に対処するための詳細な手順](#)

[SAML X.509証明書の期限切れステータスの検証](#)

[SAML X.509証明書の再生成と更新](#)

[有効期限の状態がアクティブに変更されたかどうかを検証します](#)

[追加情報](#)

はじめに

このドキュメントでは、ACI障害F3081とその修復手順について説明します。

背景説明

このエラーは、SAML X.509証明書がAPICで1か月で期限切れになる場合に発生します。

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.

注:SAMLを実装していない場合でも、同じ問題が発生する可能性があります。ただし、SAMLが使用されていない場合は、システムに影響しません。

Intersight接続ACIファブリック

このエラーは、[プロアクティブACIエンゲージメント](#)の一部としてアクティブに監視されます。

Intersightに接続されたACIファブリックがある場合、お客様に代わってサービスリクエストが生成されます。これは、このエラーのインスタンスがお客様のIntersightに接続されたACIファブリック内で検出されたことを示します。

迅速な問題解決

1. SAML X.509証明書の期限切れステータスを検証します。期限切れまたは期限切れエラーが表示される場合は、F3081が発生します。
2. 証明書発行者がシスコまたはサードパーティであるかどうかを確認します。

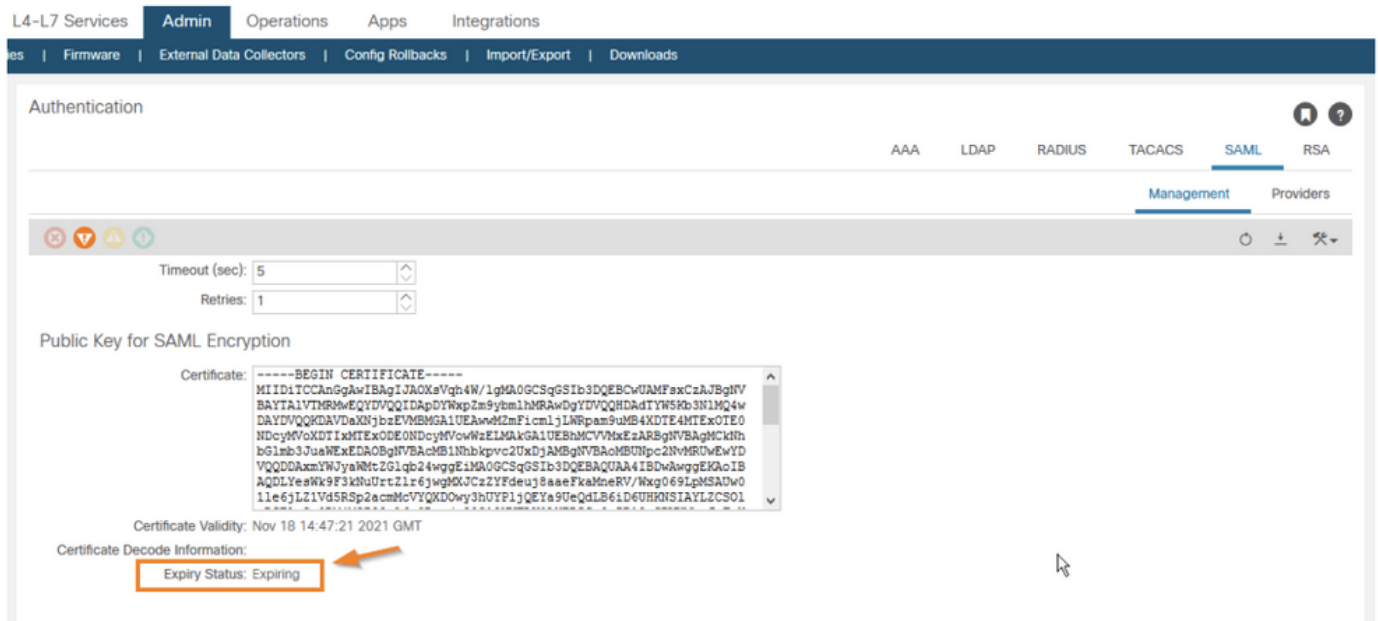
3. 発行者がシスコの場合、SAML暗号化キーペアの再生成を続行します。

障害に対処するための詳細な手順

SAML X.509証明書の期限切れステータスの検証

APIC GUIを使用

1. Admin > AAA > Authentication > SAML > Managementに移動します。
2. SAML X.509証明書の期限切れ状態を検証します。Expiringは、証明書が1か月以内に期限切れになることを意味します。



SAML X.509証明書の再生成と更新

このエラーを解決するには、証明書を再生成して更新し、有効期限を延長することでクリアできます。

SAML X.509証明書を再生成しても影響はありません。

先に進む前に、証明書の認証局(CA)発行者がシスコであるかサードパーティのエンティティであるかを必ず再確認してください。

APICから証明書の内容を取得するには、任意のX.509デコーダで証明書をデコードして、証明書パラメータを取得します。

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

証明書がサードパーティCAによって発行された場合は、SAML X.509証明書の更新についてCAに問い合わせてください。

ただし、証明書の発行者がシスコの場合は、次の手順に進むことができます。

APIC GUIを使用

1. Admin > AAA > Authentication > SAML > Management > Regenerate SAML Encryption Key Pairに移動します。

AAA

LDAP

RADIUS

TACACS

SAML

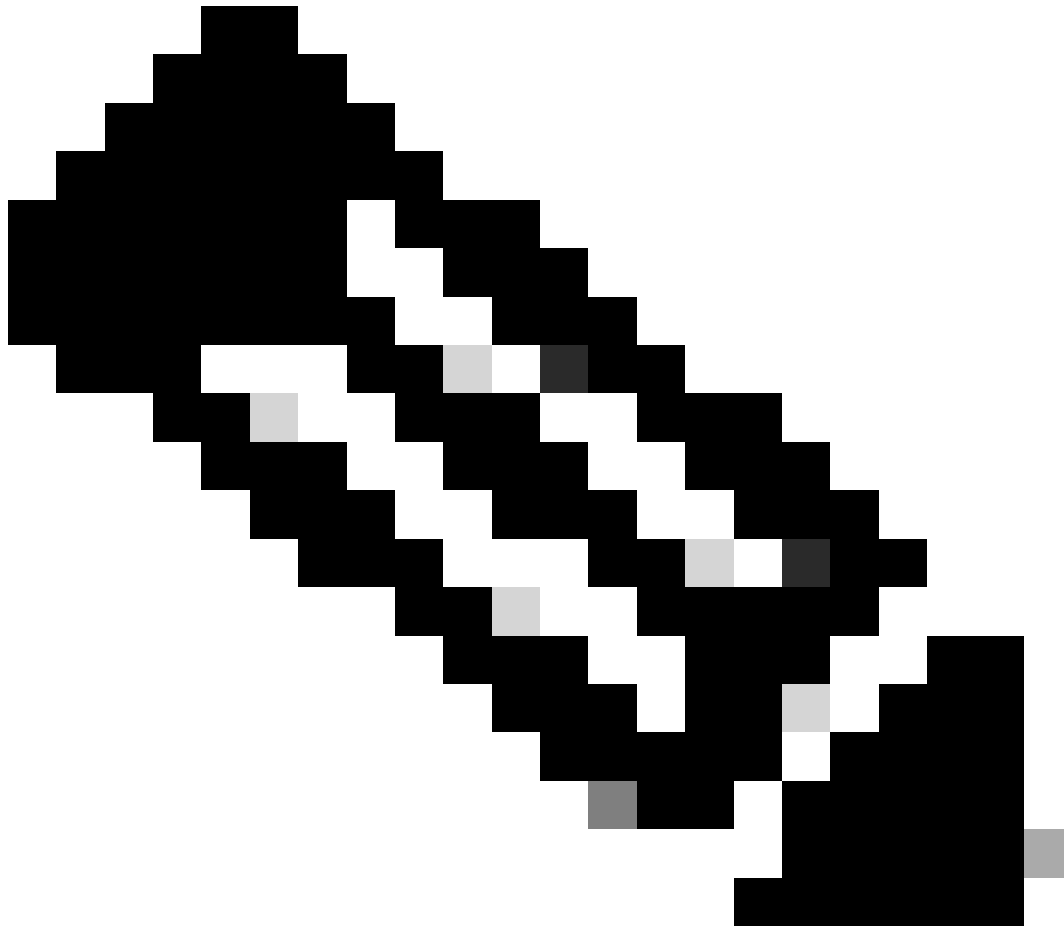
RSA

Management

Providers



Regenerate SAML Encryption Key Pair



注：証明書を更新すると、証明書の有効期間に表示される有効期限が、更新日から3年後の日付に延長されます。

有効期限の状態がアクティブに変更されたかどうかを検証します

APIC GUIを使用

1. Admin > AAA > Authentication > SAML > Managementに移動します。

Authentication

AAA LDAP RADIUS TACACS **SAML**

Management Pr

Timeout (sec): 5
Retries: 1

Public Key for SAML Encryption

Certificate: -----BEGIN CERTIFICATE-----
MIIDIITCCAnGgAwIBAgIJAPX4i1RSszUcMA0GCSqGSIb3DQEBCwUAMFsx CzA JBgNV
BAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRAwDgYDVQQHDAdTYW5Kb3N1MQ4w
DAYDVQQKDAVDaXNjbzEVMBMGA1UEAwMZmFicmljLWVpam9uMB4XDTE1MDk1MDk1
MDk1MFoXDTIOMTEwOTE1MDk1MFowWzELMAkGA1UEBhMCVVMxEzARBgNVBAGMCKNh
bG1mb3JuaWEuEDAOBgNVBAcMB1Nhbkpvc2UxDjAMBgNVBAoMBUNpc2NvMRUwEwYD
VQDDAxmYWJyaWVtZG1qb24wgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQc6YVHaAqorc/4A1EFKdDlxjhGdWVeIErDgG5J7FAufyhCDcw9ra6KN87liOE4D
VZDEKiLwzkCvzmEtpCgg0iLEw01kOsX/Ogd1Dzjv8ktt8eb080F5PXkeG3IvxiYI

Certificate Validity: Nov 9 15:09:50 2024 GMT

Certificate Decode Information

Expiry Status: Active

追加情報

SAMLは、XMLベースのオープンな標準データ形式です。これにより、管理者は、シスココラボレーションアプリケーションのいずれかにサインインした後、定義された一連のシスココラボレーションアプリケーションにシームレスにアクセスできます。

SAMLは、信頼できるビジネスパートナー間でのセキュリティ関連情報の交換を表します。サービスプロバイダーによってユーザの認証に使用される認証プロトコルです。SAMLでは、アイデンティティプロバイダー(IdP)とサービスプロバイダー間でセキュリティ認証情報を交換できます。

SAML SSOは、SAML 2.0プロトコルを使用して、シスココラボレーションソリューションのクロスドメインおよびクロスプロダクトSSOを提供します。SAML 2.0では、シスコアプリケーション間のSSOが有効になり、シスコアプリケーションとIdP間のフェデレーションが有効になります。また、SAML 2.0では、シスコの管理ユーザは、高いセキュリティレベルを維持しながら、IdPとサービスプロバイダー間でユーザ認証および許可データを交換するために、セキュアなWebドメインにアクセスできます。この機能は、さまざまなアプリケーションで共通のクレデンシャルと関連情報を使用するための安全なメカニズムを提供します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。