Risolvi codice errore ACI F3081: certificato SAML in scadenza

Sommario

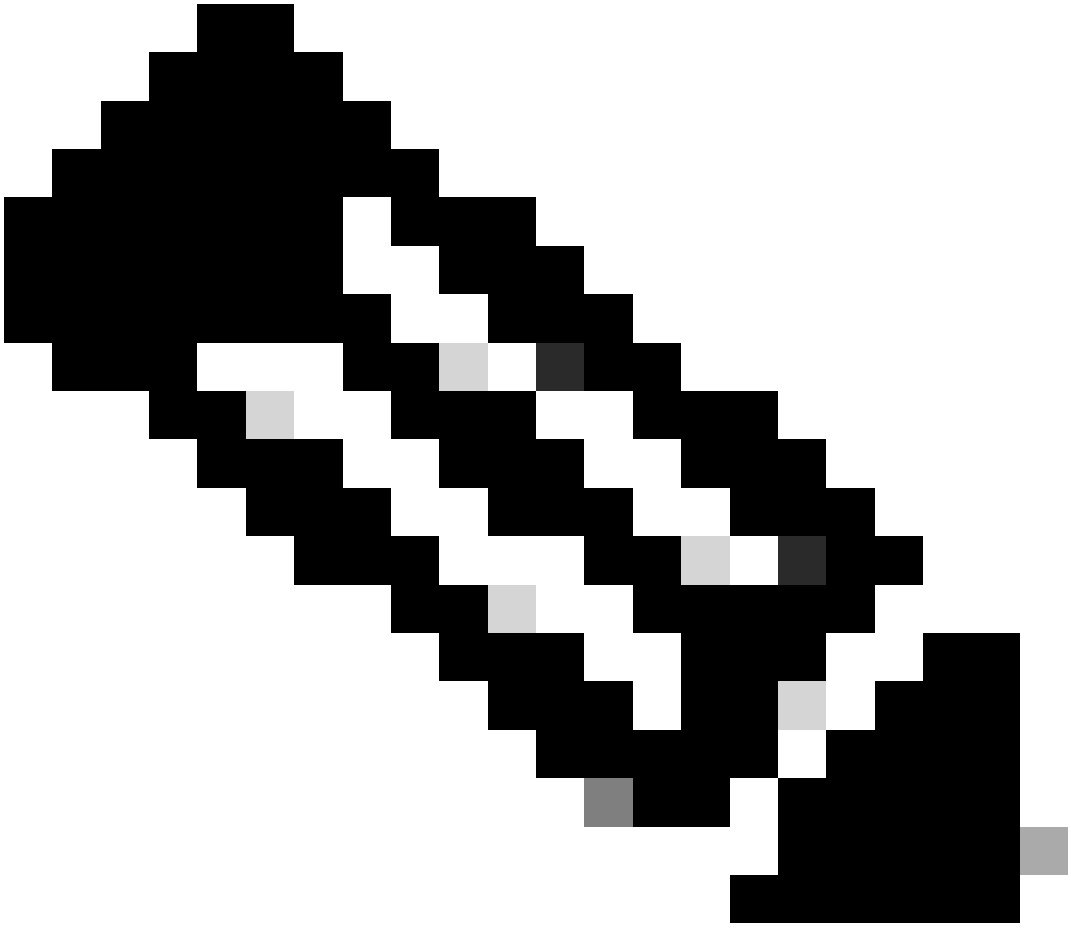
Introduzione

In questo documento viene descritto l'errore ACI F3081 e le relative procedure di correzione.

Premesse

Questo errore si verifica quando un certificato SAML X.509 scadrà tra un mese su 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 stessa occorrenza può verificarsi anche senza implementazione SAML. Tuttavia, se il SAML non viene utilizzato, non ha alcun impatto sul sistema.

Intersight Connected ACI Fabric

Questo guasto viene monitorato attivamente come parte degli accordi ACI proattivi.

Se si dispone di un'infrastruttura ACI connessa a Intersight, viene generata una richiesta di assistenza per conto dell'utente per indicare che sono state trovate istanze di questo errore nell'infrastruttura ACI connessa a Intersight.

Avvio rapido per risolvere gli errori

1. Convalida dello stato di scadenza del certificato SAML X.509. Se viene visualizzato Scadenza o Errore scaduto, viene generato F3081.

2. Verificare se l'autorità di certificazione è Cisco o di terze parti.

3. Se l'autorità emittente è Cisco, continuare con la rigenerazione della coppia di chiavi di crittografia SAML.

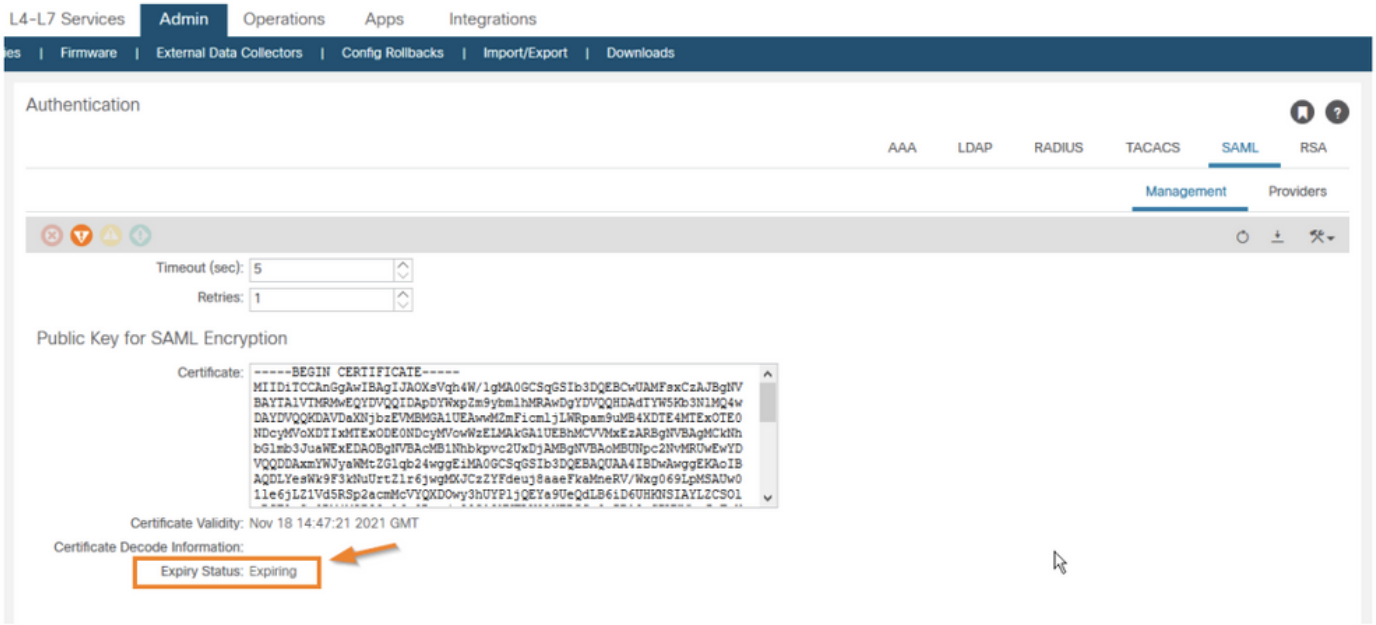
Passi dettagliati per la risoluzione degli errori

Convalida stato scadenza certificato SAML X.509

Tramite interfaccia grafica APIC

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

2. Convalida lo stato di scadenza del certificato SAML X.509. Expiring indica che il certificato sta per scadere entro un mese.



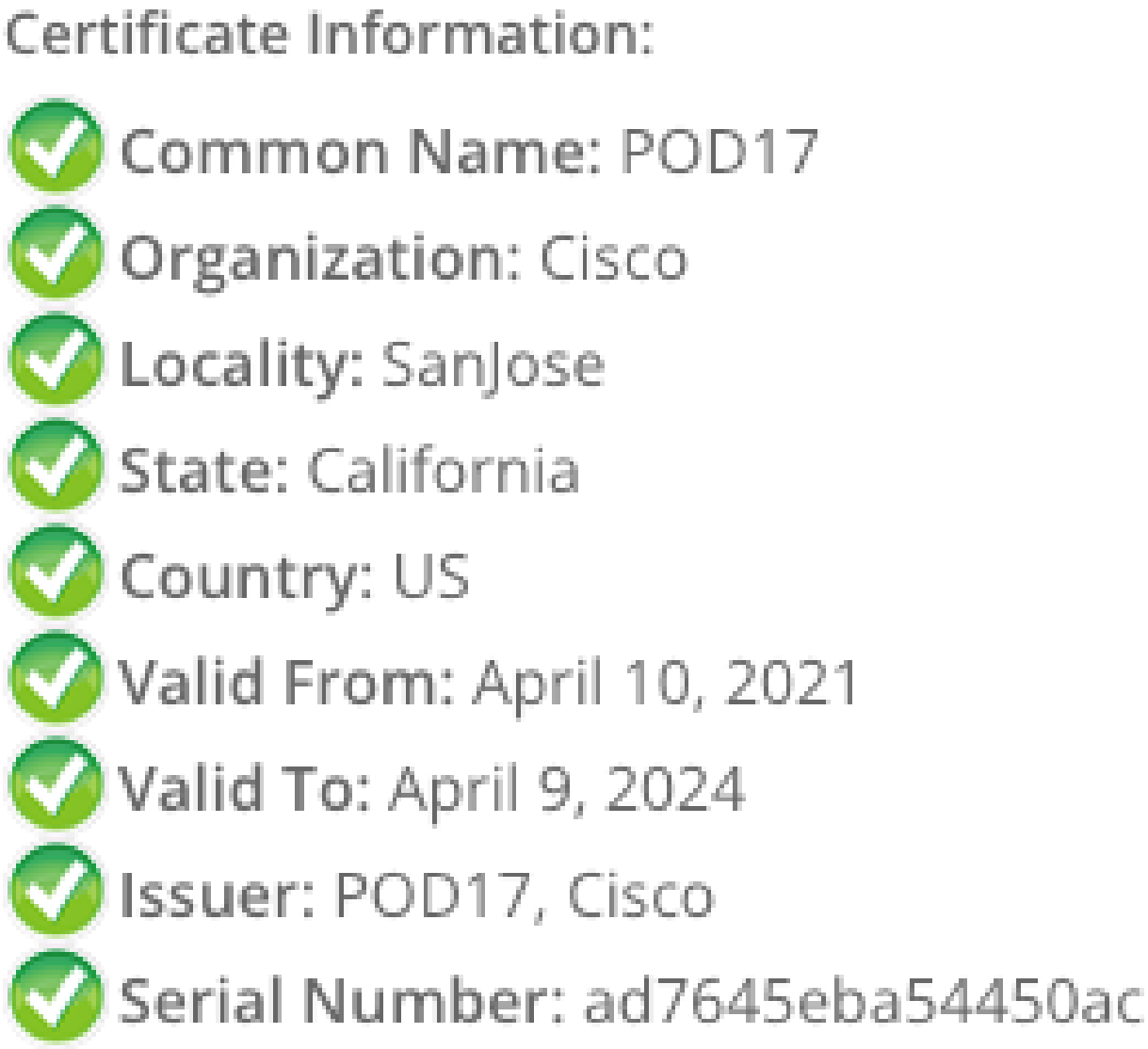
Rigenera e rinnova certificato SAML X.509

Per risolvere il problema, è possibile cancellarlo rigenerando e rinnovando il certificato ed estendendone la data di scadenza.

La rigenerazione del certificato SAML X.509 non ha alcun impatto.

Prima di procedere, verificare che l'autorità di certificazione (CA) emittente del certificato sia Cisco o un'entità di terze parti.

Per ottenere il contenuto del certificato da APIC, decodificare il certificato in qualsiasi decodificatore X.509 per ottenere i parametri del certificato:

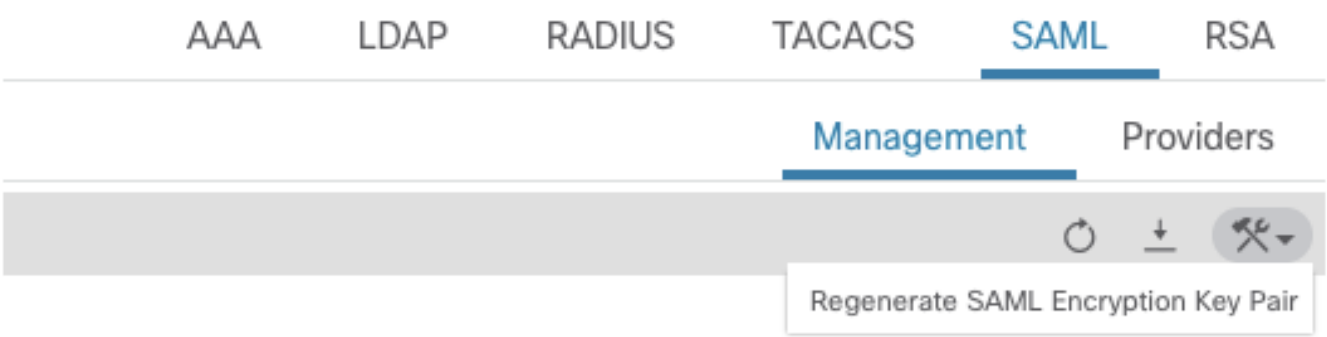


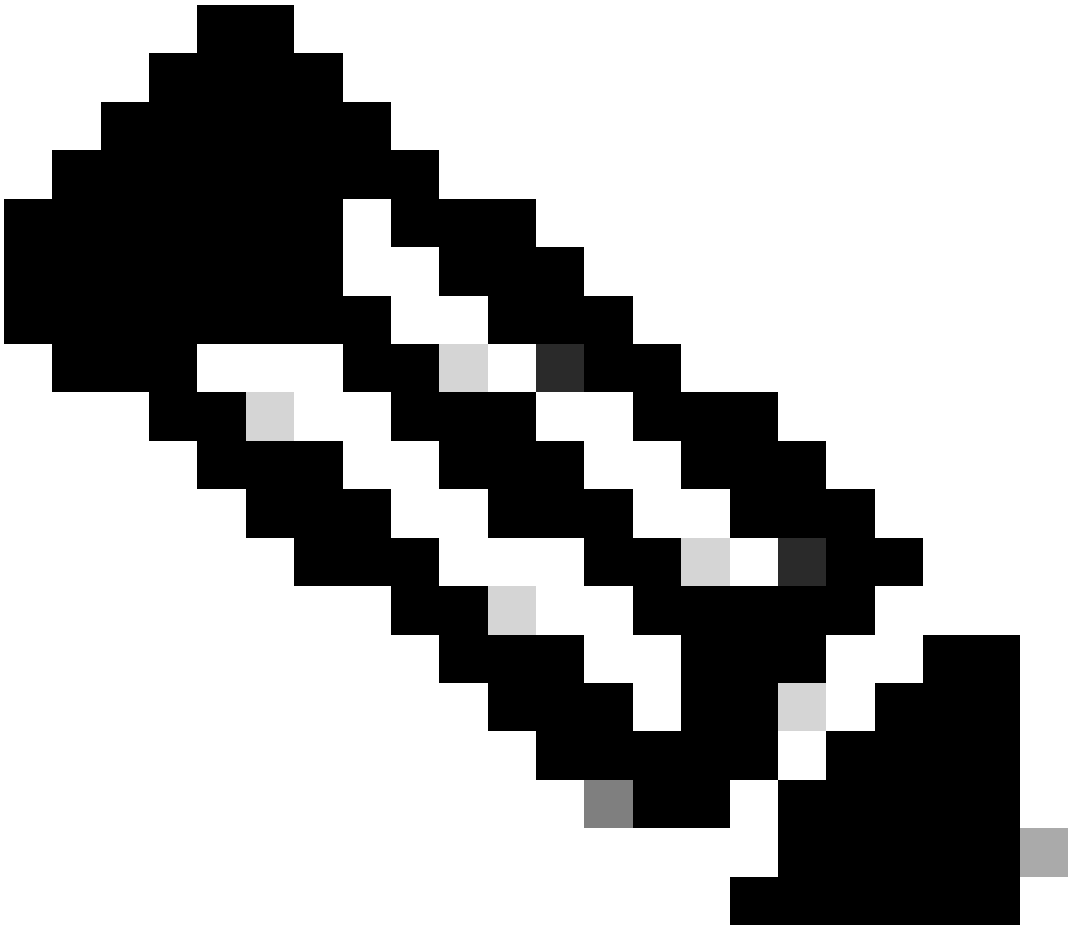
Se il certificato è stato rilasciato da un'autorità di certificazione di terze parti, contattare l'autorità di certificazione per rinnovare il certificato SAML X.509.

Tuttavia, se l'autorità di certificazione è Cisco, è possibile procedere come segue.

Tramite GUI APIC

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



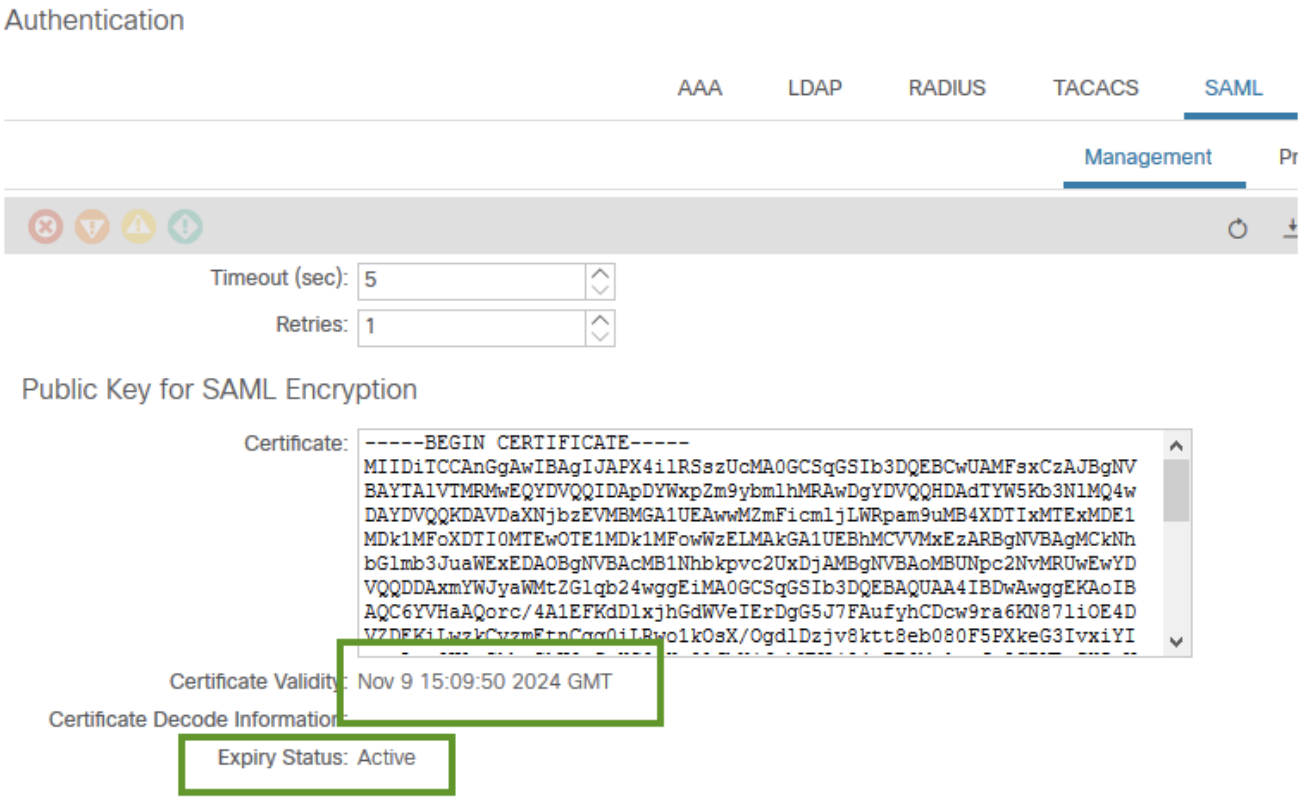


Nota: se si rinnova il certificato, la data di scadenza visualizzata nel campo Validità certificato viene estesa a tre anni dopo la data di rinnovo.

Convalida se lo stato della scadenza è impostato su Attivo

Tramite interfaccia grafica APIC

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



Ulteriori informazioni

SAML è un formato di dati standard aperto basato su XML che consente agli amministratori di accedere senza problemi a un set definito di applicazioni di collaborazione Cisco dopo aver eseguito l'accesso a una di tali applicazioni. SAML descrive lo scambio di informazioni relative alla sicurezza tra partner commerciali di fiducia. È un protocollo di autenticazione utilizzato dai provider di servizi per autenticare un utente. SAML consente lo scambio di informazioni di autenticazione di protezione tra un provider di identità (IdP) e un provider di servizi.

SAML SSO utilizza il protocollo SAML 2.0 per offrire l'SSO tra domini e prodotti per le soluzioni di collaborazione Cisco. SAML 2.0 consente l'SSO tra le applicazioni Cisco e la federazione tra le applicazioni Cisco e un IdP. SAML 2.0 consente inoltre agli utenti amministrativi Cisco di accedere a domini Web sicuri per scambiare dati di autenticazione e autorizzazione tra un IdP e un provider di servizi, mantenendo al contempo livelli di sicurezza elevati. Questa funzionalità fornisce meccanismi sicuri per l'utilizzo di credenziali comuni e informazioni rilevanti in diverse applicazioni.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).