

Risoluzione dei problemi visualizzati nei log Jabber

Sommario

[Introduzione](#)

[Premesse](#)

[Come recuperare i log](#)

[Parole chiave per effettuare le ricerche nei log](#)

[Fasi della risoluzione dei problemi](#)

[Fase 1. Individuazione servizio CUCM](#)

[Fase 2. Autenticazione utente CUCM](#)

[Fase 3. Accesso SOAP \(IM e presenza\)](#)

[Fase 4. Log in XMPP \(IM e presenza Log in\)](#)

[Controlli obbligatori](#)

[Come impostare i log su DEBUG](#)

[Log da recuperare](#)

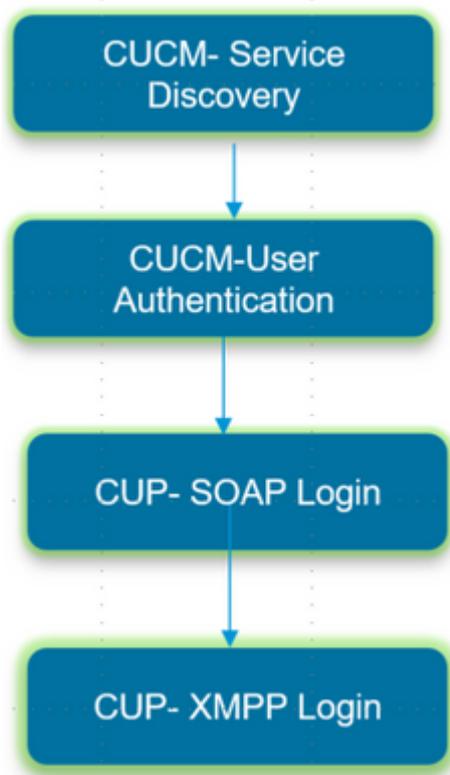
[Recupero dei log da RTMT](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi all'accesso di Jabber in caso di errore su una rete interna o aziendale.

Premesse

Jabber Log in si compone di due fasi: il server Cisco Unified Communications Manager (CUCM) Log in e il server IM e Presence (IM&P) Log in.



- L'accesso a CUCM implica l'individuazione del servizio per identificare il server CUCM a cui Jabber deve accedere.
- Jabber utilizza l'autenticazione con CUCM per recuperare i dettagli del profilo del servizio che contiene i dettagli del server IMP, di Voicemail, di Conferencing, del server CTI e il file di configurazione del dispositivo per i servizi telefonici.
- Una volta completato il login a CUCM, Jabber accede al server IMP per autenticare e recuperare l'elenco dei contatti e altri servizi di messaggistica istantanea.
- Il Log in IMP prevede due fasi: il Log SOAP in cui viene trattata l'autenticazione dell'utente e il Log XMPP in cui vengono trattate la creazione di sessioni XMPP e la gestione dei flussi.

Come recuperare i log

Cancellare la cache sul PC e raccogliere la parte clean Jabber Problem Report (PRT).

Passaggio 1. Disconnettersi e uscire dall'applicazione Jabber.

Passaggio 2. Elimina tutti i registri disponibili in

```
%AppData%\Local\Cisco\Unified Communications\Jabber\  
%AppData%\Roaming\Cisco\Unified Communications\Jabber\  

```

Passaggio 3. Riavviare Jabber e ricreare il problema.

Passaggio 4. Raccogliere il Report di problema. (Dal **menu Guida di Jabber**, selezionare **Segnala un problema** per avviare lo strumento Report di problema. Le istruzioni sono disponibili qui)

Collega a queste risorse:

- [Come raccogliere un problema Jabber](#)

- [Come richiamare i log da Expressway \(quando si usa MRA\)](#)

Parole chiave per effettuare le ricerche nei log

<#root>

```
IMPStackCap::Log in::OnLog inError
ServiceDiscoveryHandlerResult
@CupSoapCli: log in cup succeeds -
```

shows when the SOAP log in was successful.

```
[CTriTPConnectionClient::OnConnectSuccess] - @XmppSDK: -
```

shows when the XMPP log in was successful.

LERR -

shows the Log in Errors when the Jabber fails to log in to the IM&P Server.

Fasi della risoluzione dei problemi

Fase 1. Individuazione servizio CUCM

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot find your services automatically. Click advanced settings to set up manually (Impossibile trovare i servizi automaticamente. Fare clic sulle impostazioni avanzate per configurarle manualmente.)	Questo errore viene visualizzato quando _cisco-uds o _cuplog nei record SRV non è configurato nel server DNS	csf::dns::mapFromWindowsDNSResult

Esempio di frammento di codice nel log

<#root>

```
017-03-19 17:55:00,422 WARN [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns] [csf::dns::mapFromWindowsDNSResult] - *-----*
```

```
DNS query _cisco-uds._tcp.applab has failed
```

```
:
```

```
DNS name does not exist. (9003).
```

```
2017-03-19 17:55:00,438 WARN [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns] [csf::
```

```
DNS query _cuplogin._tcp.applab has failed
```

```
: DNS name does not exist. (9003).
```

Procedura di risoluzione

Passaggio 1. Avviare il prompt dei comandi (in un client Windows) e quindi immettere **nslookup**.

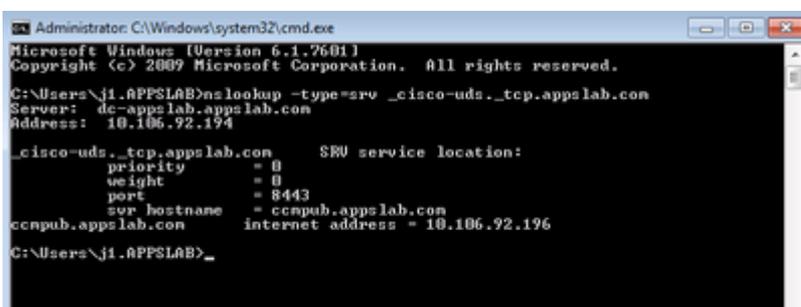
Passaggio 2. Imposta il tipo di query su SRV
set type = SRV

Passaggio 3. Inserire il record SRV da controllare
_cisco-uds._tcp.example.com

Passaggio 4. In questo modo vengono restituiti i record A DNS che puntano ai server CUCM.

Questo è un esempio di record SRV _cisco-uds restituito.

Se non viene restituito alcun record, contattare l'amministratore DNS per configurare i [record SRV](#)



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\jl.APPSLAB>nslookup -type=srv _cisco-uds._tcp.appslab.com
Server: dc-appslab.appslab.com
Address: 10.106.92.194

_cisco-uds._tcp.appslab.com    SRV service location:
        priority      = 0
        weight        = 0
        port          = 8443
        svr hostname  = ccmpub.appslab.com
ccmpub.appslab.com            internet address = 10.106.92.196

C:\Users\jl.APPSLAB>
```

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot find your services automatically. Click advanced settings to set up manually (Impossibile trovare i servizi automaticamente. Fare clic sulle impostazioni avanzate per configurarle manualmente.)	Questo errore si verifica quando Jabber non riesce a recuperare i server UDS o TFTP per raccogliere le informazioni di accesso e le impostazioni di configurazione.	HTTP response code 503 for request #29 to https://cucm.domain:8443/cucm-uds/ HTTP response code 503 for request #29 to https://cucm.domain:6972/

Procedura di risoluzione

Passaggio 1. Verificare che i nodi CUCM configurati come server TFTP siano attivi e in esecuzione.

Passaggio 2. **Riavviare** i servizi su tutti i nodi CUCM.

- Cisco TFTP
- Cisco UDS Service

Fase 2. Autenticazione utente CUCM

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Your username or password is not correct (Il nome	Questo errore viene visualizzato quando le credenziali immesse	"FAILED_UCM90_AUTHENTICATION"

utente o la password immessi non sono corretti)	sono errate o l'utente è bloccato in CUCM/LDAP	
---	--	--

Esempio di frammento di codice nel log

<#root>

2017-01-09 08:59:10,652 INFO [0x00001740] [vices\impl\DiscoveryHandlerImpl.cpp(460)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::ev

FAILED_UCM90_AUTHENTICATION

Procedura di risoluzione

Passaggio 1. Verificare che l'utente sia configurato come **utente finale** in CUCM. Passare alla pagina **Amministrazione CUCM > Utente finale**.

Passaggio 2. Verificare che le credenziali siano corrette e che l'utente sia attivo. Accedere al portale di auto-assistenza CUCM.

Questa immagine fa riferimento allo scenario in cui l'utente non può essere autenticato tramite il protocollo LDAP perché non è un utente valido oppure perché la password fornita non è corretta.



Passaggio 3. Se il problema si verifica per tutti gli utenti, verificare che le impostazioni di sincronizzazione LDAP e autenticazione LDAP in **Amministrazione CUCM > Sistema > LDAP** siano corrette.

Suggerimento: dal punto di vista del server LDAP, assicurarsi che l'**account non sia bloccato**, che le **password non siano scadute** e che tutti **gli utenti siano sincronizzati con il server CUCM**.

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot communicate with the server (Impossibile comunicare con il server)	Jabber non riesce a risolvere il nome di dominio completo/il nome host di CUCM ricevuto durante la fase di rilevamento del servizio	"FAILED_UCM90_CONNECTION"

Esempio di frammento di codice nel log

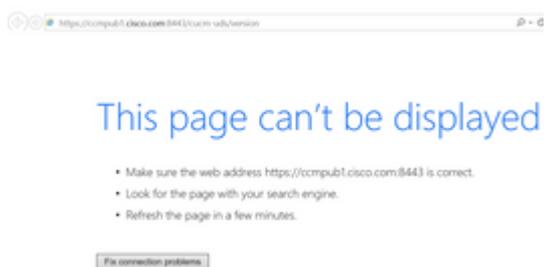
```
<#root>
```

```
2017-08-28 12:04:00,282 INFO [0x00004290] [vices\impl\DiscoveryHandlerImpl.cpp(452)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::ev  
FAILED_UCM90_CONNECTION
```

Procedura di risoluzione

Passaggio 1. Verificare se è possibile aprire questo URL nel browser del PC <https://<CUCM IP/FQDN>:8443/cucm-uds/version>

Operazione non riuscita



Operazione riuscita



Passaggio 2. Se la risposta non ha esito positivo, verificare che il DNS sia configurato correttamente per risolverli e anche se nessun elemento di rete come Firewall/ASA blocca la porta 8443.

Passaggio 3. Questo URL deve essere testato per tutti i server CUCM nel cluster. Per un elenco dei server, selezionare **Amministrazione CUCM > Sistema > Server**.

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot communicate with the server (Impossibile comunicare con il server)	Questo errore viene visualizzato quando l'ID utente immesso in Jabber non corrisponde all'ID utente configurato in CUCM	"FAILED_USER_LOOKUP"

Esempio di frammento di codice nel log

<#root>

2016-08-18 13:14:49,943 INFO [0x000036e4] [vices\impl\DiscoveryHandlerImpl.cpp(367)] [service-discovery] [DiscoveryHandlerImpl::evaluateService

FAILED_USER_LOOKUP

Procedura di risoluzione

Passaggio 1. Verificare che sia possibile aprire questo URL nel browser del PC <https://CUCM:8443/cucm-uds/clusterUser?username=<userid>>.

Passaggio 2. Verificare che l'ID utente immesso in Jabber corrisponda all'ID utente nella pagina Utente finale CUCM.

Suggerimento: per impostazione predefinita, Jabber ha abilitato l'individuazione UPN e quindi ottiene l'**ID utente** precompilato dal campo UPN LDAP. Verificare se UPN è uguale a quello configurato in CUCM, se è necessario disabilitare l'individuazione UPN, **impostare** UPN_DISCOVERY_ENABLED=false durante [l'installazione](#)

Fase 3. Accesso SOAP (IM e presenza)

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Your username or password is not correct (Il nome utente o la password immessi non sono corretti)	Questo errore è causato da un errore di autenticazione dell'utente	"LERR_CUP_AUTH"

Esempio di frammento di codice nel log

<#root>

2017-01-14 15:55:09,615 INFO [0x00000dc0] [ts\adapters\imp\components\Login.cpp(99)] [imp.service] [IMPStackCap::Login::OnLoginError] - *****

2017-01-14 15:55:09,615 INFO [0x00000dc0] [s\adapters\imp\components\Login.cpp(100)] [imp.service] [IMPStackCap::Login::OnLoginError] - OnLog

LERR_CUP_AUTH <12>:

2017-01-14 15:55:09,615 INFO [0x00000dc0] [s\adapters\imp\components\Login.cpp(101)] [imp.service] [IMP

Procedura di risoluzione

Passaggio 1. Verificare che l'utente sia assegnato a un nodo Presenza e che non vi siano duplicati per l'utente (**IM e presenza Amministrazione > Diagnostica > Risoluzione dei problemi di sistema**).

Passaggio 2. Verificare che lo stato Alta disponibilità (HA) sia Normale e che non si sia verificato alcun failover.

Se si è tentato di assegnare l'utente durante uno stato HA anomalo, gli utenti non vengono assegnati ad alcun nodo IMP e l'accesso non riesce.

Ripristinare prima lo stato HA e riassegnare l'utente.

Passaggio 3. Verificare che le credenziali siano valide.

1. Nel caso di un utente LDAP, verificare se l'utente è in grado di accedere al portale CUCM Selfcare.
2. Se l'accesso alla pagina **ccmenduser** non riesce, controllare le impostazioni di autenticazione LDAP in CUCM e verificare che le stesse impostazioni vengano replicate in IMP

```
run sql select * from ldapauthentication
run sql select * from ldapauthenticationhost
```

3. Verificare che l'account non sia bloccato in LDAP
4. Se l'utente è stato abilitato recentemente per Presence, riavviare il servizio Cisco Sync Agent in IMP Publisher.

Passaggio 4. Verificare che il server utilizzi CPU TOMCAT in modo elevato

- **show process load**
- **utils diagnose test**

Passaggio 5. Impostare il log di questi servizi su DEBUG, quindi ricreare il problema di accesso e raccogliere i log

- Client Profile Agent
- Cisco Tomcat
- Event Viewer-Log delle applicazioni
- Event Viewer-Log di sistema

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Invalid Credentials (Credenziali non valide)	Questo errore si verifica quando l'utente non è attivo o non è presente nel database.	LERR_CUP_AUTH <10>

Esempio di frammento di codice nel log

```
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - *****
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - OnLog inError: LERR_CUP_AUTH <10>:
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - *****
[http-bio-443-exec-15] handlers.Log inHandlerAbstract - preLog in:PRELOGIN reasoncode=FAILURE. User eith
```

Suggerimento: per questo errore, si consiglia anche di recuperare i log di Cisco Tomcat dai server CUCM e IM&P.

Dai log di Cisco Tomcat:

<#root>

```
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : inside check wit
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.Certificates - getCNs :
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : cns = [ldap.cisco
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.Certificates - getDNSSubjectAlts :
2019-10-27 18:33:40,374 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : subjectAlts = [
2019-10-27 18:33:40,374 ERROR [http-bio-443-exec-5] impl.AuthenticationLDAP - verifyHostName:Exception.
2019-10-27 18:33:40,374 DEBUG [http-bio-443-exec-5] impl.AuthenticationLDAP - value of hostnameverified
2019-10-27 18:33:40,374 INFO [http-bio-443-exec-5] impl.AuthenticationLDAP - verifyHostName: Closing LDA
```

Procedura di risoluzione

In questo caso si verificano due situazioni se i log di Cisco Tomcat non mostrano alcun errore di certificato. È necessario eseguire la convalida.

Passaggio 1. Verifica che l'utente sia associato a un server IM&P

- Accedere alla pagina Web **CUCM Administration > User Management > User Management > Assign Presence Users** > (Amministrazione CUCM > Gestione utenti > Gestione utenti > Assegna utenti Presence), cercare l'**ID utente** e fare clic su **Find** (Trova)

Passaggio 2. Se l'utente è associato a un server IM&P, rimuoverlo dal cluster del nodo principale

- Accedere alla pagina Web **CUCM Administration > User Management > End User** (Amministrazione CUCM > Gestione utenti > Utente finale), cercare l'**utente finale** e fare clic su **Find** (Trova). In **Service Settings (Impostazioni di servizio)**, **deselezionare la casella di controllo Home Cluster (Cluster home)** e fare clic su **Save** (Salva), **selezionare la casella di controllo Home Cluster (Cluster home)** e fare clic su **Save** (Salva)

Se i log di Cisco Tomcat mostrano l'errore dello snippet mostrato in precedenza, attenersi alla seguente procedura:

Passaggio 1. Confermare se Cisco Jabber è configurato per l'utilizzo di Secure LDAP

Passaggio 2. Se è in uso Secure LDAP, confermare le informazioni dei certificati ad essi associate, ad esempio il nome di dominio completo (FQDN), il nome host e il nome comune (CN).

Passaggio 3. Convalidare la configurazione di CUCM e IM&P, se con indirizzo IP o FQDN, e confrontarla con le informazioni contenute nel certificato

- Accedere alla pagina Web **CUCM Administration > System > Server (Amministratore CUCM > Sistema > Server)**.

Passaggio 4. Se i server sono configurati con indirizzo IP e i certificati LDAP sono configurati con FQDN, il comando successivo richiede l'esecuzione su tutti i nodi CUCM e IM&P

- **utils ldap config ipaddr**
- Oppure modificare la definizione dei server come nome di dominio completo (FQDN). Fare

riferimento a. [Modificare la definizione del server CUCM da Indirizzo IP o Nome host a Guida FQDN.](#)

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot communicate with the server (Impossibile comunicare con il server)	Questo errore è causato da problemi di connettività IMDB o TCP con IMP	"LERR_CUP_UNREACHABLE", "LERR_CUP_TIMEOUT"

Esempio di frammento di codice nel log

```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
2017-11-08 16:03:20,051 INFO [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLogin
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
```

Procedura di risoluzione

Passaggio 1. Verificare che FQDN/nomi host IMP siano risolvibili dal PC client.

Passaggio 2. Verificare che sia possibile aprire questo URL nel browser **https://<IMP SERVER FQDN/IP>:8443/EPASSoap/service/v105**

Operazione riuscita

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<error>This is a SOAP service. Send a POST request!</error>

Operazione non riuscita



HTTP Status 404 - /EPASSoap/service/v105

type: Status report

message: /EPASSoap/service/v105

description: The requested resource is not available

Passaggio 3. Verificare che il firewall/VPN non blocchi la connettività al server IMP (porta 8443.522)

Passaggio 4. Verifica se il servizio è in esecuzione nel server IMP: Agente profilo client Cisco

Passaggio 5. Impostare il log dei servizi su DEBUG, ricreare il problema di accesso e quindi raccogliere i log se i passaggi precedenti non risolvono il problema.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent

Suggerimento: se il problema persiste per un solo utente, annullare l'assegnazione e riassegnare l'utente per la presenza in CUCM. Se si tratta di un problema a livello di sistema, raccogliere i registri e controllare lo stato dei servizi

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot communicate with the server (Impossibile comunicare con il server)	In genere, questo errore è causato da problemi con l'IMDB	"LERR_CUP_INTERNAL_ERROR"

Esempio di frammento di codice nel log

```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
2017-11-08 16:03:20,051 INFO [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLogin
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
```

Procedura di risoluzione

Passaggio 1. Esegui [controlli obbligatori](#)

Passaggio 2. Verificare che questi servizi siano in esecuzione nel server IM&P

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Cisco Log in Datastore

Passaggio 3. Verifica se la presente informativa sui prodotti è applicabile

Avviso: FN - 64267 - Cisco Unified Communications Manager IM & Presence provoca errori di accesso a Cisco Jabber - Consigliato aggiornamento software

Passaggio 4. Impostare il log dei servizi su DEBUG, ricreare il problema di accesso e quindi raccogliere i log se i passaggi precedenti non risolvono il problema.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Cisco Log in Datastore
- Event Viewer-Log delle applicazioni
- Event Viewer-Log di sistema

Passaggio 5. Riavviare il cluster per ripristinare la situazione.

Fase 4. Log in XMPP (IM e presenza Log in)

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot communicate	Questo errore si verifica in genere	LERR_JABBER_AUTH <14>: errore di

with the server (Impossibile comunicare con il server)	quando Jabber non riesce a connettersi tramite MRA e non riesce a stabilire una sessione TLS con IM&P	autenticazione con il server, ad esempio binding risorse, TLS, creazione sessione o errore SASL
---	---	---

Esempio di frammento di codice nel log

```
2019-05-03 15:19:32,225 DEBUG [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(128)] [IMP Servi
2019-05-03 15:19:32,225 INFO [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(129)] [IMP Servi
2019-05-03 15:19:32,225 DEBUG [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(130)] [IMP Servi
```

Procedura di risoluzione

Passaggio 1. Verificare che la porta 5222 sia aperta tra i server IM&P e Expressways.

Passaggio 2. Verificare che questi servizi siano in esecuzione nel server IM&P e riavviarli una volta.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

Passaggio 3. Disabilitare l'opzione Alta disponibilità dai gruppi di ridondanza di presenza CUCM.

Passaggio 4. Riavviare il **servizio Router Cisco XCP** su tutti i nodi IM&P, prima con l'autore IM&P e quindi nei Sottoscrittori.

- **utils service restart Cisco XCP Router Service**

Passaggio 5. Riattivare l'alta disponibilità dai gruppi di ridondanza di presenza CUCM.

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot communicate with the server (Impossibile comunicare con il server)	Questo errore si verifica in genere quando Jabber non è in grado di creare una sessione e di associarsi al server IMP	LERR_JABBER_AUTH <17>: errore di autenticazione con il server, ad esempio binding risorse, TLS, creazione sessione o errore SASL"

Esempio di frammento di codice nel log

```
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(127)] [IMP Services] [OnLoginError] - *****
2017-10-27 10:56:47,396 INFO [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(128)] [IMP Services] [OnLoginError] - OnLoginError: LE
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(129)] [IMP Services] [OnLoginError] - *****
```

Procedura di risoluzione

Passaggio 1. Verificare che i certificati cup-xmpp siano validi.

Passaggio 2. Verificare che la porta 522 sia aperta.

Passaggio 3. Impostare il log dei servizi su DEBUG, quindi ricreare il problema di accesso e raccogliere i log prima del passaggio 4.

Se la causa principale da identificare come Riavvio del server è l'unica correzione nota.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Log delle applicazioni
- Event Viewer-Log di sistema

Passaggio 4. Riavviare il server per risolvere il problema.

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot communicate with the server (Impossibile comunicare con il server)	Questo errore viene visualizzato quando IMP non è risolvibile o raggiungibile a causa di problemi di rete, ad esempio la presenza di un firewall	"LERR_JABBER_UNREACHABLE "

Esempio di frammento di codice nel log

```
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components>Login.cpp(96)] [imp.service] [IMPStackCap::Login::OnLoginError] - *****
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components>Login.cpp(97)] [imp.service] [IMPStackCap::Login::OnLoginError] - OnLog
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components>Login.cpp(98)] [imp.service] [IMPStackCap::Login::OnLoginError] - *****
```

Procedura di risoluzione

Passaggio 1. Verificare se il nome di dominio completo (FQDN)/i nomi host dell'IMP sono risolvibili.

Passaggio 2. Verificare che il firewall/VPN non blocchi la connettività al server IM&P (porta 8443.522).

Passaggio 3. Verificare che questi servizi siano in esecuzione nel server IM&P e riavviarli una volta.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

Passaggio 4. Eseguire [i controlli obbligatori](#).

Passaggio 5. Impostare il log dei servizi su DEBUG, ricreare il problema di accesso e quindi raccogliere i log se i passaggi precedenti non risolvono il problema.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Log delle applicazioni
- Event Viewer-Log di sistema

Passaggio 6. Se tutti gli utenti riscontrano lo stesso errore, è possibile riavviare il server per un ripristino rapido.

Messaggio visualizzato	Causa	Cosa cercare nel log Jabber
Cannot Sign in your account. Contact your administrator. (Impossibile accedere all'account. Contatta l'amministratore.)	Generalmente visualizzato quando Jabber esegue il login con SSO, in locale o tramite Expressways (Mobile Remote Access (MRA))	"Log inError to ErrorCode: 27 mappato a: UnknownLog inError "

Esempio di frammento di codice nel log

```
2020-03-12 19:55:01,283 DEBUG [0x000000010b71d800][apters/imp/components/Log inUtils.cpp(96)][IMPService
2020-03-12 19:55:01,283 DEBUG [0x000000010b71d800][listeners/Log inEventListenerImpl.cpp(148)][IMPService
2020-03-12 19:55:01,283 INFO [0x000000016b61f000][ers/imp/lifecycle/Log inExecutor.cpp(314)][IMPService
2020-03-12 19:55:01,478 INFO [0x000000010b71d800][pp/tahtiti/ui/log in/YLCLog inBaseVC.m(500)][UI.Action.
```

Procedura di risoluzione

Passaggio 1. Convalida che l'utente è assegnato a IM&P.

Passaggio 2. Verificare che i certificati siano scambiati correttamente tra i nodi e Jabber.

Passaggio 3. Verificare che le chiavi di firma e crittografia OAuth siano configurate correttamente in tutti i nodi. [Vedere la sezione Verifica di questo documento.](#)

Passaggio 4. Eseguire [i controlli obbligatori](#).

Passaggio 5. Impostare il log dei servizi su DEBUG, ricreare il problema di accesso e quindi raccogliere i log se i passaggi precedenti non risolvono il problema.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Log delle applicazioni
- Event Viewer-Log di sistema
- Cisco SSO
- Cisco Tomcat
- Cisco Tomcat Security

Controlli obbligatori

Passaggio 1. Verificare che l'utente sia assegnato a un nodo Presenza (passare a **Amministrazione messaggistica immediata e presenza > Sistema > Topologia**) e che non vi siano duplicati per l'utente (passare a **Amministrazione messaggistica immediata e presenza > Diagnostica > Risoluzione dei problemi di sistema**)

Passaggio 2. Se l'opzione Alta disponibilità è abilitata, passare a **Amministrazione CUCM > Server >**

Gruppo di ridondanza presenza e verificare se si trovano nello **stato Normale**. L'immagine mostra un esempio di visualizzazione dello stato normale. Per ulteriori informazioni sull'alta disponibilità, consultare [questo documento](#).

Stato anomalo

High Availability				
<input checked="" type="checkbox"/> Enable High Availability				
Monitored Server	Assigned Users	Active Users	Server State	
192.168.100.95	0	0	Running in Backup Mode	
192.168.100.96	0	0	Failed Over	

Nota: questi servizi vengono utilizzati da Jabber per eseguire il login: Cisco Tomcat, Cisco Tomcat Security, Cisco Client Profile Agent, Cisco XCP Connection Manager, Cisco XCP Router e autenticazione Cisco XCP.

Stato normale

High Availability				
<input checked="" type="checkbox"/> Enable High Availability				
Monitored Server	Assigned Users	Active Users	Server State	
192.168.100.95	0	0	Normal	
192.168.100.96	0	0	Normal	

Passaggio 3. Controllare lo stato della replica ad alta disponibilità.

a.utils dbreplication runtimestate

```
DB Version: ccm10_5_1_13900_2
Repltimeout set to: 300s
PROCESS option set to: 1

Cluster Detailed View from IMPSUB-1051SU3 (2 Servers):
```

SERVER-NAME	IP ADDRESS	PING (msec)	DB/RPC/DbMon?	REPL. QUEUE	Replication Group ID
IMPPUB-1051SU3	192.168.100.85	6.163	Y/Y/Y	0	(g_4)
IMPSUB-1051SU3	192.168.100.86	0.025	Y/Y/Y	0	(g_5)

In caso di problemi relativi alla replica del database, [passare a questo collegamento](#).

b.esegui ttlog sql pe in select count(*) from typesysreplication

```
admin:run pe sql ttlogin select count(*) from typesysreplication
sqlRv(t) sqlstmt(select count(*) from typesysreplication;)
***result set start***
count(0), success(t)
***result set end***
```

o utilizza `imdb_replication status` (10.5.2 SU2a e versioni successive)

```
admin:utils imdb_replication status
Running IMDB DSN (ttsoft, ttlogin, ttreg) replication checks on all nodes in clust
NOTE: For diagnostic test to run, ports 6603, 6604 & 6605 must be open on any fire

Sub Cluster Name / Id :: galacticRepublic / 1000
  Checking connectivity & removing old data prior to running diagnostic
  Cisco Presence Datastore Replication
    10.3.85.23 -> 10.3.85.24      Passed
    10.3.85.24 -> 10.3.85.23      Passed
  Cisco Login Datastore Replication
    10.3.85.23 -> 10.3.85.24      Passed
    10.3.85.24 -> 10.3.85.23      Passed
  Cisco SIP Registration Datastore Replication
    10.3.85.23 -> 10.3.85.24      Passed
    10.3.85.24 -> 10.3.85.23      Passed

Sub Cluster Name / Id :: rebelAllianceCluster / 3000
  rebelAllianceCluster has a single node, IMDB replication not required

SUCCESS :: IMDB DSN Replication is correctly configured accross cluster
Log file for the test can be gathered as follows:
  file get activelog epas/trace/imdb/sdi/imdb_state-20210705-1851.log
admin:█
```

I tre archivi dati devono risultare **PASSED** e il comando deve essere eseguito su tutti i nodi IM&P, in quanto è possibile che su un nodo tutte le repliche degli archivi dati risultino **Passed** e su un altro nodo **Failed**.

Se la replica IMDB (In-memory Database) non è corretta, alcuni o tutti gli utenti potrebbero non essere in grado di accedere o lo stato di presenza potrebbe non essere visualizzato correttamente.

Questa è la procedura per risolvere i problemi di replica IMDB:

Passaggio 1. Disabilitare l'alta disponibilità (HA) per il sottocluster IM&P interessato.

Passaggio 2. Arresta Cisco Presence Engine su tutti i nodi

utils service stop Cisco Presence Engine

Passaggio 3. Verificare che tutti i servizi dell'archivio dati siano in esecuzione: Cisco Log in Datastore, Cisco Route Datastore, Cisco Presence Datastore, Cisco SIP Registration Datastore.

utils service list

Passaggio 4. Riavviare Cisco Config Agent su ogni nodo uno alla volta.

utils service restart Cisco Config Agent

Passaggio 5. Avviare Cisco Presence Engine.

utils service start Cisco Presence Engine

Passaggio 6. Abilitare HA per il sottocluster.

Come impostare i log su DEBUG

Passaggio 1 Selezionare **Navigation > Unified Serviceability > Trace > Configuration** (Navigazione > Unified Serviceability > Traccia > Configurazione).

2. Dall'elenco a discesa Server, scegliere il server (ad esempio il nodo IMP) che esegue il servizio per configurare la traccia e fare clic su **Go**.

3. Dalla casella di riepilogo a discesa Service Group (Gruppo di servizi), scegliere il gruppo di servizi per il servizio da configurare come traccia, quindi fare clic su **Go** (Vai).

4. Dalla casella di riepilogo a discesa Servizio, scegliere il servizio per il quale si desidera configurare la traccia, quindi fare clic su **Vai**.

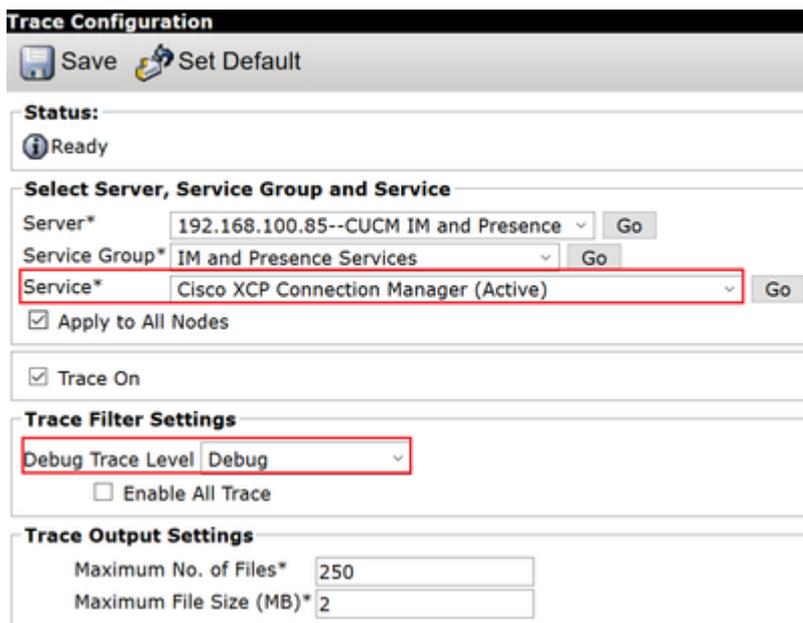
Passaggio 5 Selezionare la casella di controllo **Apply to All Nodes** (Applica a tutti i nodi), quindi selezionare il livello di traccia su **DEBUG**.

Passaggio 6 Per salvare la configurazione dei parametri di traccia, fare clic sul pulsante **Save** (Salva).

Per ulteriori informazioni su come impostare i livelli di traccia, consultare il documento [Cisco Unified Serviceability Administration Guide](#).

Video utili:

- [Recupero dei log da RTMT](#)



Trace Configuration

Save Set Default

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence Go

Service Group* IM and Presence Services Go

Service* Cisco XCP Connection Manager (Active) Go

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level Debug

Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 2

Trace Configuration

Save Set Default

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence Go

Service Group* IM and Presence Services Go

Service* Cisco Client Profile Agent (Active) Go

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level Debug

Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 1

Trace Configuration

Save Set Default

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence Go

Service Group* IM and Presence Services Go

Service* Cisco Login Datastore (Active) Go

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level Debug

Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 1

Trace Configuration

Save Set Default

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence Go

Service Group* IM and Presence Services Go

Service* Cisco XCP Authentication Service (Active) Go

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level Debug

Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 2

Trace Configuration

Save Set Default

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence Go

Service Group* IM and Presence Services Go

Service* Cisco XCP Router (Active) Go

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level Debug

Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 2

Log da recuperare

RTMT	CLI di amministrazione
Cisco Client Profile Agent	file get activelog tomcat/logs/epassoap/log4j/*
Cisco Log in Datastore	file get activelog epas/trace/imdb/sdi/ttlog in/
Log di Cisco Tomcat Security	file get activelog tomcat/logs/security/log4j/*
Cisco XCP Authentication Service	file get activelog epas/trace/xcp/log/auth*
Cisco XCP Connection Manager	file get activelog epas/trace/xcp/log/client-cm-1*.log
Cisco XCP Router	file get activelog epas/trace/xcp/log/rtr-jsm-1
Event Viewer-Log delle applicazioni	file get activelog syslog/CiscoSyslog*
Event Viewer-Log di sistema	file get activelog syslog/messages*

Recupero dei log da RTMT

Real Time Monitoring Tool For Cisco Unified Communications Solutions

System

- System Summary
 - System Summary
- Server
 - CPU and Memory
 - Process
 - Disk Usage
 - Critical Services
- Performance
 - Performance
 - Performance Log Viewer
- Tools
 - Alert Control
 - Trace & Log Central**
 - Job Status
 - SysLog Viewer
 - VLT
 - AuditLog Viewer

Trace & Log Central

- Trace & Log Central
 - Remote Browse
 - Collect Files**
 - Query Wizard
 - Schedule Collection
 - Local Browse
 - Real Time Trace
 - Collect Crash Dump
 - Collect Install Logs
 - Audit Logs

Collect Files

Select System Services/Applications Select all Services on all

Name	All Servers
Cisco Role-based Security	<input type="checkbox"/>
Cisco Row Information Spooling	<input type="checkbox"/>
Cisco SOAP Web Service	<input type="checkbox"/>
Cisco SOAPMessage Service	<input type="checkbox"/>
Cisco SSO	<input type="checkbox"/>
Cisco Serviceability Reporter	<input type="checkbox"/>
Cisco Serviceability Reporter AlertReport	<input type="checkbox"/>
Cisco Serviceability Reporter CallActivitiesR...	<input type="checkbox"/>
Cisco Serviceability Reporter DeviceReport	<input type="checkbox"/>
Cisco Serviceability Reporter PRRReport	<input type="checkbox"/>
Cisco Serviceability Reporter ServerReport	<input type="checkbox"/>
Cisco Serviceability Reporter ServiceReport	<input type="checkbox"/>
Cisco Stored Procedure Trace	<input type="checkbox"/>
Cisco Syslog Agent	<input type="checkbox"/>
Cisco Tomcat	<input type="checkbox"/>
Cisco Tomcat Security Logs	<input checked="" type="checkbox"/>
Cisco Tomcat Stats Servlet	<input type="checkbox"/>
Cisco Trace Collection Service	<input type="checkbox"/>
Cisco Unified OS Admin Web Service	<input type="checkbox"/>
Cisco Unified OS Platform API	<input type="checkbox"/>
Cisco Unified Reporting Web Service	<input type="checkbox"/>
Cisco WebDialerRedirector Web Service	<input type="checkbox"/>
Cron Logs	<input type="checkbox"/>
Event Viewer-Application Log	<input type="checkbox"/>
Event Viewer-System Log	<input type="checkbox"/>
FIPS Logs	<input type="checkbox"/>

< Back Next > Finish

Voice/Video

AnalysisManager

IM and Presence

Trace&LogCentral

System

System Summary

- System Summary

Server

- CPU and Memory
- Process
- Disk Usage
- Critical Services

Performance

- Performance
- Performance Log Viewer

Tools

- Alert Central
- Trace & Log Central**
- Job Status
- SysLog Viewer
- VLT
- AuditLog Viewer

Voice/Video

AnalysisManager

IM and Presence

Trace & Log Central

- Trace & Log Central
 - Remote Browse
 - Collect Files**
 - Query Wizard
 - Schedule Collector
 - Local Browse
 - Real Time Trace
 - Collect Crash Dump
 - Collect Install Logs
 - Audit Logs

Collect Files

Select IM_AND_PRESENCE Services/Applications

Select all Services on all Servers

Name	All Servers
Cisco AXL Web Service	<input type="checkbox"/>
Cisco Bulk Provisioning Service	<input type="checkbox"/>
Cisco Client Profile Agent	<input checked="" type="checkbox"/>
Cisco Config Agent	<input type="checkbox"/>
Cisco IM and Presence Admin	<input type="checkbox"/>
Cisco IM and Presence Data Monitor	<input type="checkbox"/>
Cisco Intercluster Sync Agent	<input type="checkbox"/>
Cisco Login Datastore	<input checked="" type="checkbox"/>
Cisco OAM Agent	<input type="checkbox"/>
Cisco Presence Datastore	<input type="checkbox"/>
Cisco Presence Engine	<input type="checkbox"/>
Cisco RCC Device Selection Service	<input type="checkbox"/>
Cisco Route Datastore	<input type="checkbox"/>
Cisco SIP Proxy	<input type="checkbox"/>
Cisco SIP Registration Datastore	<input type="checkbox"/>
Cisco Server Recovery Manager	<input type="checkbox"/>
Cisco Sync Agent	<input type="checkbox"/>
Cisco XCP Authentication Service	<input checked="" type="checkbox"/>
Cisco XCP Config Manager	<input type="checkbox"/>
Cisco XCP Connection Manager	<input checked="" type="checkbox"/>
Cisco XCP Directory Service	<input type="checkbox"/>
Cisco XCP File Transfer Manager	<input type="checkbox"/>
Cisco XCP Message Archiver	<input type="checkbox"/>
Cisco XCP Router	<input checked="" type="checkbox"/>
Cisco XCP SIP Federation Connection Man...	<input type="checkbox"/>
Cisco XCP Text Conference Manager	<input type="checkbox"/>

< Back **Next >** Finish

Trace&LogCentral

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).