Risoluzione dei problemi relativi ai messaggi di errore in Unity Connection in Serviceability

Sommario

Introduzione

Questo documento descrive come risolvere i problemi relativi a un messaggio di errore comune di Cisco Unity Connection nella pagina relativa alla disponibilità dei servizi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unity Connection (CUC)
- Gestione certificati per server unificati

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si installa un nuovo nodo in Cisco Unity Connection, è necessario assegnare un utente e una password. L'utente viene creato e archiviato nel database Cisco Unity.

Questo errore viene visualizzato per motivi diversi e rende impossibile l'utilizzo della pagina di disponibilità.

Fasi della risoluzione dei problemi

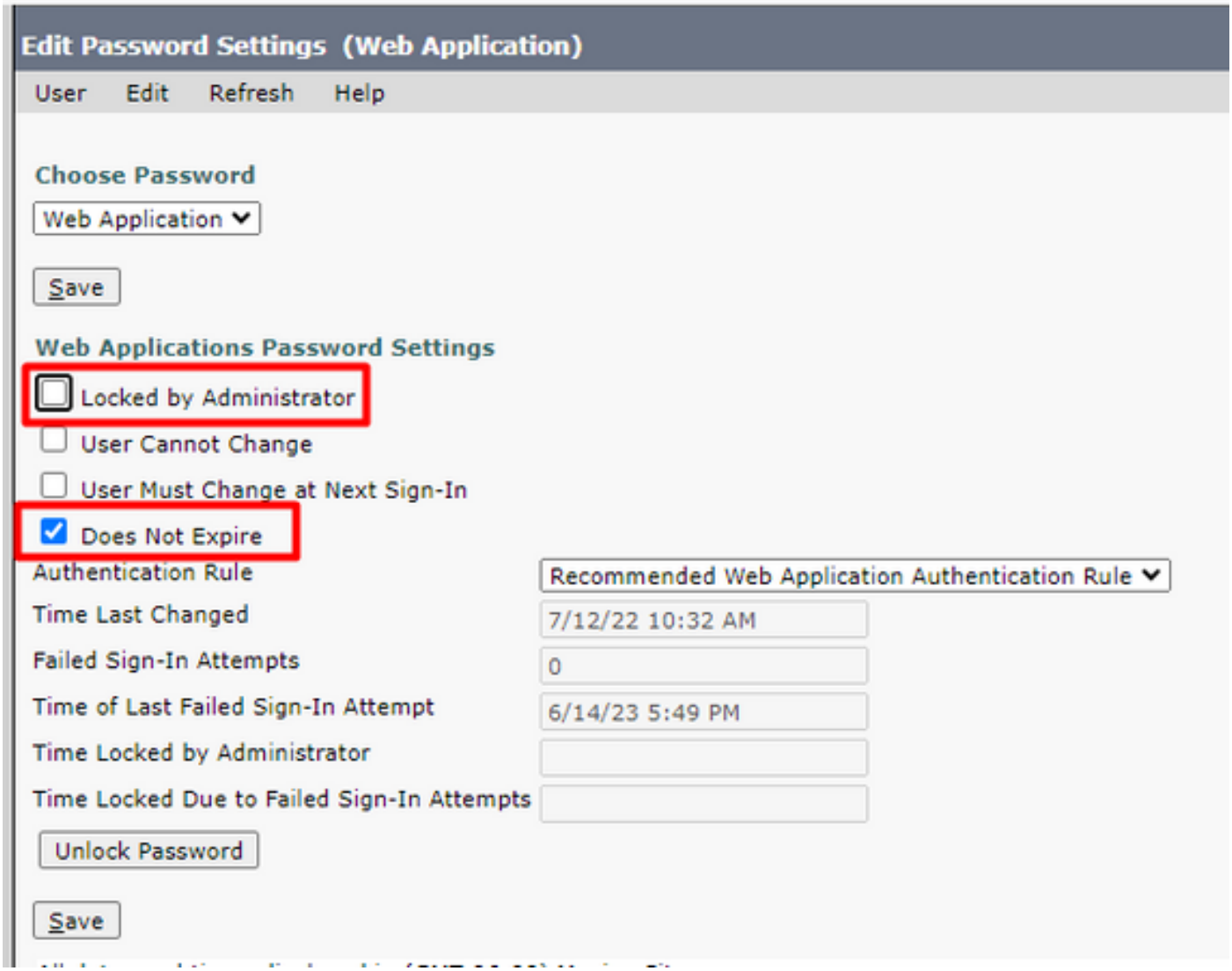
Per iniziare la risoluzione del problema, è necessario innanzitutto rivolgersi all'utente amministratore creato al momento dell'installazione di Unity:

Processo 1

Passare a Amministrazione di Cisco Unity Connection > Vai > Utenti > Seleziona utente di amministrazione > Modifica > Impostazioni password

Deselezionare la casella di controllo Bloccato dall'amministratore per sbloccare l'account utente.

Per evitare che la password scada, selezionare la casella di controllo Non scade.



Fare clic su Sblocca password > Salva.

Passare alla pagina Disponibilità dei servizi di Cisco Unity Connection.

Processo 2

Se il problema può ancora essere replicato:

Passare a Amministrazione di Cisco Unity Connection > Vai > Utenti > Selezionare l'utente amministratore > Modifica > Modifica password e immettere una nuova password.

Passare alla pagina Disponibilità dei servizi di Cisco Unity Connection e verificare se è possibile accedervi.

Processo 3

Se il problema persiste:

Passare a Cisco Unified OS Administration > Go > Security > Certificate Management (Amministrazione del sistema operativo unificato Cisco > Vai > Sicurezza > Gestione certificati) e

verificare se i certificati Ipsec e Tomcat non sono scaduti.

Se i certificati sono scaduti, è necessario rigenerarli.

Processo di rigenerazione:

- Autofirmato:processo di rigenerazione dei certificati autofirmati
- CA -signed: processo di rigenerazione certificati firmati da CA

Processo 4

Se i certificati sono firmati dalla CA, è necessario verificare se Cisco Unity Connection non corrisponde all'ID bug Cisco CSCvp31528.

Nel caso in cui Unity corrisponda, procedere come segue:

Soluzione 1

Chiedere alla CA di firmare il certificato del server senza l'estensione critica del nome alternativo del soggetto X509v3 e lasciare invariate le altre estensioni.

Soluzione 2

Chiedere all'autorità di certificazione di firmare il certificato del server e di aggiungere l'estensione specificata in seguito per consentirne il corretto funzionamento.
Vincoli di base X509v3: critici

Soluzione 3

Utilizzare i certificati autofirmati, non è sempre la soluzione giusta per tutti.

Soluzione 4

Come ultima soluzione disponibile, eseguire l'aggiornamento a una release che contiene la correzione del difetto e generare la CSR su una release fissa e ottenerla firmata da CA come è noto con il processo normale.

Processo 5

Dalla CLI CUC:

1. Recuperare l'objectID dell'utente amministratore applicazione predefinito dal database Unity Connection.

```
run cuc dbquery unitydirdb select name, value from vw_configuration where name='DefaultAdministrator'
```

Output comando:

```
name                  value
--------------------  -------------------------------------
DefaultAdministrator  XXXX-XXXX-XXXXX-XXXX
```

2. Recuperare l'alias associato all'objectID predefinito dell'amministratore dell'applicazione. Nella query sostituire il campo objectid='XXXX-XXXX-XXXXX-XXXX' con il valore dell'output precedente.

```
run cuc dbquery unitydirdb select alias,objectid from vw_user where objectid='XXXX-XXXX-XXXXX-XXXX'
```

Output comando:

```
alias    objectid
-----  -------------------------------------
admin  XXXX-XXXX-XXXXX-XXXX
```

3. Confermare che il tipo di crittografia sia 4 per l'autenticazione Web per l'utente amministratore applicazione predefinito (il tipo di credenziali 3 è per la password dell'applicazione Web).

```
run cuc dbquery unitydirdb select objectid, userobjectid, credentialtype, encryptiontype from tbl_crede
```

Output comando:

```
objectid                              userobjectid                         credentialtype encryptionty
------------------------------------  ------------------------------------ -------------- ------------
ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ                 XXXX-XXXX-XXXXX-XXXX                          3              4
TTTTT-TTTTT-TTTTT-TTTTT                 XXXX-XXXX-XXXXX-XXXX                          4              3
```

Se il tipo di crittografia è = 3, passare a 4.

```
run cuc dbquery unitydirdb update tbl_credential set encryptiontype = "4" where objectid = "ZZZZZ-ZZZZZ
```

5. È necessario modificare la password perché l'utente è stato crittografato con la vecchia password di tipo 3

```
utils cuc reset password <accountalias>
```

6. Riavviare Tomcat tramite CLI

```
utils service restart Cisco Tomcat
```

Verificare se la pagina dei servizi è accessibile.

Se il problema persiste, raccogliere i log Tomcat CUC da RTMT.

A tale scopo:

1. Aprire RTMT.

2. Inserire IP/nome host Cisco Unity Connection.

3. Inserire utente e password.

4. Fare doppio clic su Raccogli file. Viene visualizzata la finestra Raccogli file in cui è possibile selezionare Servizi/applicazioni UCM.

5. In Seleziona servizi/applicazioni UCM fare clic sulla casella di controllo nella colonna Tutti i server per:

- Cisco Tomcat

Informazioni correlate

- Supporto tecnico e download Cisco

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).