Résoudre le code d'erreur ACI F3081 : expiration du certificat SAML

Table des matières

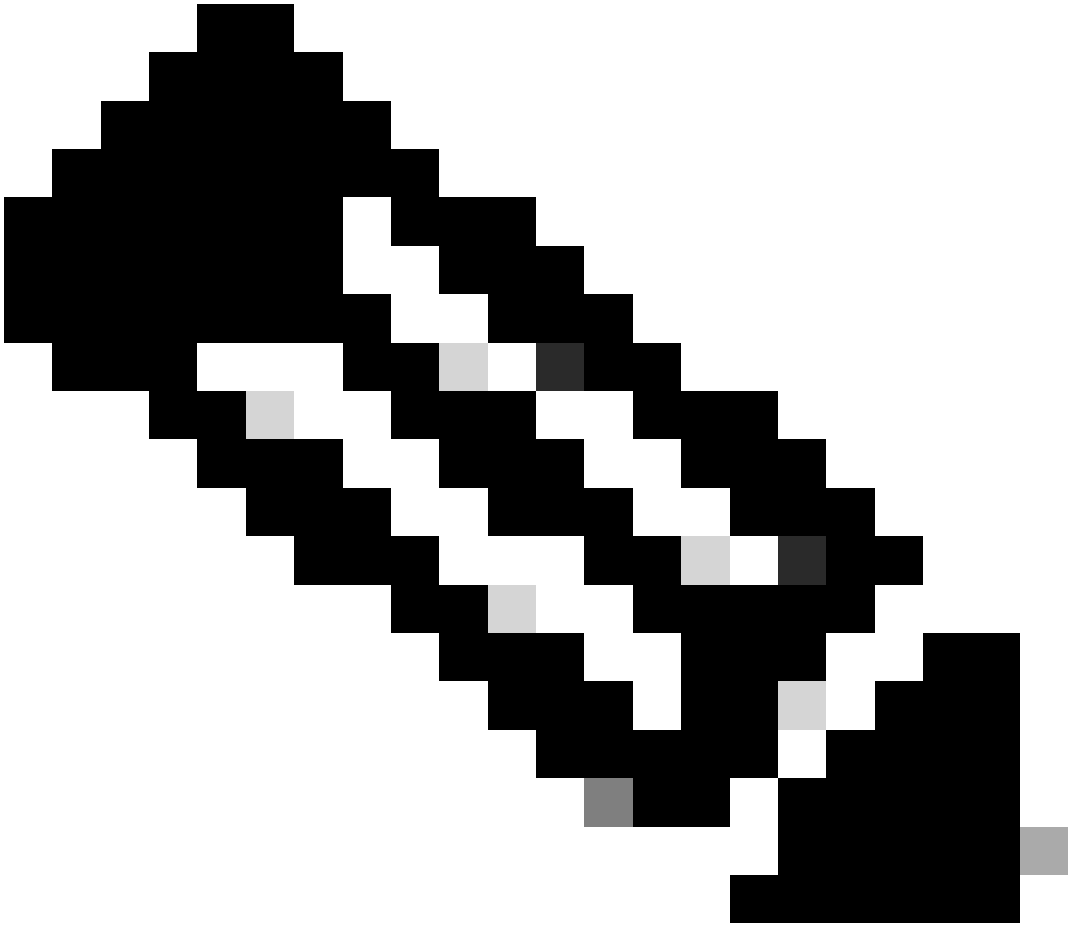
Introduction

Ce document décrit la panne de l'ACI F3081 et ses étapes de correction.

Informations générales

Cette erreur se produit lorsqu'un certificat X.509 SAML arrive à expiration dans un mois sur 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.
```



Remarque : la même occurrence peut se produire même sans implémentation SAML. Toutefois, si SAML n'est pas utilisé, il n'a aucun impact sur le système.

Fabrics ACI Intersight Connected

Cette panne est activement surveillée dans le cadre des engagements proactifs de l'ACI.

Si vous disposez d'un fabric ACI connecté à Intersight, une demande de service est générée en votre nom afin d'indiquer que des instances de cette défaillance ont été trouvées dans votre fabric ACI connecté à Intersight.

Démarrage rapide pour résoudre les défaillances

1. Validez l'état Expiration du certificat SAML X.509, s'il indique Expiring ou Expired Fault, F3081 est activé.

2. Vérifiez si l'émetteur du certificat est Cisco ou un tiers.

3. Si l'émetteur est Cisco, poursuivez la régénération de la paire de clés de chiffrement SAML.

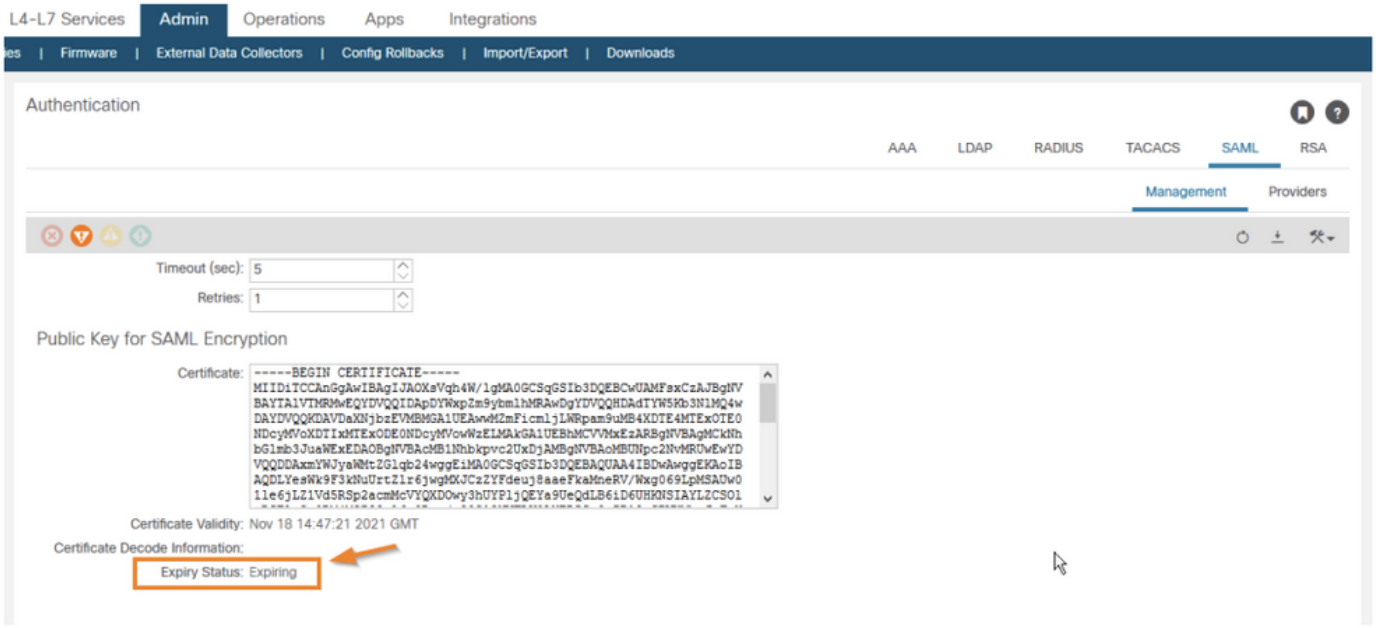
Étapes détaillées pour résoudre les défaillances

Valider l'état d'expiration du certificat SAML X.509

Via l'interface graphique APIC

1. Accédez à Admin > AAA > Authentication > SAML > Management.

2. Validez l'état Expiration du certificat SAML X.509. Expiring signifie que le certificat est sur le point d'expirer dans un mois.



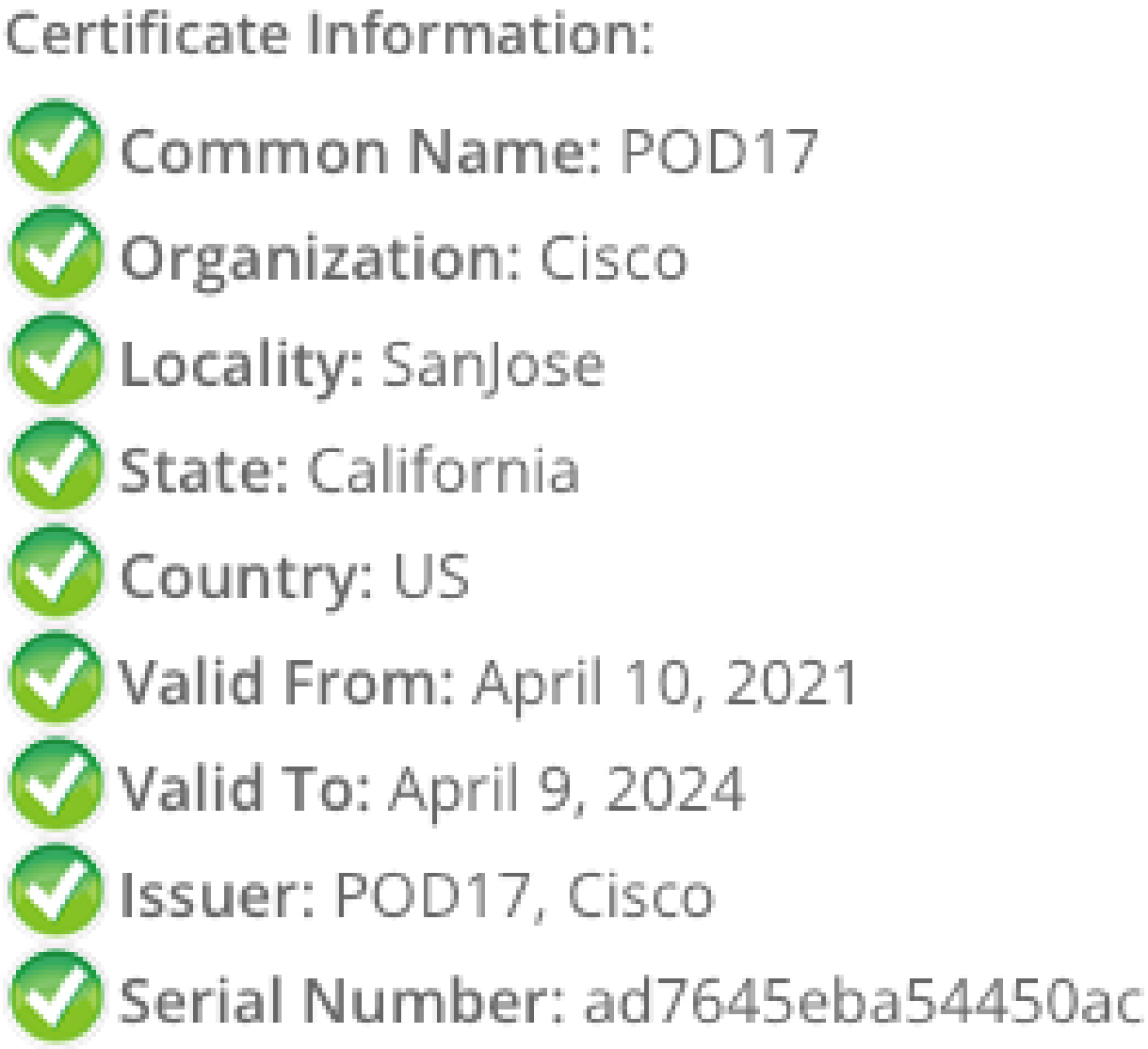
Régénérer et renouveler le certificat SAML X.509

Afin de résoudre cette erreur, vous pouvez l'effacer en régénérant et en renouvelant le certificat et en prolongeant sa date d'expiration.

La régénération du certificat SAML X.509 n'a aucun impact.

Avant de continuer, assurez-vous de vérifier si l'émetteur de l'autorité de certification (CA) pour le certificat est Cisco ou une entité tierce.

Afin d'obtenir le contenu du certificat de l'APIC, décodez le certificat dans n'importe quel décodeur X.509 pour obtenir les paramètres du certificat :

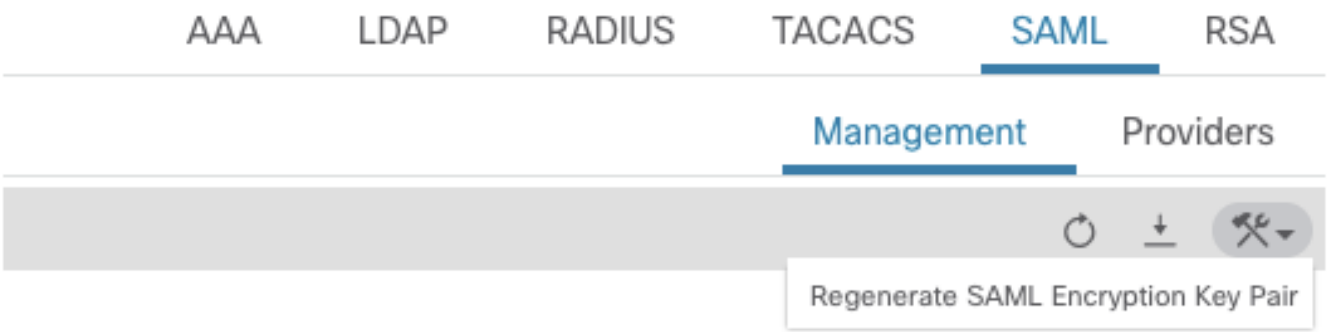


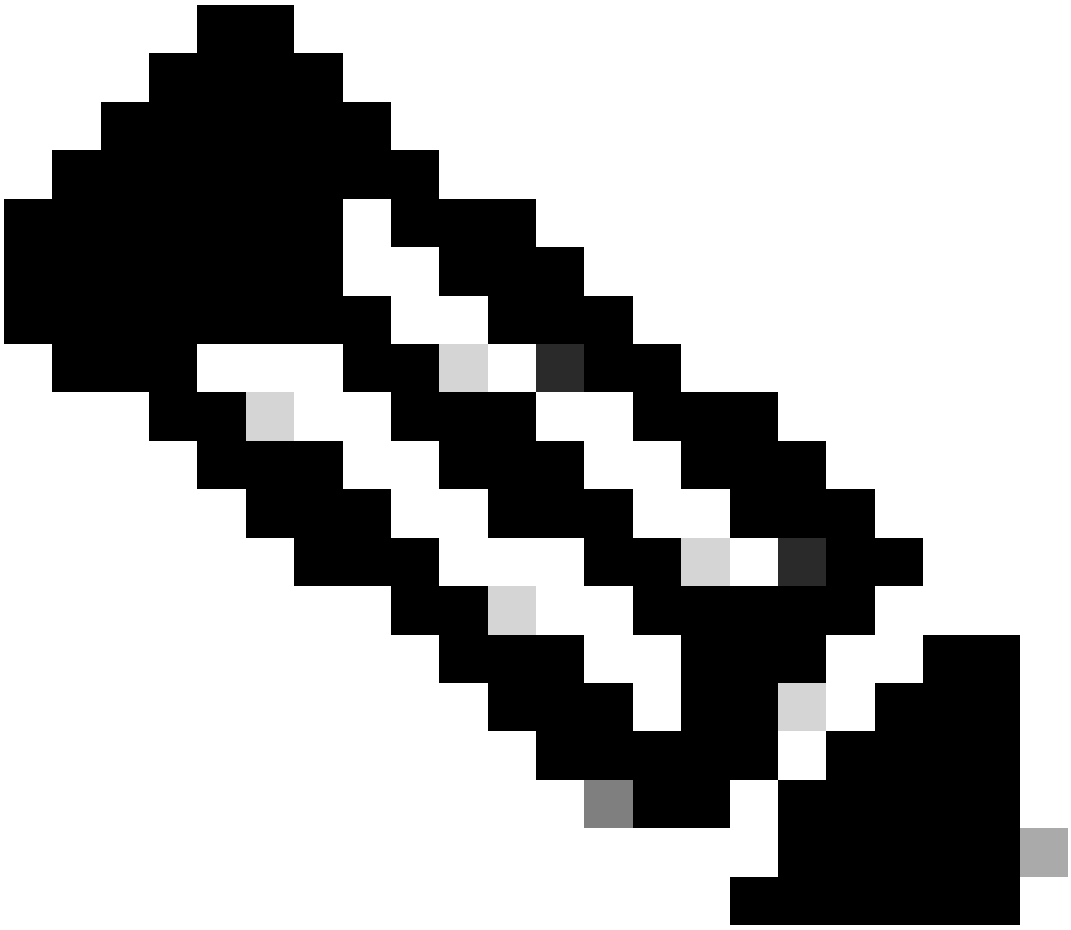
Si le certificat a été émis par une autorité de certification tierce, contactez-la pour renouveler votre certificat SAML X.509.

Toutefois, si l'émetteur du certificat est Cisco, vous pouvez procéder comme suit.

Via l'interface APIC

1. Accédez à Admin > AAA > Authentication > SAML > Management > Regenerate SAML Encryption Key Pair.



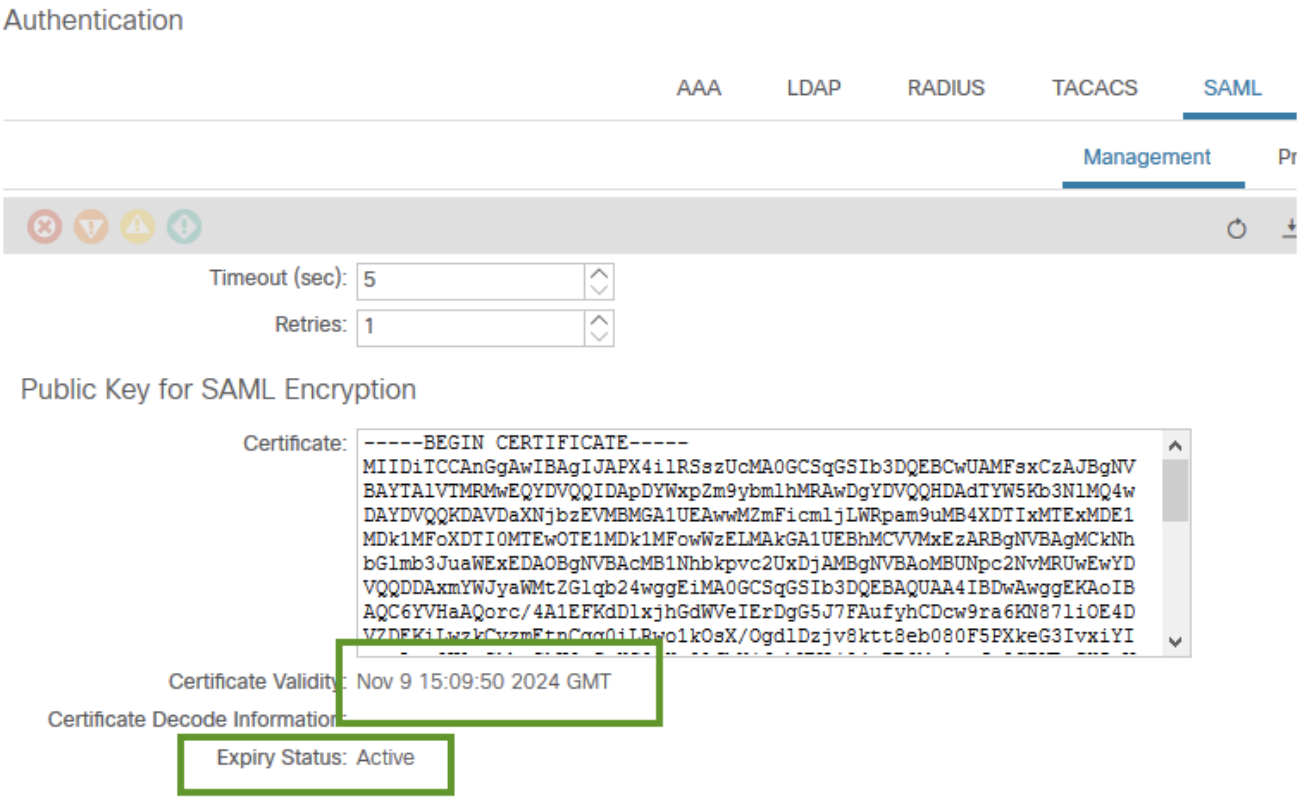


Remarque : en renouvelant le certificat, la date d'expiration affichée dans le champ Validité du certificat est prolongée jusqu'à une date postérieure de trois ans à la date de renouvellement.

Valider si l'état d'expiration passe à Actif

Via l'interface graphique APIC

1. Accédez à Admin > AAA > Authentication > SAML > Management.



Additional Information

SAML est un format de données standard ouvert basé sur XML qui permet aux administrateurs d'accéder à un ensemble défini d'applications de collaboration Cisco de manière transparente après s'être connectés à l'une de ces applications. SAML décrit l'échange d'informations relatives à la sécurité entre des partenaires commerciaux de confiance. Il s'agit d'un protocole d'authentification utilisé par les fournisseurs de services pour authentifier un utilisateur. SAML permet l'échange d'informations d'authentification de sécurité entre un fournisseur d'identité (IdP) et un fournisseur de services.

L'authentification unique SAML utilise le protocole SAML 2.0 afin de proposer l'authentification unique interdomaine et interproduit pour les solutions de collaboration Cisco. SAML 2.0 active l'authentification unique sur toutes les applications Cisco et permet la fédération entre les applications Cisco et un fournisseur d'identité. SAML 2.0 permet également aux utilisateurs administratifs Cisco d'accéder à des domaines Web sécurisés afin d'échanger des données d'authentification et d'autorisation des utilisateurs, entre un fournisseur d'identité et un fournisseur de services, tout en maintenant des niveaux de sécurité élevés. Cette fonctionnalité fournit des mécanismes sécurisés permettant d'utiliser des informations d'identification et des informations pertinentes communes sur diverses applications.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.