

Configurazione e risoluzione dei problemi di Live Data in un ambiente UCCE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Introduzione](#)

[Controlli della connettività dei dati in tempo reale con Router e PG](#)

[Failover Live Data Server](#)

[Failover TIP](#)

[Failover SocketIO](#)

[Controlli pre-configurazione](#)

[Passaggi di configurazione di Live Data per le distribuzioni UCCE](#)

[Elenco di controllo per la risoluzione dei problemi](#)

[Passaggio 1: Verificare lo stato del servizio Live Data](#)

[Passaggio 2: Verificare la connettività dei dati dinamici a AW](#)

[Passaggio 3: Verificare lo stato del cluster Live Data tramite il comando show live-data failover](#)

[Passaggio 4: Verificare la configurazione dell'origine dati dinamica](#)

[Passaggio 5: Verificare lo stato di Live Data Datasource su CUIC](#)

[Passaggio 6: Verifica della connettività delle porte sui server Live Data](#)

[Passaggio 7: Verifica della connettività delle porte sui server ICM](#)

[Fase 8: controlli aggiuntivi](#)

[Registri necessari per la risoluzione dei problemi relativi a Live Data](#)

[Dai server ICM](#)

[Router](#)

[PG](#)

[Dai server LiveData](#)

[Utilizzo di RTMT](#)

[Uso della CLI](#)

[Dai server CUIC](#)

[Utilizzo di RTMT](#)

[Uso della CLI](#)

[Console del browser e registri di rete](#)

[Acquisizione pacchetti](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi a Live Data in un ambiente UCCE (Unified Contact Center Enterprise).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

Cisco Unified Contact Center Enterprise (UCCE)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Versione ICM: 12.6

Versione Finesse: 12.6

CUIC/Live Data versione: 12.6

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.

Introduzione

Live Data è un framework di dati che elabora eventi in tempo reale con elevata disponibilità per i report Live Data. Live Data elabora in modo continuo gli eventi dell'agente e delle chiamate dal gateway periferico e dal router. Quando si verificano gli eventi, Live Data invia continuamente aggiornamenti in tempo reale ai client di reporting di Unified Intelligence Center. Il PG e l'agente push del router e chiamano gli eventi a Live Data non appena si verificano gli eventi. Live Data aggrega ed elabora continuamente gli eventi in-stream e pubblica le informazioni. CUIC si iscrive al flusso di messaggi per ricevere gli eventi in tempo reale e aggiornare continuamente i report Live Data. I valori dei singoli stati, ad esempio gli stati dell'agente, vengono aggiornati man mano che si verificano. Altri valori, ad esempio le chiamate in coda, vengono aggiornati approssimativamente ogni 3 secondi.

In Unified CCE, Live Data risiede su una macchina virtuale (VM) Cisco Voice Operating System. È possibile incorporare i report Live Data nei desktop degli agenti Finesse.

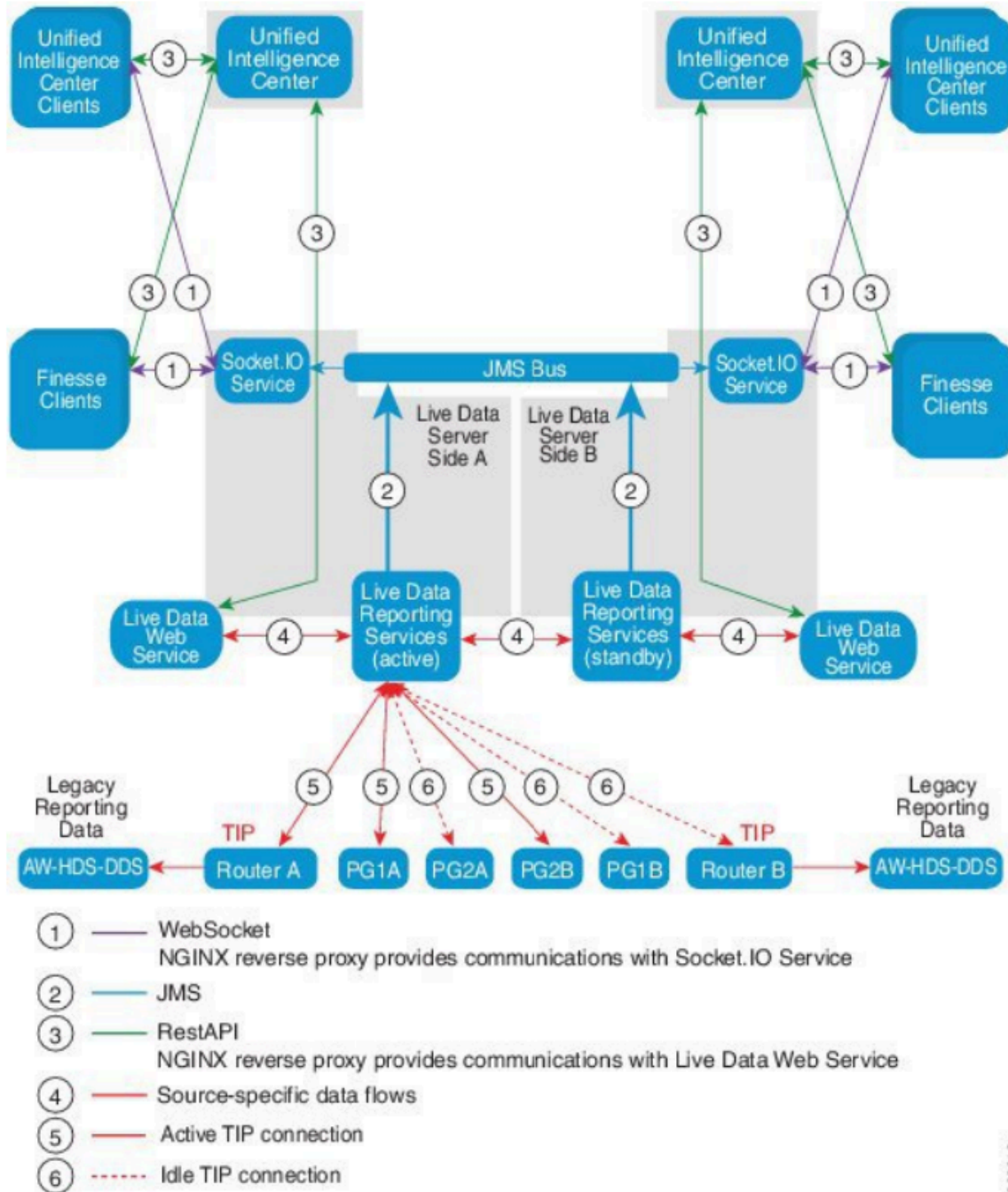
Per installazioni di agenti nel 2000

- Il server Live Data è installato in una VM con Cisco Unified Intelligence Center (CUIC) e

Cisco Identity Service (IdS)

Per installazioni di agenti 4000 e superiori

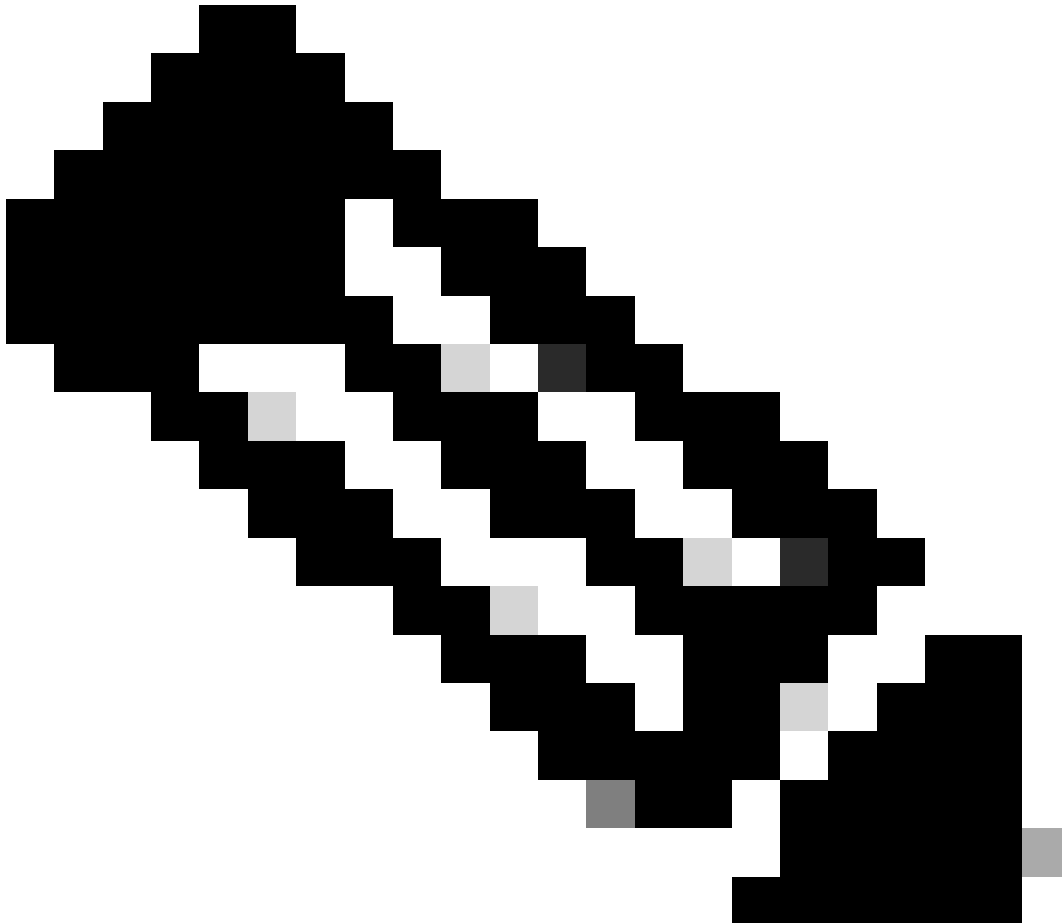
- Il server Live Data è installato su una VM standalone.



Controlli della connettività dei dati in tempo reale con Router e PG

Il server Live Data attivo deve stabilire una connessione TIP e TOS ai router e a tutti i PG agente. Il server Live Data in-attivo (standby) deve stabilire solo una connessione TOS ai router e a tutte le pagine dell'agente.

- La porta Router/PG per la connessione TIP ha il formato indicato in questo regexp: 4[0-5]034 (si presume che esista una sola istanza di CCE, ad esempio: 40034, 41034, 42034...)
 - La porta Router/PG per la connessione TOS ha il formato indicato in questo regexp: 4[0-5]035 (si presume che esista solo un'istanza di CCE, ad esempio: 40035, 41035, 42035...)
-



Nota:

- Le porte per le connessioni TIP/TOS vengono assegnate in base all'ordine in cui la coppia PG (lato A/B) è installata sullo stesso server.
 - Ad esempio, alla prima coppia PG (PG1 Side A/B) installata vengono assegnate rispettivamente le porte TIP base 42034 e 43034. Alla seconda coppia PG (PG2 Side A/B) installata sono assegnate rispettivamente le porte 44034 e 45034. La stessa assegnazione è applicabile anche alle porte TOS.
 - Le porte TIP e TOS possono variare in base al numero di istanza. Per ulteriori informazioni, consultare la Port Utilization Guide for Cisco Unified Contact Center Solutions.
-

Failover Live Data Server

I server Live Data funzionano in modalità cold-active o standby. È attivo un solo server Live Data alla volta. L'altro server Live Data è in standby. Il server Live Data di standby controlla costantemente lo stato del server attivo. Quando si verifica un errore sul server attivo, il server di standby subentra e diventa attivo. Il server che ha generato l'errore diventa il server in standby quando è pronto per essere utilizzato.

Failover TIP

Live Data utilizza il protocollo di trasporto TIP per comunicare con il router e i server PG. Il server Live Data attivo stabilisce connessioni TIP su entrambi i lati del router e dei server PG. Il server Live Data in standby non stabilisce connessioni TIP. È attiva una sola connessione TIP alla volta, verso il lato A o verso il lato B. Quando la connessione TIP attiva non riesce, il server Live Data attivo viene ripristinato alla connessione TIP inattiva.

Failover SocketIO

Un client SocketIO si connette a entrambi i lati del server Live Data per ricevere il flusso di eventi del report Live Data (flusso SocketIO). I client di Unified Intelligence Center sono un esempio di client SocketIO. Il server Live Data di standby produce inoltre il flusso SocketIO per proxy dal server attivo. Le perdite di heartbeat del client SocketIO determinano un errore di connessione SocketIO. Il client SocketIO esegue quindi il failover sull'altro server Live Data.

Controlli pre-configurazione

Prima di distribuire Live Data, eseguire i controlli seguenti:

Controllo 1

Dai server ICM, verificare la ricerca DNS diretta e inversa per Live Data Publisher e il Sottoscrittore, utilizzando il comando nslookup.

```
<#root>
```

```
nslookup <Live-Data-Server-FQDN>
```

```
nslookup <Live-Data-Server-IP>
```

Controllo 2

Dalla CLI di Live Data Server, verificare la ricerca di DNS forward e reverse per i router e i PG (eseguire i controlli del lato A e del lato B).

```
<#root>
```

```
utils network host <FQDN>
```

Sostituire <FQDN> con gli FQDN pubblici dei router/gruppi di continuità

```
<#root>
```

```
utils network host <IP>
```

Sostituire <IP> con l'indirizzo IP pubblico dei router/PG (controllare sia il lato A che il lato B)

Controllo 3

Verificare le configurazioni NTP e i requisiti per un ambiente CCE. Fare riferimento alla sezione NTP and Time Synchronization nella Guida alla progettazione di soluzioni CCE.

Controllo 4

Assicurarsi che i limiti di configurazione siano rispettati come indicato nella Guida alla progettazione della soluzione CCE

- Limiti per gli agenti e i supervisori, ad esempio: Agenti configurati per gruppo, Agenti per gruppo, Numero di agenti è un gruppo di abilità e così via. Per ulteriori informazioni, consultare la Guida alla progettazione della soluzione CCE.

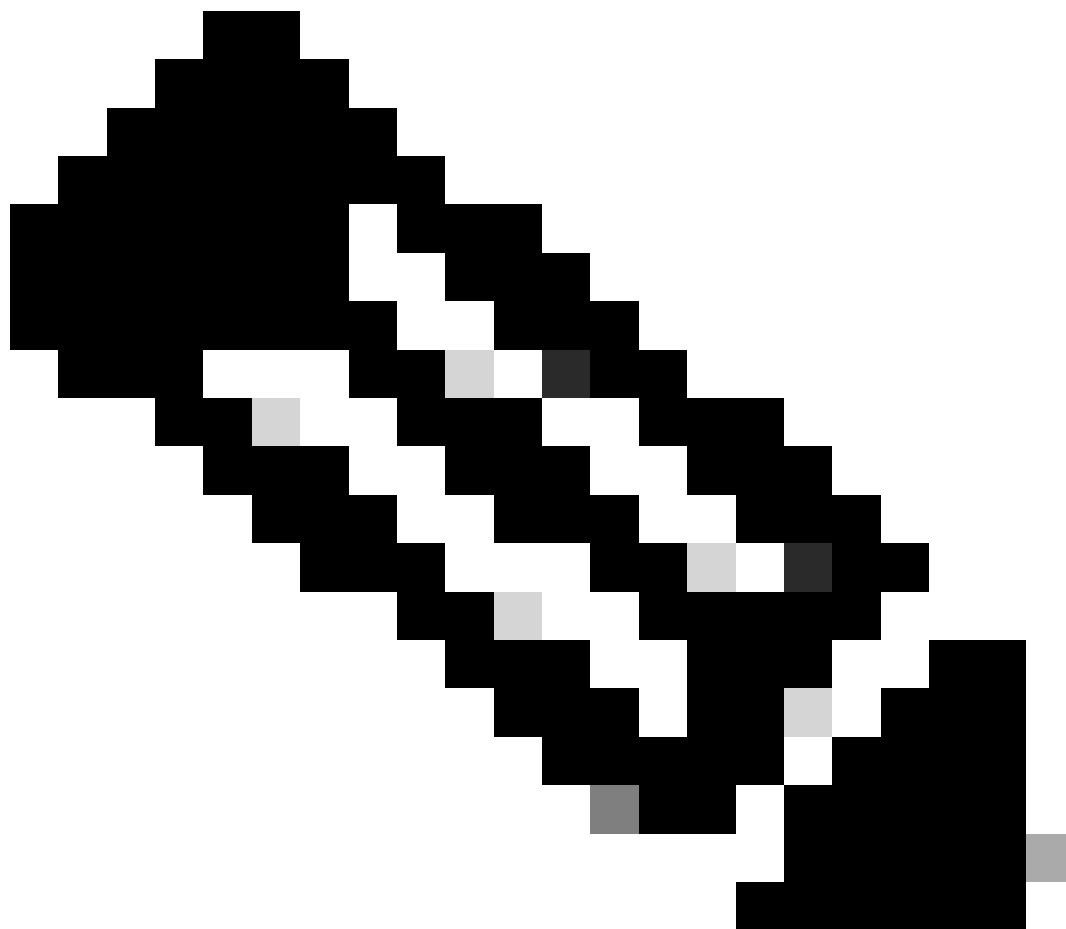


Nota:

- Se i server Live Data non vengono distribuiti come indicato nella Guida alla progettazione (in modalità co-residente o standalone) o se vengono superate le limitazioni di configurazione, il servizio Live Data può rimanere fuori servizio.
- Per evitare problemi con il servizio Live Data, è consigliabile che la versione di Live Data Server corrisponda esattamente alla versione ICM per la distribuzione.

Controllo 5

Scambio di certificati per Live Data in una distribuzione UCCE



Nota: se nella distribuzione CCE vengono utilizzati certificati firmati dall'autorità di certificazione (ICM, Finesse, CUIC, LD e IdS) (firmati dalla stessa autorità di certificazione), questo controllo può essere ignorato.

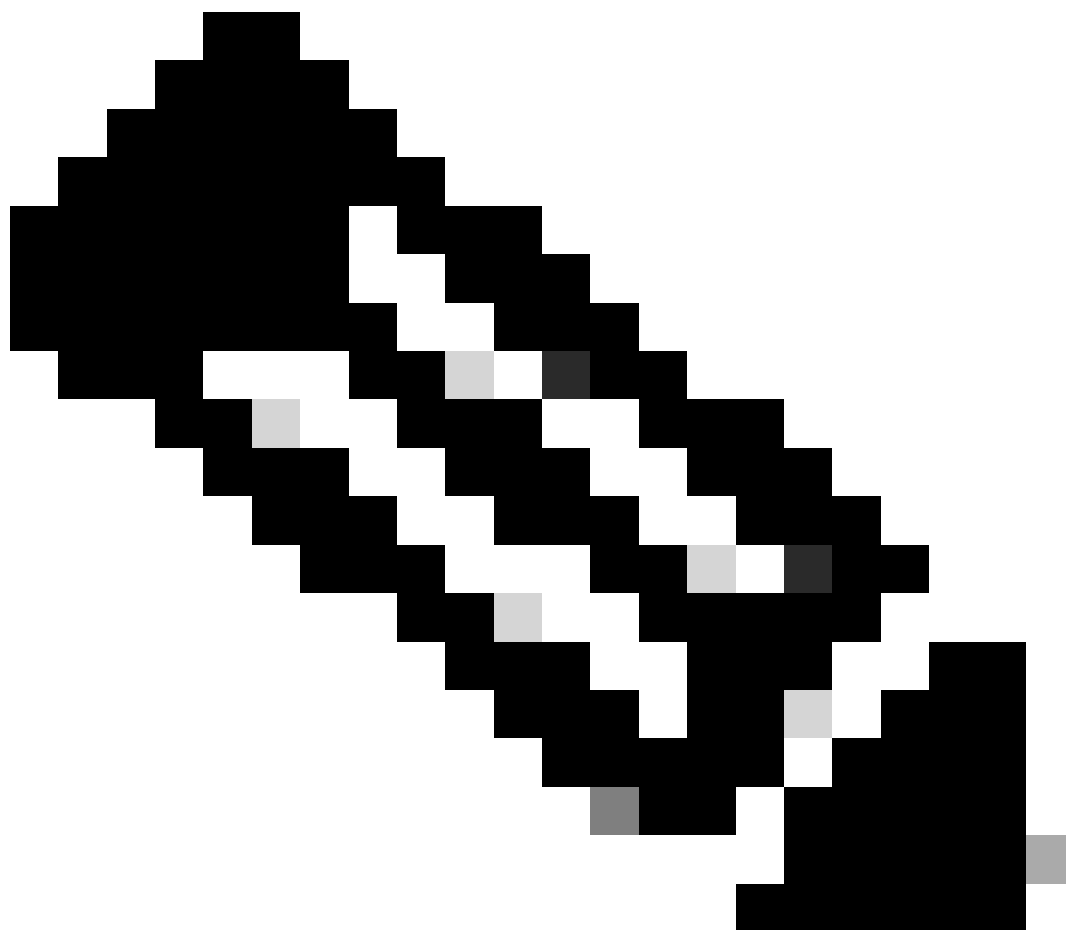
Quando si utilizzano certificati autofirmati

Per le distribuzioni di agenti 2000

- Assicurarsi che i certificati tomcat del server di pubblicazione CUIC-LD-IdS e dei server sottoscrittori vengano caricati nel server di pubblicazione Finesse come tomcat-trust
- Accertarsi che i certificati tomcat dei server Finesse Publisher e Subscriber vengano caricati nel server CUIC-LD-IdS Publisher come tomcat-trust.
- Verificare che i certificati tomcat del server di pubblicazione CUIC-LD-IdS e dei server sottoscrittori vengano caricati in tutti i server AW.

Per installazioni di agenti 4000 e 12000

- Accertarsi che i certificati tomcat dei server Live Data Publisher e Subscriber vengano caricati in CUIC Publisher e in Finesse Publisher come tomcat-trust.
 - Accertarsi che i certificati tomcat dei server di pubblicazione CUIC e dei server sottoscrittori vengano caricati in Live Data Publisher e in Finesse Publisher come tomcat-trust.
 - Accertarsi che i certificati tomcat dei server Finesse Publisher e Subscriber siano caricati in CUIC Publisher e in Live Data Publisher come tomcat-trust.
 - Verificare che i certificati tomcat di tutti i server CUIC, Live Data e Finesse vengano caricati in tutti i server AW.
 - Verificare che il certificato IIS dei server AW venga caricato nel server Live Data Publisher come tomcat-trust.
-



Nota:

- I certificati caricati come tomcat-trust nel server di pubblicazione vengono replicati nel nodo del Sottoscrittore nello stesso cluster.
-

-
- Quando un certificato viene caricato su un server VOS, è necessario un riavvio completo del server utilizzando il comando CLI utilizza il riavvio del sistema affinché il nuovo certificato caricato abbia effetto su quel server.
 - Per i server AW, è necessario riavviare il servizio Apache Tomcat affinché il certificato appena caricato abbia effetto su tale server AW.
-

Controllo 6

È NECESSARIO utilizzare il nome di dominio completo (FQDN) per tutti i comandi di configurazione Live Data. L'utilizzo dell'indirizzo IP durante la configurazione di Live Data può causare problemi con il servizio Live Data.

Controllo 7

a. Per tutti i comandi set Live Data, digitate manualmente le password anziché un'azione di copia e incolla.

b. Set di caratteri supportati per i comandi CLI di Live Data Installation

Quando si utilizza la CLI (e non solo per Live Data), è possibile utilizzare i caratteri alfanumerici semplici [0-9] [A-Z] [a-z] e i seguenti caratteri aggiuntivi:

- "." (punto)
- "!" (punto esclamativo)
- "@" (simbolo at)
- "#" (cancellotto)
- "\$" (dollaro)
- "%" (percentuale)
- "Accentso circonflesso"
- "*" (stella)
- "_" (trattino basso)
- "+" (segno più)
- "=" (segno di uguale)
- "~" (tilde)
- ":" (due punti)
- "(" e ")" (parentesi aperte e chiuse)
- "{" e "}" (parentesi quadre di apertura e chiusura)
- "[" e "]" (parentesi quadre di apertura e chiusura)
- Gli spazi vengono utilizzati come separatori di input. La maggior parte dei caratteri speciali ha un significato specifico per la console dei comandi di Cisco Voice Operating System (VOS) (ad esempio, "\", "| e così via). I caratteri diversi da ASCII standard vengono ignorati.

Passaggi di configurazione di Live Data per le distribuzioni UCCE

Passaggio 1

Verificare che il tipo di distribuzione corretto sia impostato in Amministrazione CCE in Infrastruttura > Impostazioni di distribuzione (<https://<AW-Server>/cceadmin>).

Passaggio 2

Aggiungere il server all'inventario CCE.

Per le distribuzioni di agenti 2000, aggiungere il cluster CUIC-LD-IdS coresidente selezionando l'opzione CUIC-LD-IdS Publisher.

Add Machine ✕

Type

Note: The CUIC-LD-IdS Subscriber will be added automatically

Per le distribuzioni di agenti della versione 4000 e successive, aggiungere il cluster CUIC autonomo selezionando l'opzione Unified Intelligence Center Publisher.

Add Machine ✕

Type

Note: Unified Intelligence Center Subscribers will be added automatically



Nota: per le distribuzioni di agenti 4000 e versioni successive, i server Live Data vengono aggiunti all'inventario utilizzando il comando `set live-data machine-services`.

Passaggio 3

Utilizzare il comando `set live-data reporting-interval <reporting-interval-in-minute>` per impostare l'intervallo di reporting dei dati in minuti.

- Gli intervalli validi sono: 5 (impostazione predefinita), 10, 15, 30 e 60.
- Se e quando questo valore viene modificato, è necessario riavviare il cluster Live Data.

Utilizzare il comando `show live-data reporting-interval` per visualizzare l'impostazione corrente dell'intervallo di reporting.

Passaggio 4

Configurare un utente SQL nel database AW per l'utilizzo di Live Data

Sul server di database AW primario e secondario > avviare SQL Server Management Studio

(SSMS):

- Creare un utente con l'appartenenza ai ruoli del database db_datareader e db_datawriter con l'impostazione Mapping utente del database awdb.
- Il ruolo del database public è controllato per impostazione predefinita. Questo ruolo è necessario per gli utenti CUIC, Finesse e Live Data.

Passaggio 5

Eseguire la query SQL per l'utente SQL configurato per l'utilizzo di Live Data.

```
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "<user>"
GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "<user>"
```

Sostituire <user> con il nome utente dell'utente creato nel passaggio 4.

Passaggio 6

Configurazione di Live Data con AW

<#root>

```
set live-data aw-access primary <aw1-server-fqdn> <port> <aw-database> <sql-user>
```

```
set live-data aw-access secondary <aw2-server-fqdn> <port> <aw-database> <sql-user>
```

Dove

- porta: porta SQL (per impostazione predefinita, il motore di database di SQL Server resta in ascolto sulla porta TCP 1433)
- aw-database: awdb
- sql-user: utente SQL creato nel database AW (passaggio 4)

Questo comando indica a Live Data come accedere al database AW primario e al database AW secondario. Il comando verifica inoltre automaticamente la connessione da Live Data all'AW principale o secondario, verifica se l'utente configurato dispone dell'accesso appropriato a AW DB e riporta i risultati. (Lo stato del test deve essere 'Completato'). Non è necessario configurare AW DB su entrambi i server Live Data Publisher e Subscriber. La configurazione viene replicata tra Live Data Publisher e il nodo Subscriber.

Per visualizzare i database AW primari e secondari configurati, utilizzare il comando:

<#root>

```
show live-data aw-access
```

Passaggio 7

Connetti i server dati Live ai record del servizio computer (solo per le distribuzioni di agenti 4000 e versioni successive)

```
<#root>
```

```
set live-data machine-services <user@domain>
```

Questo comando consente ai server LD di registrarsi nella tabella Machines Services in modo che i server LD siano individuabili. Vengono inoltre registrate le credenziali per la chiamata dell'API Live Data.

Requisiti di cui l'utente deve disporre per eseguire correttamente il comando di servizi computer:

- Deve essere un utente di dominio.
- Deve essere in formato UPN (User Principal Name). Esempio: admin@stooges.cisco.com
- È necessario disporre dell'autorizzazione di accesso in scrittura per le tabelle Machine.
- Deve essere autorizzato a modificare la configurazione di Unified CCE.



Nota:

- Quando si esegue questo comando, viene richiesto di specificare la password di accesso per `user@domain`, da utilizzare per l'autenticazione con accesso al database AW. Inoltre, richiede di specificare la password dell'utente connesso per la sessione CLI corrente.
- Per le distribuzioni dell'agente 2000, il servizio Live Data che fa parte di un cluster coresidente, viene aggiunto all'inventario quando vengono aggiunti i nodi coresidenti selezionando l'opzione 'CUIC-LD-IdS Publisher' nel passo 2. E quindi non è necessario un comando 'set live-data machine-services `<user@domain>`'.

Passaggio 8

Impostare l'origine dati Live Data in CUIC.

```
<#root>
```

```
set live-data cuic-datasource <cuic-fqdn> <cuic-port> CUIC\<cuic-user>
```

Dove

- cuic-port = 8444
- cuic-user = Utente applicazione CUIC (credenziali di accesso utente privilegiato)

Una volta eseguito correttamente questo comando, le origini dati Live primarie e secondarie possono essere visualizzate nella scheda Origini dati nell'interfaccia GUI CUIC.

Per visualizzare la configurazione dell'origine dati Live Data, utilizzare il comando:

<#root>

```
show live-data cuic-datasource <cuic-fqdn> <cuic-port> CUIC\<cuic-user>
```

Passaggio 9

Scaricate i report Live Data da cisco.com e importate i report Live Data sul server CUIC.



Nota: i report Live Data DEVONO corrispondere alla versione del controller centrale.

Passaggio 10

Nella pagina Cisco Finesse Administration (<https://<Finesse>/cfadmin>), passare alla scheda Finesse Desktop Layout e sostituire il nome di dominio completo (my-cuic-server) predefinito con il nome di dominio completo (FQDN) corretto del server CUIC.

Passaggio 11

Configurazione di Cross Origin Resource Sharing (CORS) per Live Data

a. Su Finesse Publisher e Subscriber, verificare che CORS sia abilitato utilizzando il comando `utilizza lo stato finesse cors`.

Se l'opzione è disabilitata, è possibile abilitarla usando il comando `finesse cors enable`.

b. Eseguire i comandi CORS su tutti i server CUIC:

```
<#root>
```

```
utils cuic cors enable
```

```
utils cuic cors allowed_origin add https://<finesse-publisher>
```

```
utils cuic cors allowed_origin add https://<finesse-subscriber>
```

```
utils cuic cors allowed_origin add https://<finesse-publisher>:8445
```

```
utils cuic cors allowed_origin add https://<finesse-subscriber>:8445
```

c. Eseguire i comandi CORS sui server Live Data Publisher e Subscriber:

```
<#root>
```

```
utils live-data cors enable
```

```
utils live-data cors allowed_origin add https://<finesse-publisher>
```

```
utils live-data cors allowed_origin add https://<finesse-subscriber>
```

```
utils live-data cors allowed_origin add https://<finesse-publisher>:8445
```

```
utils live-data cors allowed_origin add https://<finesse-subscriber>:8445
```

d. Per verificare la configurazione CORS:

Su tutti i server CUIC:

```
<#root>
```

```
utils cuic cors status
```

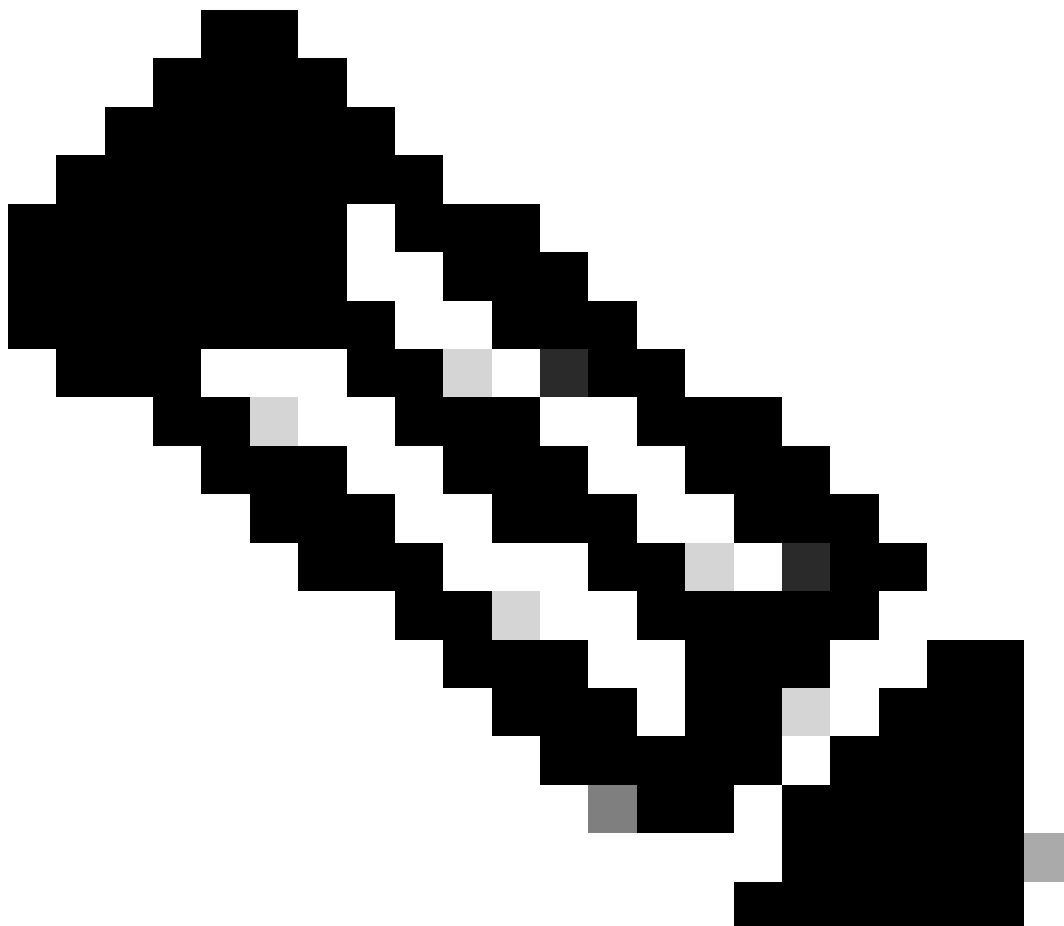
```
utils cuic cors allowed_origin list
```

In Live Data Publisher e Subscriber:

<#root>

```
utils live-data cors status
```

```
utils live-data cors allowed_origin list
```



Nota:

- Per le distribuzioni co-residenti, è necessario eseguire i core cuic e i core live-data set di comandi sui server di pubblicazione e di sottoscrizione co-residenti.
 - Per le distribuzioni standalone, il set di comandi utils cuic cors deve essere eseguito su tutti i nodi CUIC nel cluster CUIC e il set di comandi utils live-data cors deve essere eseguito sui server Live Data Publisher e Subscriber.
-

Riavviare tutti i server CUIC/LD e Finesse utilizzando il comando CLI:

```
<#root>
```

```
utils system restart
```

Elenco di controllo per la risoluzione dei problemi

Passaggio 1: Verificare lo stato del servizio Live Data

Verificare che tutti i servizi Live Data siano AVVIATI utilizzando il comando 'utils service list'.

```
CCE Live Data ActiveMQ Service[STARTED]
CCE Live Data Cassandra Service[STARTED]
CCE Live Data Event Store Service[STARTED]
CCE Live Data SocketIO Service[STARTED]
CCE Live Data Storm DRPC Service[STARTED]
CCE Live Data Storm Nimbus Service[STARTED]
CCE Live Data Storm Supervisor Service[STARTED]
CCE Live Data Web Service[STARTED]
CCE Live Data Zookeeper Service[STARTED]
```

Passaggio 2: Verificare la connettività dei dati dinamici a AW

Verificare la connettività ai server AW utilizzando il comando:

```
<#root>
```

```
show live-data aw-access
```

Lo stato del test deve essere 'Completato'.

Passaggio 3: Verificare lo stato del cluster Live Data tramite il comando show live-data failover

Verificare lo stato del cluster Live Data utilizzando il comando

```
<#root>
```

```
show live-data failover
```

Stato cluster	Descrizione
ACCOPPIATO-ATTIVO	Il server Live Data si trova nello stato attivo e sta comunicando con il lato remoto.
PAIRED-STANDBY	Il server Live Data è in stato di standby e sta comunicando con il lato remoto.
ISOLATO-ATTIVO	Il server Live Data si trova nello stato attivo, ma non è in grado di comunicare con il lato remoto.
STANDBY ISOLATO	Il server Live Data è in stato di standby, ma non è in grado di comunicare con il lato remoto.
MODALITÀ SEMPLIFICATA	Il server Live Data funziona in modalità simplex.
FUORI SERVIZIO	Il server Live Data è fuori servizio.
CONNESSIONE	Il server Live Data sta tentando di eseguire un handshake con il lato remoto.
TEST	Il server Live Data non è in grado di comunicare con il lato remoto e utilizza la procedura Test-Other-Side per determinare se si trova nello stato ISOLATED-ACTIVE o ISOLATED-STANDBY.
NON DISPONIBILE	Live Data non distribuito.



Nota: lo stato di standby/attivo ISOLATO indica una comunicazione tra server Live Data. In questo modo l'origine dati Live Data su CUIC non sarà in linea.

r. Se il comando 'show live-data failover' visualizza lo stato del cluster come NON DISPONIBILE.

- Questo stato indica che Live Data non è stato distribuito correttamente a causa di configurazioni incomplete.

Azioni:

- Accertarsi che tutti i passaggi di configurazione siano stati completati correttamente.
- Scaricare i log di CCE Live Data Storm Services utilizzando RTMT e analizzare il file `deployment_control.log`
- In alternativa, è possibile scaricare il file utilizzando il comando CLI `get active log livedata/logs/livedata-storm/deployment_control.log`

b. Se il comando 'show live-data failover' visualizza lo stato del cluster come OUT-OF-SERVICE.

- Questo stato indica che Live Data è stato distribuito correttamente, ma possono essersi verificati problemi di connettività o che i limiti di configurazione sono stati superati.

Azioni

- Assicurare la connettività di rete tra i server Live Data e i router/gruppi di continuità (consultare la Guida all'utilizzo della porta CCE)
- Assicurarsi che il server Live Data sia stato distribuito come indicato nella guida alla progettazione (in modalità co-residente e standalone)
- Assicurarsi che i limiti di configurazione NON siano stati superati.
- Scaricare e analizzare i log di CCE Live Data Storm Services (principalmente il file worker.log)
- In alternativa, è possibile scaricare il file di log utilizzando il file di comando CLI get activelog livedata/logs/livedata-storm/

c. Se il comando 'show live-data failover' visualizza lo stato del cluster come ISOLATED.

- Questo stato indica un problema di connettività tra i due server Live Data e pertanto non sono in grado di comunicare tra loro.

Passaggio 4: Verificare la configurazione dell'origine dati dinamica

Assicurarsi che l'origine dati Live Streaming rifletta gli host corretti utilizzando il comando:

```
<#root>
```

```
show live-data cuic-datasource <cuic-fqdn> <cuic-port> CUIC\<cuic-user>
```

Passaggio 5: Verificare lo stato di Live Data Datasource su CUIC

Se in 'show live-data cuic-datasource' vengono visualizzate le configurazioni corrette, ma in Live Data Datasource viene visualizzato offline in CUIC:

- Verificare che le porte del servizio Web Live Data e del servizio Live Data SocketIO siano aperte in modo bidirezionale tra il server Live Data e il browser.
- I servizi CCE Live Data Storm, il servizio CCE Live Data SocketIO e i registri della console del browser possono contribuire a isolare ulteriormente la possibile causa del problema.



Nota: a partire dalla versione 12.6.2 di Live Data, le porte 12005 e 12008 sono obsolete e verranno rimosse nelle versioni future. La porta 443 è ora utilizzata per Live Data Web Service e Live Data SocketIO Service.

Passaggio 6: Verifica della connettività delle porte sui server Live Data

Verificare la connettività delle porte dalla CLI di Live Data Server utilizzando il comando `show open ports`.

- L'output del server Live Data attivo deve mostrare 2 connessioni stabilite a ciascuno dei router e delle pagine dell'agente (per le connessioni TIP e TOS).
- L'output del Live Data Server in-active (standby) deve mostrare una connessione stabilita ai router e ai PG (per le connessioni TOS).

<#root>

```
show open ports regexp 4[0-5]03[45]
```


(For Instance-0)

```
show open ports regexp 4[0-5]07[45]
```

(For Instance-1)

Passaggio 7: Verifica della connettività delle porte sui server ICM

Verificare la connettività delle porte dal prompt dei comandi sui router e i PG utilizzando il comando netstat.

- L'output deve visualizzare le porte nello stato STABILITO per Live Data Publisher e Subscriber.
- Nell'output devono essere visualizzate due connessioni STABILITE al server Active Live Data (per le connessioni TIP e TOS).
- L'output deve mostrare 1 connessione STABILITA al server Live Data in-active (standby) (per le connessioni TOS).

<#root>

```
netstat -an | findstr "<LD-SideA-IP> <LD-SideB-IP>"
```

OR

```
netstat -an | findstr 4[0-5]03[45]
```

(For Instance-0)

```
netstat -an | findstr 4[0-5]07[45]
```

(For Instance-1)

r. Se le porte non risultano neanche in stato LISTENING:

- Verificare che il tipo di distribuzione corretto e supportato sia impostato in base alla guida alla progettazione.
- Può essere necessario riavviare il server.

b. Se le porte non si trovano nello stato STABILITO e continuano a trovarsi nello stato LISTENING:

- Verificare la connettività di rete tra i router/server PG e i server Live Data.
- Dai router/PG, verificare le ricerche DNS dirette e inverse per il server Live Data.
- Dai server LiveData, verificare le ricerche DNS dirette e inverse per gli indirizzi pubblici del server Router/PG.

Fase 8: controlli aggiuntivi

a. Query SQL per controllare il numero di agenti configurati per team:

Esegui query su awdb (nessun impatto sulla produzione)

```
Select TeamName = AT.EnterpriseName, NumAgentsOnTeam = COUNT(ATM.SkillTargetID), SupervisorName = Person
FROM Agent_Team AT LEFT OUTER JOIN
(Select * from Agent ) Agent ON AT.PriSupervisorSkillTargetID = Agent.SkillTargetID LEFT OUTER JOIN Per
Agent_Team_Member ATM
WHERE ATM.AgentTeamID = AT.AgentTeamID
GROUP BY AT.EnterpriseName, Person.LastName + ', ' + Person.FirstName
ORDER BY AT.EnterpriseName
```

b. Query SQL per controllare il numero di agenti configurati per gruppo di abilità:

Esegui query su awdb (nessun impatto sulla produzione)

```
Select Skill_Group.EnterpriseName, NumAgentsInSG = COUNT(Skill_Group_Member.AgentSkillTargetID)
FROM Skill_Group, Skill_Group_Member
WHERE Deleted = 'N' AND Skill_Group.SkillTargetID = Skill_Group_Member.SkillGroupSkillTargetID
GROUP BY EnterpriseName;
```

c.

Se dopo un aggiornamento vengono rilevati problemi relativi a Live Data, controllare il valore di configurazione 'DBMaintenance'.

- 0 - abilitato
- 1 - disattivato.

Se è disattivata, abilitare le modifiche alla configurazione impostando DBMaintenance su 0 e riavviare il servizio Apache Tomcat sul server AW.

Percorso Registro di sistema: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\

Registri necessari per la risoluzione dei problemi relativi a Live Data

Dai server ICM

- Impostare l'impostazione di traccia per il processo rtr e opc su livello 1 o livello 2, a seconda dei dettagli che si desidera vengano visualizzati nei log.

Router

- registri rtr

PG

- registri opc

Dai server LiveData

Utilizzo di RTMT

Collect Files

Select LiveData Services/Applications

Select all Services on all Servers

Name	All Servers
CCE Live Data ActiveMQ Service	<input type="checkbox"/>
CCE Live Data Cassandra Service	<input type="checkbox"/>
CCE Live Data Event Store Service	<input type="checkbox"/>
CCE Live Data Socket.IO Service	<input type="checkbox"/>
CCE Live Data Storm Services	<input type="checkbox"/>
CCE Live Data Web Service	<input type="checkbox"/>
CCE Live Data Zookeeper Service	<input type="checkbox"/>

Uso della CLI

```
admin:file get activelog ?
Syntax:
file get activelog file-spec [options]
file-spec    mandatory    file to transfer
options      optional     reltime months|weeks|days|hours|minutes timevalue
                                abstime hh:mm:MM/DD/YY hh:mm:MM/DD/YY
                                match regex
                                recurs
                                compress
```

<#root>

```
file get activelog livedata/logs recurs compress
```

Questo comando raccoglie i log per tutti i componenti Live Data

In alternativa, è possibile raccogliere i log anche per i singoli componenti Live Data.

<#root>

CCE Live Data ActiveMQ

```
file get activelog livedata/logs/livedata-activemq
```

CCE Live Data Cassandra Service

```
file get activelog livedata/logs/livedata-cassandra
```

CCE Live Data Event Store Service

```
file get activelog livedata/logs/livedata-event-store
```

CCE Live Data SocketIO Service

```
file get activelog livedata/logs/socketio-service
```

CCE Live Data Storm Services

```
file get activelog livedata/logs/livedata-storm
```

CCE Live Data Web Service

```
file get activelog livedata/logs/livedata-web
```

CCE Live Data Zookeeper Service

```
file get activelog livedata/logs/livedata-zookeeper
```

Dai server CUIC

Utilizzo di RTMT

Collect Files

Select CUIC Services/Applications

Select all Services on all Servers

Name	All Servers
Intelligence Center OAMP Service	<input type="checkbox"/>
Intelligence Center Perfmon Service	<input type="checkbox"/>
Intelligence Center Reporting Service	<input type="checkbox"/>
Intelligence Center SNMP Java Adapter Ser...	<input type="checkbox"/>
Intelligence Center Serviceability Service	<input type="checkbox"/>

Uso della CLI

```
<#root>
```

```
Intelligence Center Reporting Service
```

```
file get activelog cuic/logs/ recurs compress
```

Console del browser e registri di rete

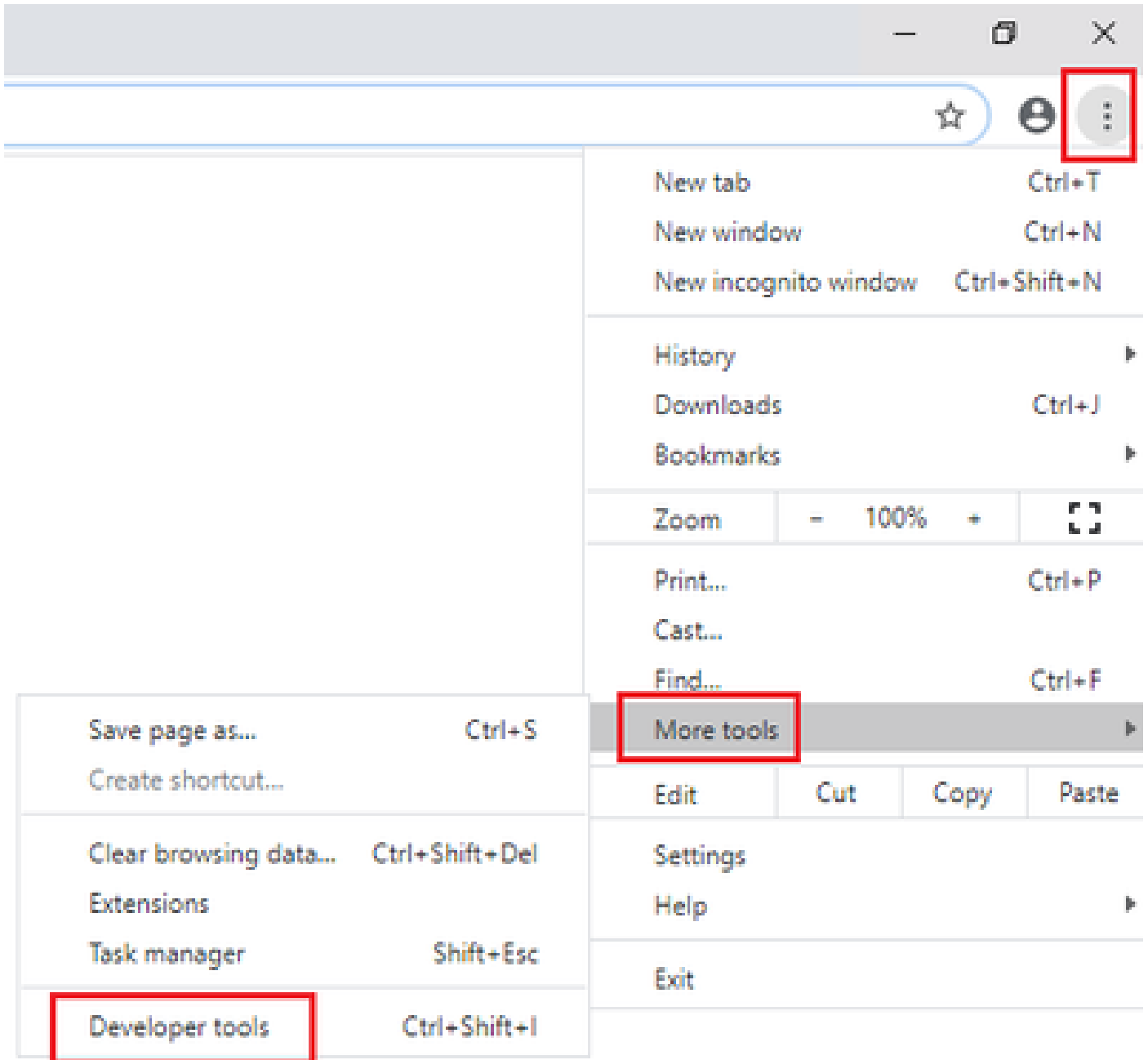
Raccogliere i registri di rete e console del browser per la durata del problema. Iniziare con la cancellazione della cache, riavviare il browser e acquisire i log dall'ora di accesso in poi, includendo il tentativo effettuato di riprodurre il problema

Per il browser Chrome/Edge:

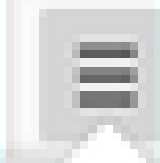
- Fare clic sull'icona Impostazioni e selezionare Strumenti di sviluppo > Altri strumenti > Strumenti di sviluppo.
- In Strumenti di sviluppo > scheda Console, fare clic sul simbolo di ingranaggio e controllare le opzioni: Mantieni registro, Mostra timestamp, Log XMLHttpRequests.
- Nella scheda Strumenti di sviluppo > Rete, fare clic sul simbolo dell'ingranaggio e selezionare l'opzione: Mantieni registro.
- Chiudere la pagina delle impostazioni.
- È ora possibile raccogliere i registri della console e della rete facendo clic con il pulsante destro del mouse sulle rispettive schede e selezionando Salva tutto con nome.

Per il browser Firefox:

- Fare clic sull'icona del menu Applicazioni e selezionare Altri strumenti > Strumenti di sviluppo Web.
- Nella scheda Rete, fare clic sul simbolo dell'ingranaggio e selezionare l'opzione: Registri persistenti.
- È ora possibile raccogliere i registri della console e della rete facendo clic con il pulsante destro del mouse sulle rispettive schede e selezionando Salva tutto con nome.



Chrome



Sign in to Sync



Content Blocking

Standard



New Window

Ctrl+N



New Private Window

Ctrl+Shift+P



Restore Previous Session

Zoom



100%



Edit



Library



Logins and Passwords



Add-ons

Ctrl+Shift+A



Options



Customize...

[Guida alla progettazione della soluzione](#)
[Guida di installazione e aggiornamento](#)

12.6(2)

[Guida alla progettazione della soluzione](#)
[Guida di installazione e aggiornamento](#)

[Documentazione e supporto tecnico – Cisco Systems](#)

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).