Configurar e solucionar problemas de Live Data em um ambiente UCCE

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Informações de Apoio

- Verificações de conectividade de dados em tempo real com roteador e PG
- Failover do Servidor de Dados ao Vivo
- Failover de TIP
- Failover de SocketIO

Verificações de pré-configuração

Etapas de configuração do Live Data para implantações do UCCE

Checklist de Troubleshooting

- Passo 1: Verificar Status do Serviço Live Data
- Passo 2: Verificar a Conectividade de Dados ao Vivo com o AW
- Passo 3: Verificar o Estado do Cluster de Dados ao Vivo Usando o comando - show live-data failover
- Passo 4: Verificar Configuração da Fonte de Dados Live Data
- Passo 5: Verificar o status da fonte de dados do Live Data no CUIC
- Passo 6: Verificar a conectividade de porta em servidores de dados dinâmicos
- Passo 7: Verificar a Conectividade de Portas em Servidores ICM
- Passo 8: Verificações adicionais

Logs necessários para solucionar problemas de dados dinâmicos

- Dos servidores do ICM
  - Router
  - PG
- Nos servidores LiveData
  - Usando RTMT
  - Usando CLI
- Dos servidores CUIC
  - Usando RTMT
  - Usando CLI
- Console do navegador e registros de rede
- Captura do pacote

Informações Relacionadas

Introdução

Este documento descreve as etapas necessárias para configurar e solucionar problemas de Live Data em um ambiente Unified Contact Center Enterprise (UCCE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Enterprise (UCCE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do ICM: 12.6
- Versão do Finesse: 12.6
- Versão do CUIC/Live Data: 12.6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Live Data é uma estrutura de dados que processa eventos em tempo real com alta disponibilidade para relatórios de Live Data. Os Dados dinâmicos processam continuamente eventos de agentes e chamadas do gateway periférico e do roteador. À medida que os eventos ocorrem, o Live Data envia continuamente atualizações em tempo real para os clientes de relatórios do Unified Intelligence Center. O PG e o Roteador enviam eventos de chamada e de agente para Live Data à medida que os eventos ocorrem. Os Live Data agregam e processam continuamente os eventos em fluxo e publicam as informações. O CUIC se inscreve no fluxo de mensagens para receber os eventos em tempo real e atualizar continuamente os relatórios de dados dinâmicos. Valores de estados individuais, como estados de agentes, são atualizados à medida que ocorrem. Outros valores, como chamadas na fila, são atualizados aproximadamente a cada 3 segundos.

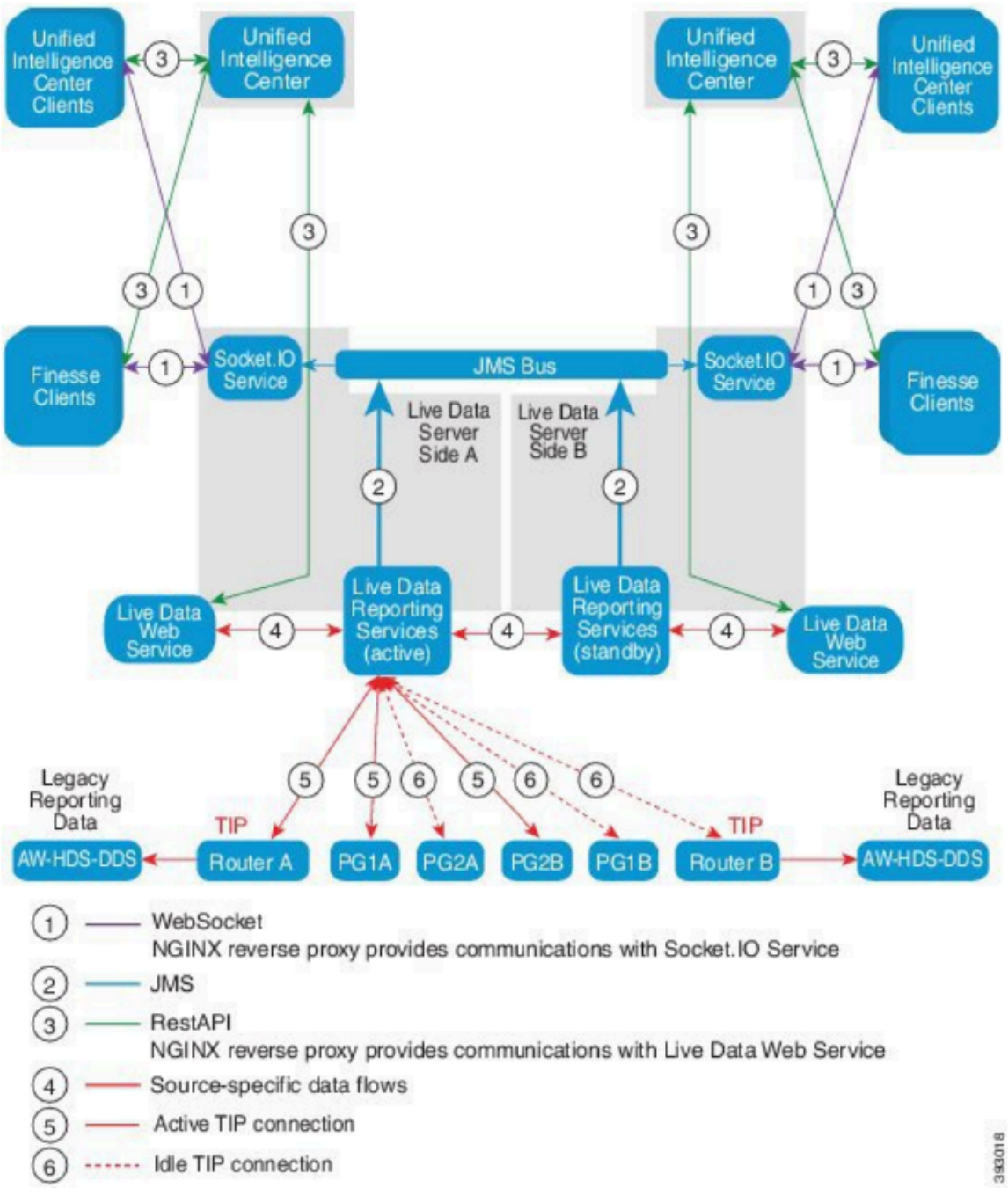
No Unified CCE, o Live Data reside em uma máquina virtual (VM) do sistema operacional de voz da Cisco. Você pode incorporar relatórios de Dados dinâmicos em áreas de trabalho de agentes do Finesse.

Para implantações do Agente 2000:

- O servidor Live Data é instalado em uma VM com o Cisco Unified Intelligence Center (CUIC) e o Cisco Identity Service (IdS)

Para implantações de agente 4000 e superiores:

- O servidor Live Data é instalado em uma VM autônoma.



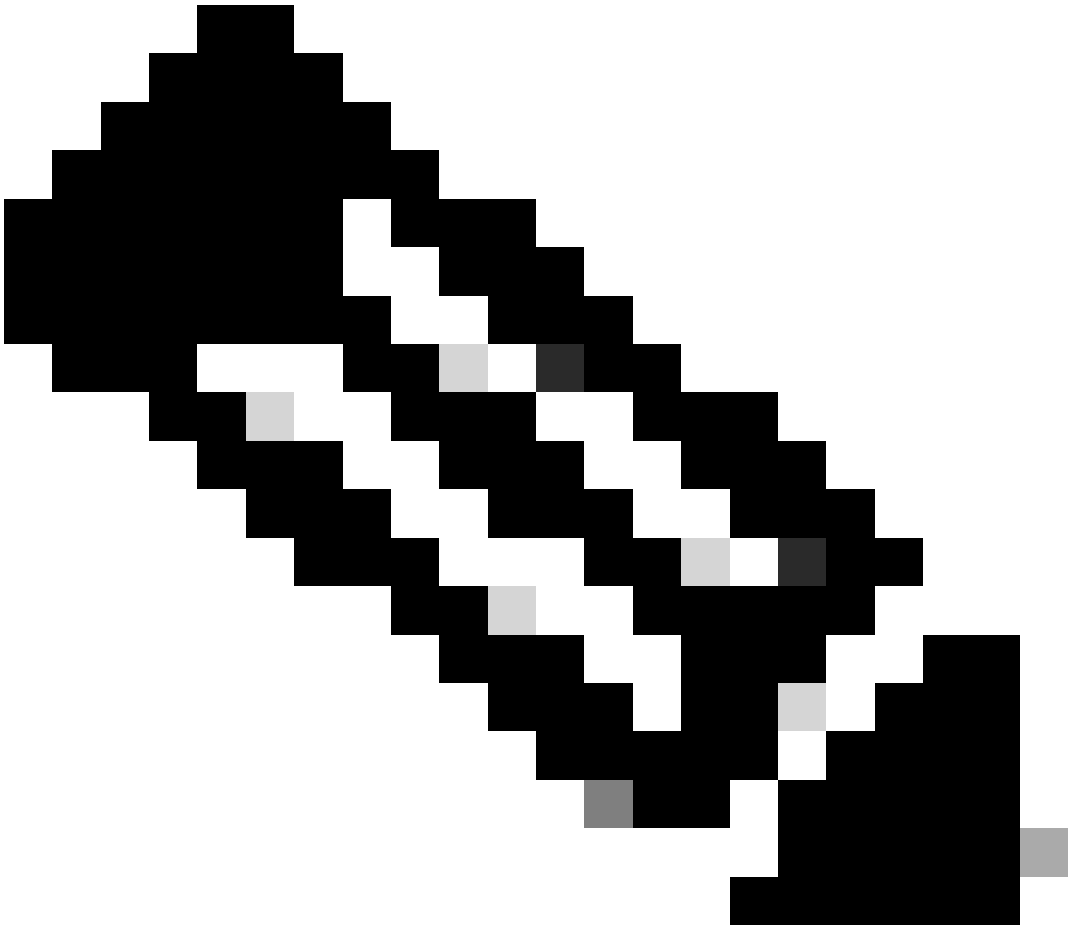
Verificações de conectividade de dados em tempo real com roteador e PG

O servidor de Live Data ativo deve estabelecer conexões TIP e TOS com os Roteadores e com todos os PGs do Agente. O servidor de Live Data inativo (em espera) deve estabelecer apenas a conexão TOS com os Roteadores e com todos os PGs do Agente.

- A porta do roteador/PG para conexão TIP tem o formato conforme este regexp: 4[0-5]034 (Isso pressupõe que haja apenas uma instância do CCE. Por exemplo, 40034, 41034,

42034...)

- A porta do roteador/PG para conexão TOS tem o formato conforme este regexp: 4[0-5]035 (Isso pressupõe que haja apenas uma instância do CCE. Por exemplo, 40035, 41035, 42035...)



Note:

- As portas para conexões TIP/TOS são atribuídas com base na ordem em que o par PG (lado A/B) é instalado no mesmo servidor.
- Por exemplo, o primeiro par PG (PG1 Lado A/B) instalado recebe as portas de base TIP 42034 e 43034, respectivamente. O segundo par PG (PG2 Lado A/B) instalado recebe as portas 44034 e 45034, respectivamente. A mesma atribuição também se aplica às portas TOS.
- As portas TIP e TOS podem variar com base no número da instância; para obter mais detalhes, consulte o Guia de utilização de porta para soluções Cisco Unified Contact Center.

Failover do Servidor de Dados ao Vivo

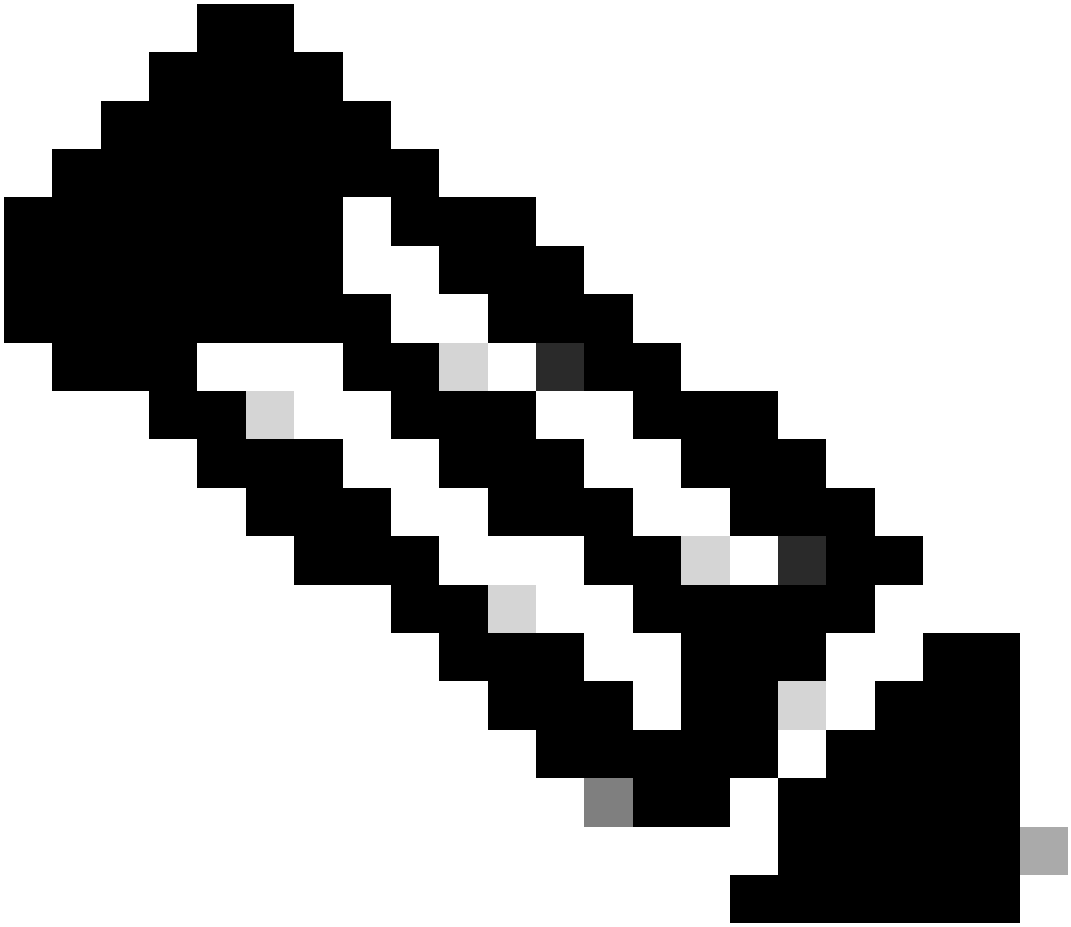
Os servidores Live Data funcionam no modo de espera ou com ativação forçada. Apenas um servidor Live Data está ativo por vez. O outro servidor Live Data está em espera. O servidor de Live Data em standby monitora constantemente o status do servidor ativo. Quando o servidor ativo falha, o servidor em espera assume e torna-se ativo. O servidor com falha torna-se o servidor em espera quando está pronto para servir.

Failover de TIP

O Live Data usa o protocolo de transporte TIP para se comunicar com o Roteador e os servidores PG. O servidor ativo de Live Data estabelece conexões TIP para ambos os lados do Roteador e dos PGs. O servidor Live Data em standby não estabelece nenhuma conexão TIP. Apenas uma conexão TIP está ativa por vez, para o Lado A ou para o Lado B. Quando a conexão TIP ativa falha, o servidor Live Data ativo recupera a conexão TIP ociosa.

Failover de SocketIO

Um cliente SocketIO se conecta a um dos lados do servidor Live Data para receber o fluxo de eventos do relatório Live Data (fluxo SocketIO). Os clientes do Unified Intelligence Center são um exemplo de um cliente SocketIO. O servidor Live Data em standby também produz o fluxo de SocketIO por proxy a partir do servidor ativo. As perdas de pulsação do cliente SocketIO resultam em uma falha de conexão SocketIO. O cliente SocketIO então executa o failover para o outro servidor Live Data.



Note: Quando ocorre um failover de Live Data devido a qualquer um dos motivos mencionados e o servidor de Live Data em espera assume como o servidor ativo, os relatórios de Live Data existentes e as métricas de relatórios são redefinidos.

Verificações de pré-configuração

Antes de implantar Dados dinâmicos, execute estas verificações:

Verificação 1

Nos servidores ICM, verifique a Pesquisa DNS Reversa e Encaminhamento para o Publicador de Dados ao Vivo e o Assinante, usando o comando nslookup.

<#root>

```
nslookup
```

```
nslookup
```

Verificação 2

Na CLI do servidor de dados em tempo real, verifique a pesquisa de DNS reverso e encaminhado para os roteadores e PGs (execute verificações para os lados A e B).

<#root>

```
utils network host
```

Substitua <FQDN> pelos FQDNs públicos dos Roteadores/PGs

<#root>

```
utils network host
```

Substitua <IP> pelo endereço IP público dos Roteadores/PGs (verifique os lados A e B)

Verificação 3

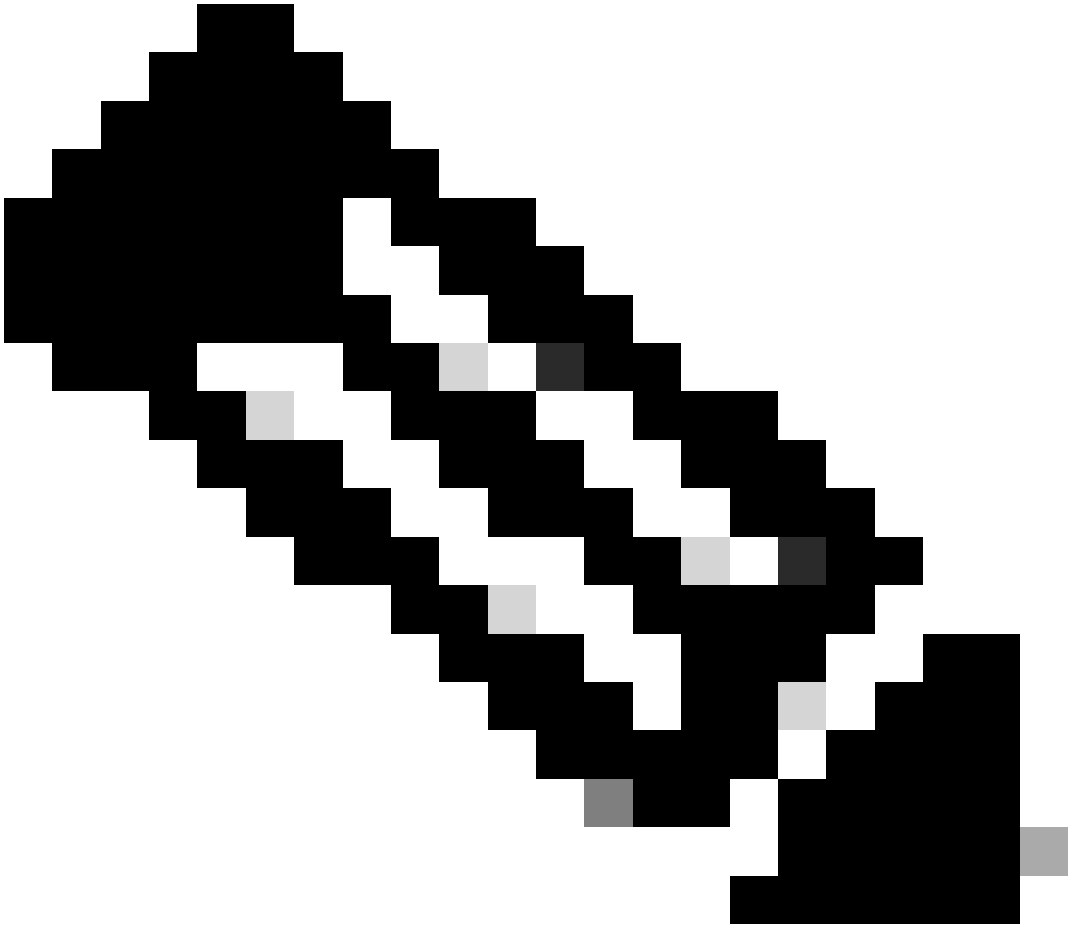
Verifique as configurações e os requisitos de NTP para um ambiente CCE. Consulte a seção NTP e Sincronização de Tempo no Guia de Design da Solução CCE.

Verificação 4

Verifique se os limites de configuração estão sendo seguidos de acordo com o Guia de design da solução CCE.

- Limites de Agente e Supervisor como: Agentes configurados por PG, Agentes por equipe,

Número de agentes é um grupo de habilidades, etc. Consulte o Guia de design da solução CCE para obter mais detalhes.

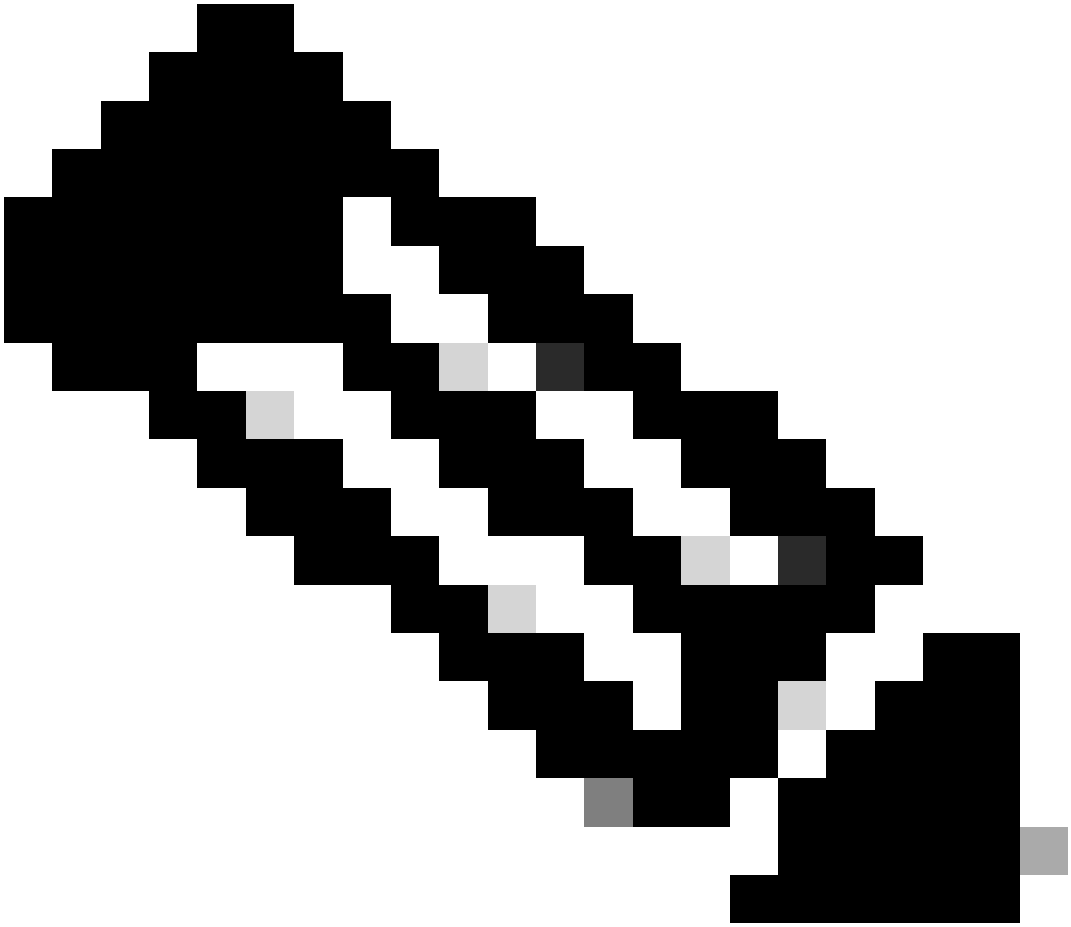


Note:

- Se os servidores Live Data não forem implantados de acordo com o guia de design (co-residentes vs autônomos) ou se as limitações de configuração forem excedidas, o serviço Live Data pode ficar fora de serviço.
- Para evitar problemas com o serviço Live Data, é recomendável que a versão do Live Data Server corresponda à versão exata do ICM para essa implantação.

Verificação 5

Troca de certificados para Live Data em uma implantação de UCCE.



Note: Se os certificados assinados por CA estiverem sendo usados na implantação do CCE - ICM, Finesse, CUIC, LD e IdS - (assinados pela mesma Autoridade de Certificação), essa verificação poderá ser ignorada.

Ao usar certificados autoassinados:

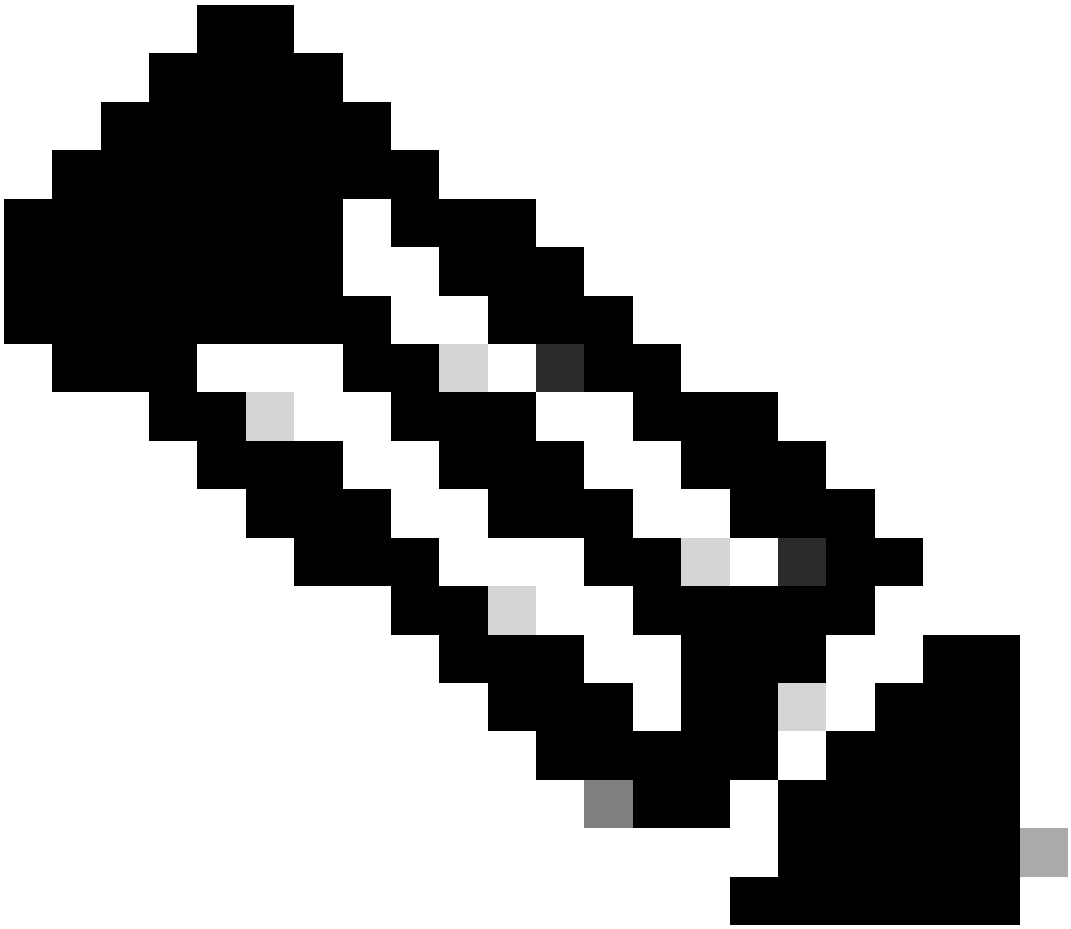
Para implantações de agentes do 2000:

- Verifique se os certificados tomcat dos servidores editor e assinante CUIC-LD-IdS foram carregados no editor Finesse como tomcat-trust.
- Verifique se os certificados tomcat dos servidores do editor e do assinante do Finesse foram carregados no servidor do editor CUIC-LD-IdS como tomcat-trust.
- Verifique se os certificados tomcat dos servidores editor e assinante CUIC-LD-IdS foram carregados em todos os servidores AW.

Para implantações de agente 4000 e 12000:

- Verifique se os certificados tomcat dos servidores do editor de dados ao vivo e do assinante foram carregados no editor CUIC e no editor Finesse como tomcat-trust.
- Verifique se os certificados tomcat dos servidores do editor e do assinante CUIC foram carregados no editor de dados dinâmicos e no editor Finesse como tomcat-trust.
- Verifique se os certificados tomcat dos servidores do editor e do assinante do Finesse foram carregados no editor do CUIC e no editor de dados dinâmicos como tomcat-trust.

- Verifique se os certificados tomcat de todos os servidores CUIC, Live Data e Finesse estão carregados em todos os servidores AW.
- Verifique se o certificado IIS dos servidores AW foi carregado para o servidor do Publicador de Dados ao Vivo como tomcat-trust.



Note:

- Os certificados carregados como tomcat-trust no servidor do Publicador são replicados no nó Assinante nesse mesmo cluster.

- Quando um certificado é carregado em um servidor VOS, uma reinicialização completa do servidor usando o comando CLI utils system restart é necessária para que o certificado recém-carregado tenha efeito nesse servidor.
- Para servidores AW, uma reinicialização do serviço Apache Tomcat é necessária para que o certificado recém-carregado tenha efeito nesse servidor AW.

Verificação 6

Você DEVE usar o FQDN (nome de domínio totalmente qualificado) para todos os comandos de configuração do Live Data. O uso do endereço IP ao configurar Live Data pode causar problemas com o serviço Live Data.

Verificação 7

a. Para todos os comandos set Live Data, digite manualmente as senhas em vez de uma ação copiar e colar.

b. Conjunto de caracteres com suporte para comandos CLI de instalação de dados dinâmicos

Ao trabalhar com a CLI (e não exclusivamente para Live Data), você pode usar caracteres alfanuméricos simples [0-9] [A-Z] [a-z] e estes caracteres adicionais:

- ". " (ponto)
- "!" (ponto de exclamação)
- "@" (no sinal)
- "#" (sinal numérico)
- "$" (dólar)
- "%" (porcentagem)
- "^" (acento circunflexo)
- "*" (estrela)
- "_" (sublinhado)
- "+" (sinal de mais)
- "=" (sinal de igual)
- "~" (til)
- ":" (dois-pontos)
- "(" e ")" (parênteses de abertura e fechamento)
- "{" e "}" (colchetes de abertura e fechamento)
- "[" e "]" (colchetes de abertura e fechamento)
- Os espaços são usados como separadores de entrada. A maioria dos caracteres especiais possui significado específico para o console de comando do Cisco Voice Operating System (VOS) (por exemplo, "\", "|" e assim por diante). Caracteres além do ASCII padrão são ignorados em sua maioria.

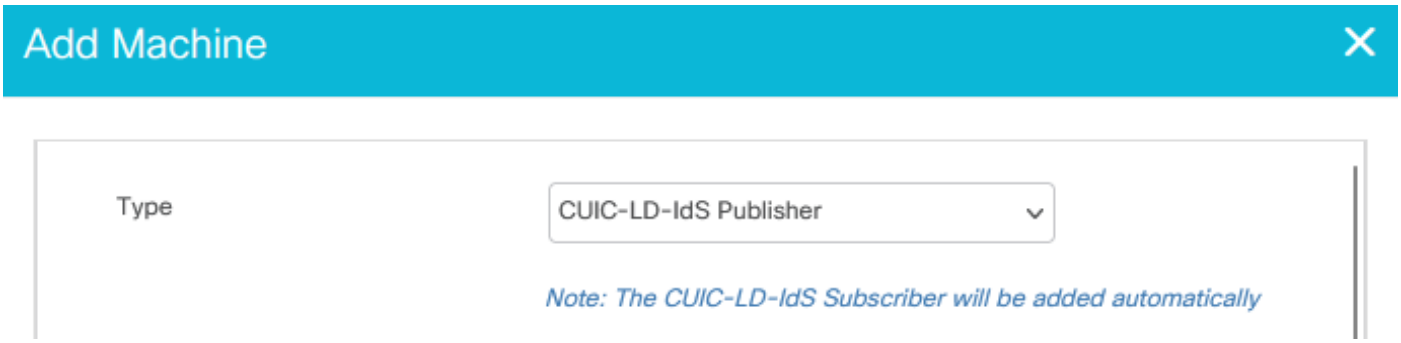
Etapas de configuração do Live Data para implantações do

UCCE

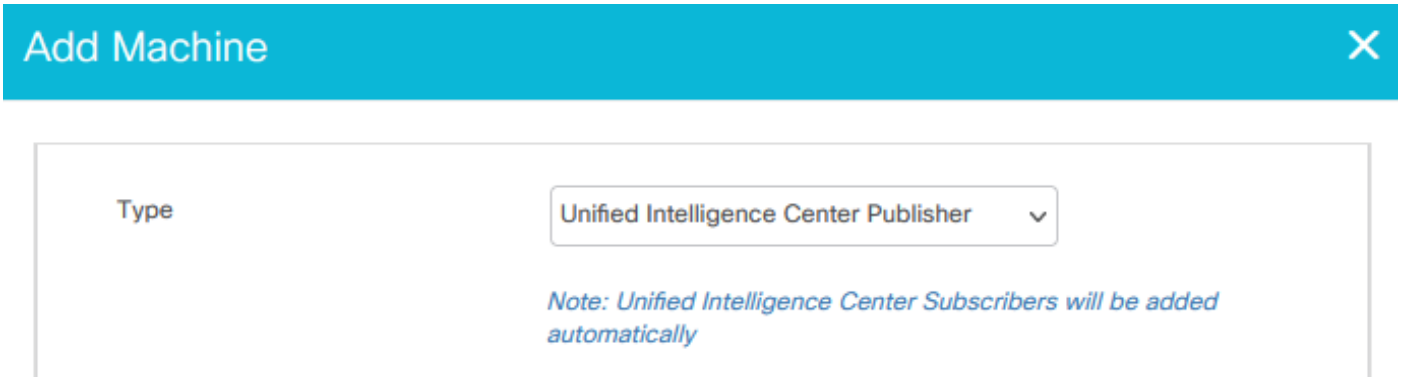
Passo 1
Verifique se o tipo de implantação correto está definido na Administração do CCE em Infraestrutura > Configurações de implantação (https://<AW-Server>/cceadmin).

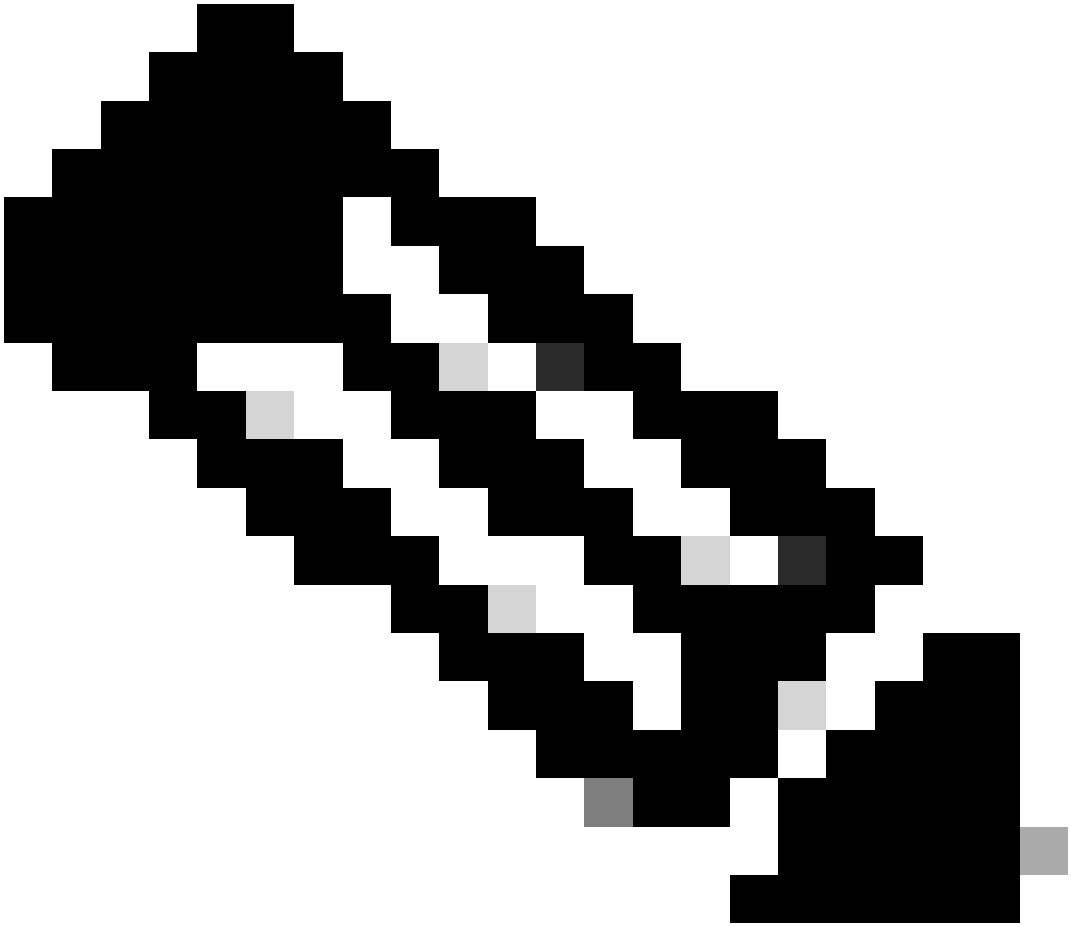
Passo 2
Adicione o servidor ao inventário do CCE.

Para implantações do 2000 Agent, adicione o cluster co-residente CUIC-LD-IdS selecionando a opção Publicador CUIC-LD-IdS.



Para implantações de agente 4000 e superiores, adicione o cluster CUIC autônomo selecionando a opção Editor do Unified Intelligence Center.





Note: Para implantações de agentes 4000 e superiores, os servidores Live Data são adicionados ao Inventário usando o comando set live-data machine-services.

Etapa 3
Use o comando set live-data reporting-interval <reporting-interval-in-minutes> para definir o intervalo de relatório de dados dinâmicos em minutos.

- Os intervalos válidos são: 5 (padrão), 10, 15, 30 e 60.
- Uma reinicialização do cluster de Dados dinâmicos será necessária se e quando esse valor for modificado.

Use o comando show live-data reporting-interval para exibir a configuração atual do intervalo de relatório.

Passo 4

Configure um usuário SQL no AW DB para trabalhar com Live Data.

No servidor primário e secundário do AW DB > inicie o SQL Server Management Studio (SSMS):

- Crie um usuário com a associação de atribuição de banco de dados db_datareader e db_datawriter na configuração Mapeamento de Usuário do banco de dados awdb.
- A atribuição de banco de dados public é verificada por padrão. Essa função é necessária para usuários do CUIC, Finesse e Live Data.

Etapa 5
Execute a consulta SQL para o usuário SQL configurado para trabalhar com Live Data.

```
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "


        "


GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "


        "
```

Substitua <user> pelo nome de usuário do usuário criado na Etapa 4.

Etapa 6
Configurar Live Data com AW.

<#root>

```
set live-data aw-access primary
```

```
set live-data aw-access secondary
```

Where:

- porta: Porta SQL (por padrão, o Mecanismo de Banco de Dados do SQL Server escuta na porta TCP 1433)
- banco de dados aw: awdb
- sql-user: Usuário SQL criado no AW DB (etapa 4)

Esse comando informa ao Live Data como acessar o AW DB primário e o AW DB secundário. O comando também testa automaticamente a conexão do Live Data com o AW primário ou secundário, verifica se o usuário configurado tem acesso apropriado ao AW DB e relata os resultados. (O status do teste deve mostrar Êxito). Não é necessário configurar o AW DB nos servidores do Publicador de Dados ao Vivo e do Assinante. A configuração é replicada entre o Publicador de Dados ao Vivo e o nó Assinante.

Para visualizar os BDs AW primário e secundário configurados, use o comando:

<#root>

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

Etapa 7

Conecte servidores de dados dinâmicos a registros de Serviço de Máquina (somente para

implantações de Agente 4000 e superiores).

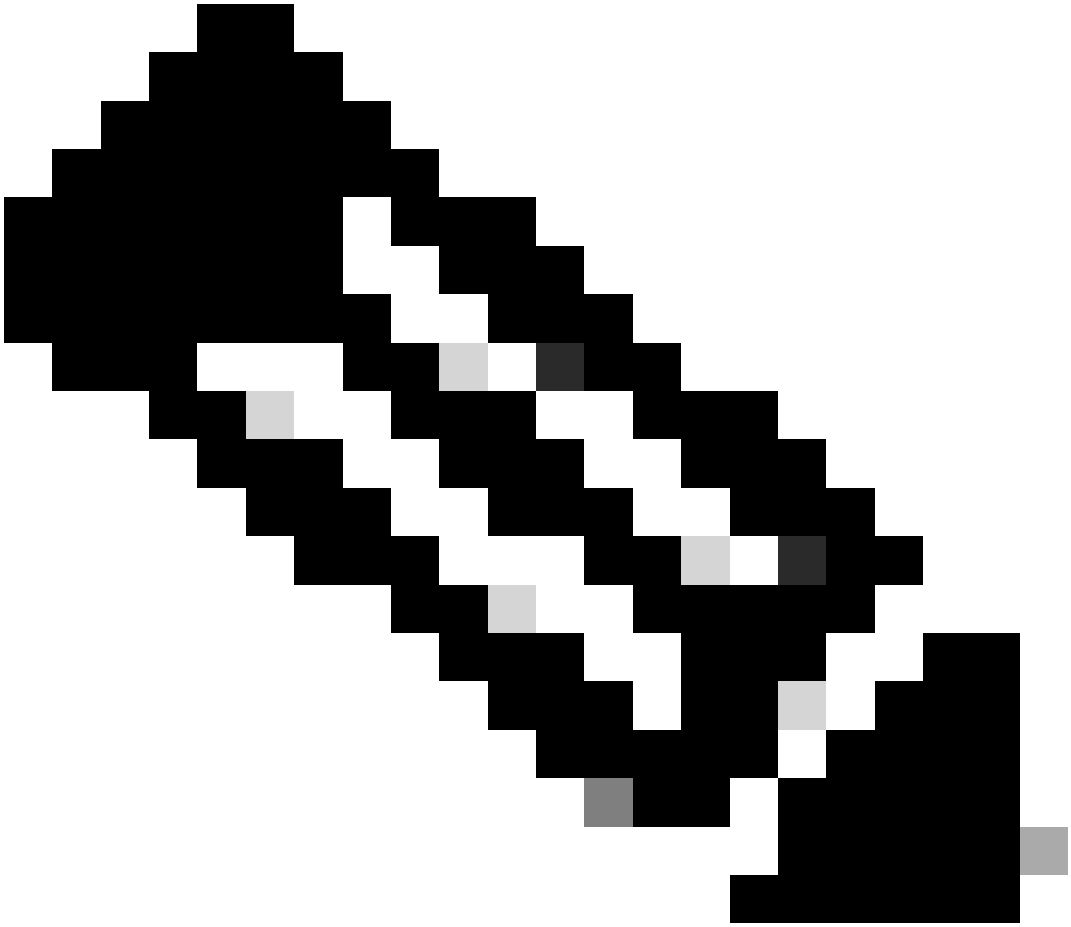
<#root>

```
set live-data machine-services
```

Esse comando permite que os servidores LD se registrem na tabela de serviços de máquinas para que os servidores LD sejam detectáveis. Isso também registra as credenciais para chamar a API Live Data.

Requisitos que o usuário deve ter para executar o comando de serviços da máquina com êxito:

- Deve ser um usuário de domínio.
- Deve estar em um formato de Nome UPN. Exemplo: admin@stooges.cisco.com.
- É necessário ter permissão de acesso de gravação nas tabelas do Computador.
- Deve ser autorizado a alterar a configuração do Unified CCE.



Note:

- Quando você executa esse comando, ele solicita que você especifique a senha de login para user@domain, a ser usada para autenticação com acesso ao banco de dados AW. Ele também solicita que você especifique a senha do usuário conectado para a sessão CLI atual.
- Para implantações do 2000 Agent, o serviço Live Data que faz parte de um cluster co-residente, é adicionado ao Inventário quando os nós co-residentes são adicionados, selecionando a opção CUIC-LD-IdS Publisher na Etapa 2. E, portanto, não precisa de um comando set live-data machine-services <user@domain>.

Passo 8
Configure a fonte de dados Live Data no CUIC.

<#root>

```
set live-data cuic-datasource
```

```
CUIC\
```

Where:

- porta cuic = 8444
- cuic-user = Usuário do aplicativo CUIC (credenciais de login de superusuário)

Quando esse comando for executado com êxito, as fontes de dados primárias e secundárias do Live Data poderão ser vistas na guia Fontes de dados na GUI do CUIC.

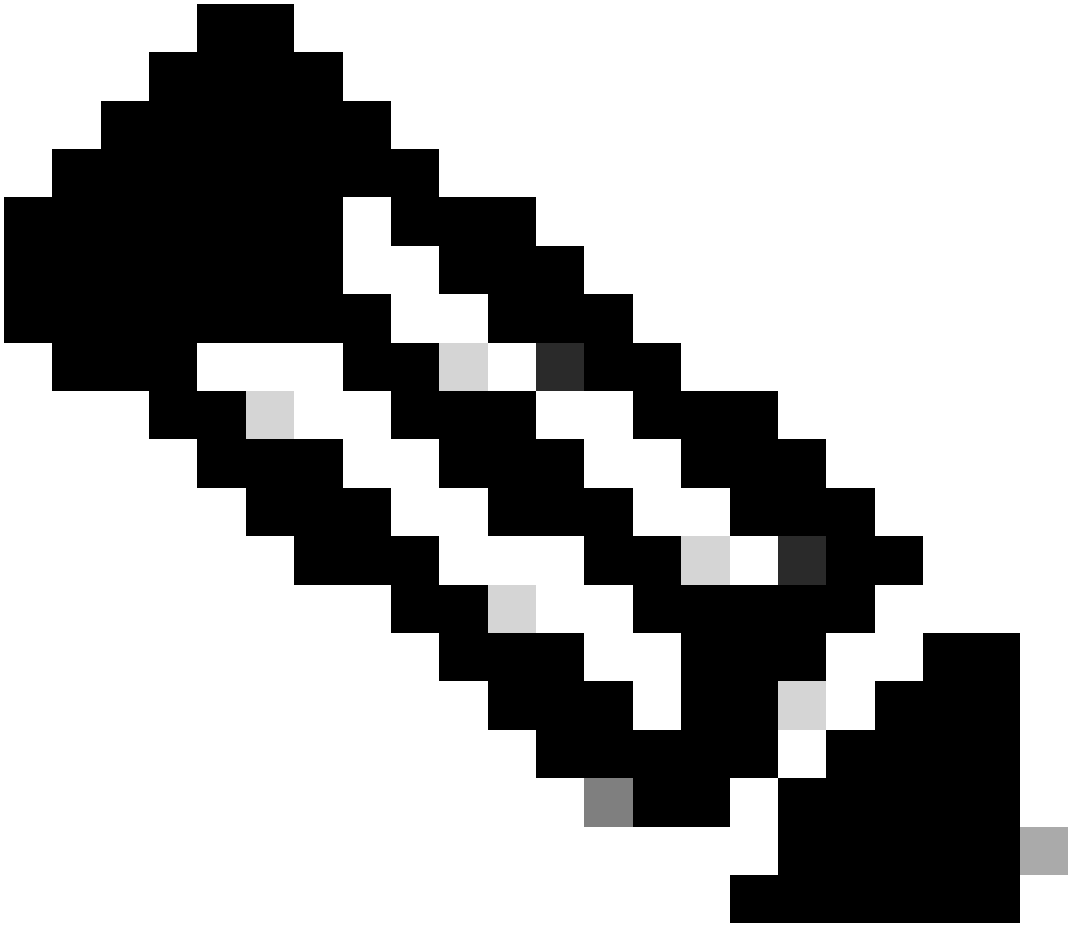
Para exibir a configuração da fonte de dados Live Data, use o comando:

<#root>

```
show live-data cuic-datasource
```

```
CUIC\
```

Passo 9
Baixe os relatórios de Dados dinâmicos de cisco.com e importe os relatórios de Dados dinâmicos para o servidor CUIC.



Note: Os relatórios de Dados dinâmicos DEVEM corresponder à versão do seu controlador central.

Passo 10
Na página Cisco Finesse Administration (https://<Finesse>/cfadmin), navegue até a guia Finesse Desktop Layout e substitua o my-cuic-server padrão pelo FQDN do servidor CUIC correto.

Passo 11
Configure o Compartilhamento de Recursos entre Origens (CORS) para Dados Dinâmicos.

a. No Finesse Publisher e Subscriber, verifique se o CORS está habilitado usando o comando utils finesse cors status.

Se estiver desabilitado, você poderá habilitá-lo usando o comando utils finesse cors enable.

b. Execute os comandos CORS em todos os servidores CUIC:

<#root>

```
utils cuic cors enable

utils cuic cors allowed_origin add https://




utils cuic cors allowed_origin add https://




utils cuic cors allowed_origin add https://

        :8445

utils cuic cors allowed_origin add https://

        :8445
```

c. Execute os comandos CORS nos servidores do Publicador de Dados ao Vivo e do Assinante:

<#root>

```
utils live-data cors enable

utils live-data cors allowed_origin add https://




utils live-data cors allowed_origin add https://




utils live-data cors allowed_origin add https://

        :8445

utils live-data cors allowed_origin add https://
```

```
:8445
```

d. Para verificar a configuração do CORS:

Em todos os servidores CUIC:

<#root>

```
utils cuic cors status
```

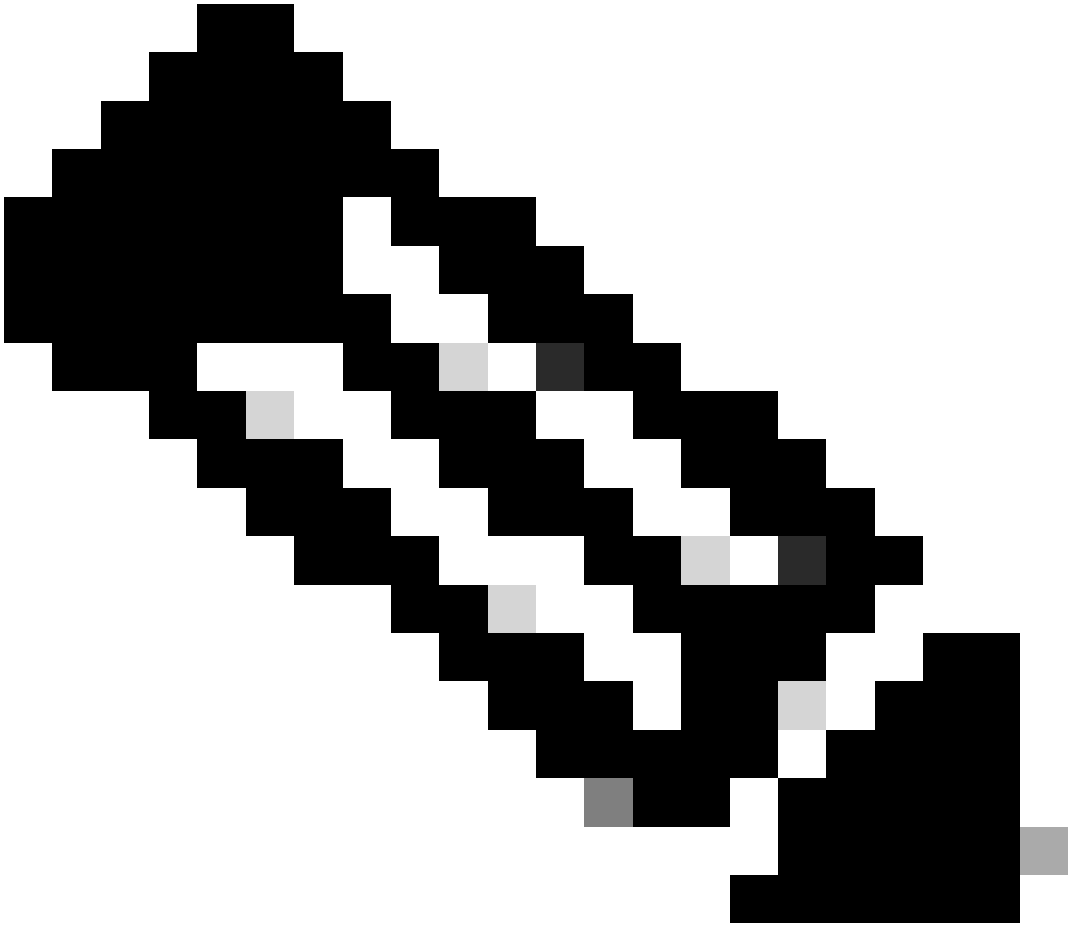
```
utils cuic cors allowed_origin list
```

No Publicador e Assinante do Live Data:

<#root>

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

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



Note:

- Para implantações co-residentes, o conjunto de comandos utils cuic cors e utils live-data cors precisa ser executado nos servidores co-residentes do Publicador e do Assinante.
- Para implantações autônomas, o conjunto de comandos utils cuic cors deve ser executado em todos os nós CUIC no cluster CUIC e o conjunto de comandos utils live-data cors deve ser executado nos servidores do Publicador de Dados ao Vivo e do Assinante.

Etapa 12
Reinicie todos os servidores CUIC/LD e Finesse usando o comando CLI:

<#root>

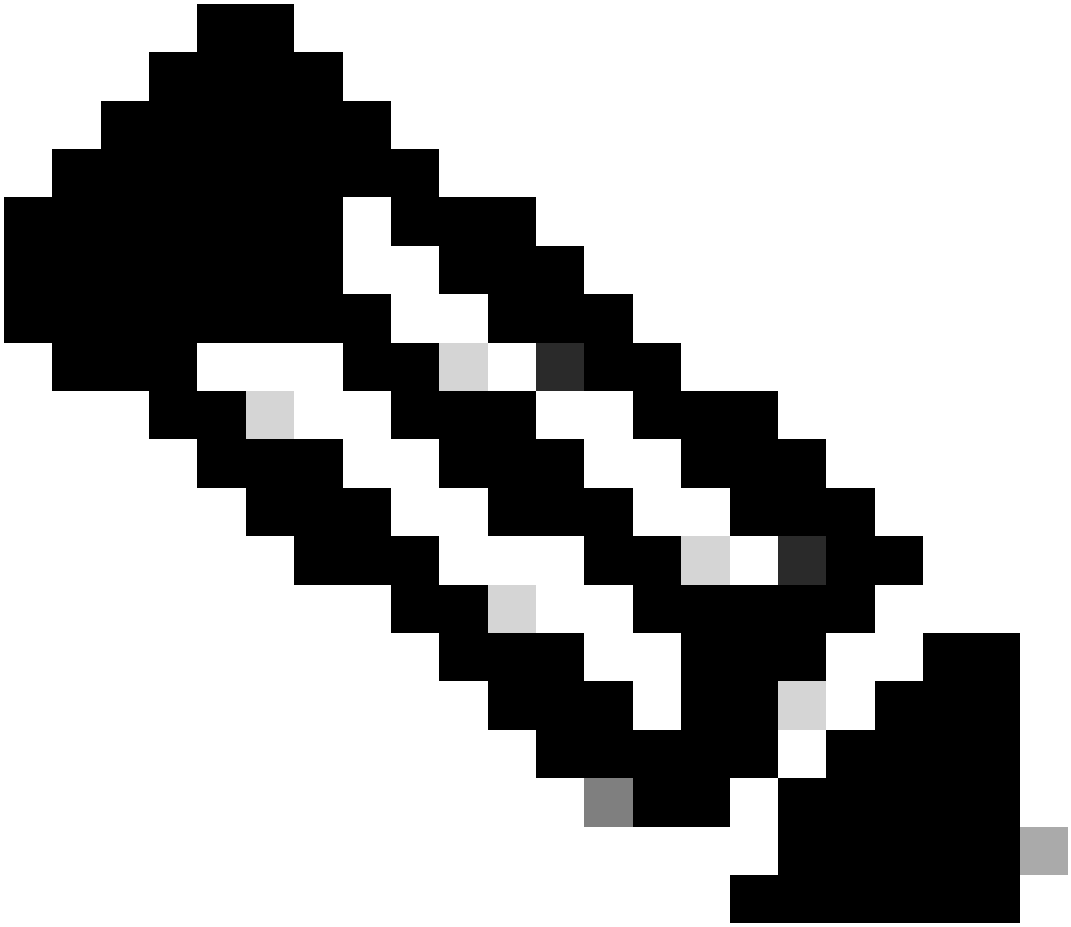
```
utils system restart
```

Checklist de Troubleshooting

Passo 1: Verificar Status do Serviço Live Data

Certifique-se de que todos os serviços Live Data sejam INICIADOS usando o 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]
```



Note:

- A partir da versão 15.0, o componente Cassandra foi removido do servidor Live Data. As informações de acesso ao AW agora são armazenadas na tabela de banco de dados platform informix - mmca_propertydef
- As referências a Cassandra foram removidas da lista do gerenciador de serviços do ServM, RTMT e caminho da pasta de registro.
- Para exibir a configuração do awdb, execute o comando 'run sql select * from mca_propertydef' na CLI do servidor Live Data.

Passo 2: Verificar a Conectividade de Dados ao Vivo com o AW

Assegure a conectividade com os servidores AW usando o comando:

<#root>

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

O status do teste deve mostrar Êxito.

Passo 3: Verificar o Estado do Cluster de Dados ao Vivo Usando o comando - show live-data failover

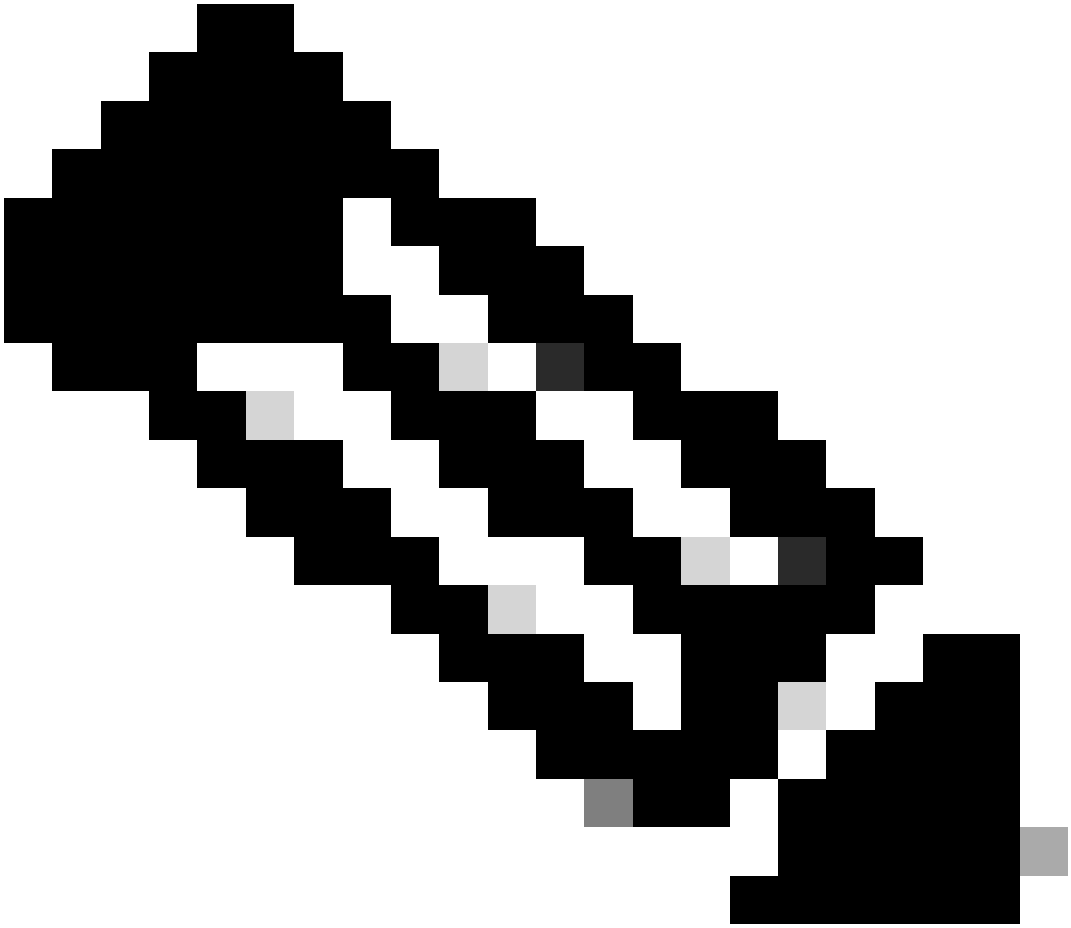
Verifique o estado do Cluster de Dados Dinâmicos usando o comando:

<#root>

```
show live-data failover
```

Estado do Cluster	Descrição
EMPARELHADO-ATIVO	O servidor Live Data está no estado ativo e se comunica com o lado remoto.
EMPARELHADO - EM ESPERA	O servidor Live Data está no estado de espera e se comunica com o lado remoto.
ISOLADO-ATIVO	O servidor Live Data está no estado ativo, mas não pode se comunicar com o lado remoto.
ISOLATED-STANDBY	O servidor de Live Data está no estado de espera, mas não pode se comunicar com o lado remoto.
MODO SIMPLIFICADO	O servidor Live Data está funcionando no modo simplex.
FORA DE SERVIÇO	O servidor Live Data está fora de serviço.
CONECTANDO	O servidor Live Data está tentando fazer um handshake com o lado remoto.
TESTANDO	O servidor de Dados dinâmicos não pode se comunicar com o lado remoto e está usando o procedimento Test-Other-Side para determinar se deve estar no estado ISOLATED-ATIVE ou ISOLATED-STANDBY.

INDISPONÍVEL	O Live Data não foi implantado.



Note: O status ISOLADO ativo/em espera indica uma comunicação entre servidores Live Data. Isso não faz com que a fonte de dados Live Data no CUIC fique offline.

a. Se o comando show live-data failover mostrar o estado do cluster como INDISPONÍVEL.

- Este status indica que os Dados dinâmicos não foram implantados com êxito devido a configurações incompletas.

Itens de ação:

- Verifique se todas as etapas de configuração foram concluídas com êxito.
- Baixe os logs do CCE Live Data Storm Services usando RTMT e analise o arquivo deployment_control.log.
- Como alternativa, você pode fazer download do arquivo usando o comando CLI file get

ativelog livedata/logs/livedata-storm/deployment_control.log.

b. Se o comando show live-data failover mostrar o estado do cluster como OUT-OF-SERVICE.

- Esse status indica que o Live Data foi implantado com êxito, mas pode haver problemas de conectividade ou os limites de configuração foram excedidos.

Itens de Ação

- Garanta a conectividade de rede entre os servidores Live Data e os Roteadores/PGs (consulte o Guia de utilização de porta do CCE).
- Certifique-se de que o servidor Live Data tenha sido implantado de acordo com o guia de design (co-residente versus autônomo).
- Verifique se os limites de configuração NÃO foram excedidos.
- Baixe e analise os logs do CCE Live Data Storm Services (principalmente o arquivo worker.log).
- Como alternativa, você pode fazer download do arquivo de registro usando o comando CLI file get ativelog livedata/logs/livedata-storm/.

c. Se o comando show live-data failover mostrar o estado do cluster como ISOLADO.

- Esse status indica um problema de conectividade entre os dois servidores Live Data devido ao qual eles não conseguem se comunicar.

Passo 4: Verificar Configuração da Fonte de Dados Live Data

Certifique-se de que a fonte de dados Streaming Live Data reflita os hosts corretos usando o comando:

<#root>

```
show live-data cuic-datasource
```

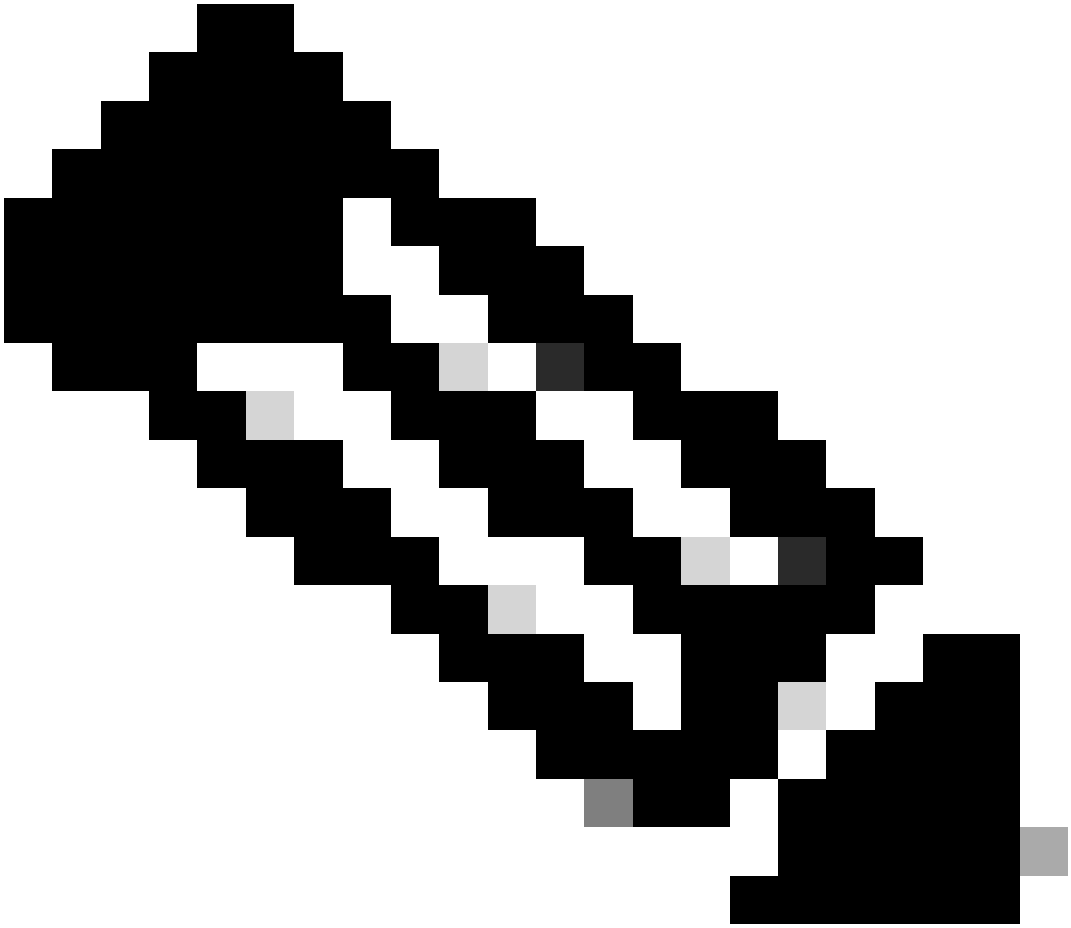
```
CUIC\
```

Passo 5: Verificar o status da fonte de dados do Live Data no CUIC

Se show live-data cuic-datasource mostrar as configurações corretas, mas Live Data Datasource

mostrar offline no CUIC:

- Verifique se as portas do Serviço Web Live Data e do Serviço SocketIO Live Data estão abertas bidirecionalmente entre o servidor Live Data e o navegador.
- Os Serviços CCE Live Data Storm, o Serviço CCE Live Data SocketIO e os logs do Console do navegador podem ajudar a isolar ainda mais a possível causa do problema.



Note: Iniciando o Live Data versão 12.6.2, as portas 12005 e 12008 são preteridas e removidas em versões futuras. A porta 443 agora é usada para o Serviço Web Live Data e o Serviço SocketIO Live Data.

Passo 6: Verificar a conectividade de porta em servidores de dados dinâmicos

Verifique a conectividade de porta da CLI do Live Data Server usando o comando show open ports.

- A saída do Servidor de Dados Dinâmicos ativo deve mostrar 2 conexões estabelecidas com

cada um dos Roteadores e PGs do Agente (para as conexões TIP e TOS).
- A saída do Servidor de Dados Dinâmicos (standby) inativo deve mostrar 1 conexão estabelecida com os Roteadores e os PGs (para as conexões 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)

Passo 7: Verificar a Conectividade de Portas em Servidores ICM

Verifique a conectividade da porta a partir do prompt de comando nos Roteadores e PGs usando o comando netstat.

- A saída deve mostrar as portas no estado ESTABLISHED para o Publicador de Dados ao Vivo e o Assinante.
- A saída deve mostrar 2 conexões ESTABLISHED com o servidor Ative Live Data (para as conexões TIP e TOS).
- A saída deve mostrar 1 conexão ESTABLISHED com o servidor Live Data inativo (em espera) (para as conexões TOS).

<#root>

```
netstat -an | findstr "
```

```
"
```

OR

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

(For Instance-0)

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

(For Instance-1)

a. Se as portas nem mesmo mostrarem estar no estado LISTENING:

- Verifique se o tipo de implantação correto e compatível está definido de acordo com o guia de design.
- Pode ser necessário reiniciar o servidor.

b. Se as portas não estiverem no estado ESTABLISHED e continuarem no estado LISTENING:

- Verifique a conectividade de rede entre os Roteadores/PGs e os servidores Live Data.
- Nos Roteadores/PGs, verifique as pesquisas de DNS direto e reverso para o servidor de dados dinâmicos.
- Nos servidores LiveData, verifique as pesquisas de DNS direto e reverso para os endereços públicos do servidor Roteador/PG.

Passo 8: Verificações adicionais

a. Consulta SQL para verificar o número de agentes configurados por equipe:

Executar consulta no awdb (Sem impacto na produção).

```
Select TeamName = AT.EnterpriseName, NumAgentsOnTeam = COUNT(ATM.SkillTargetID), SupervisorName = Perso
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. Consulta SQL para verificar o número de Agentes configurados por grupo de habilidades:

Executar consulta no awdb (Sem impacto na produção).

```
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 problemas de Live Data forem observados após uma atualização, verifique o valor de configuração de DBMaintenance.

- 0 - habilitado
- 1 - desativado.

Se estiver desabilitado, habilite as alterações de configuração definindo DBMaintenance como 0 e reinicie o serviço Apache Tomcat no AW Server.

Caminho do Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<nome da instância>\Router<A/B>\Router\CurrentVersion\Configuration\Global\DBMaintenance.

Logs necessários para solucionar problemas de dados dinâmicos

Dos servidores do ICM

- Defina a configuração de rastreamento para o processo rtr e opc como nível 1 ou nível 2, dependendo de quão detalhado você deseja que os logs sejam.

Router

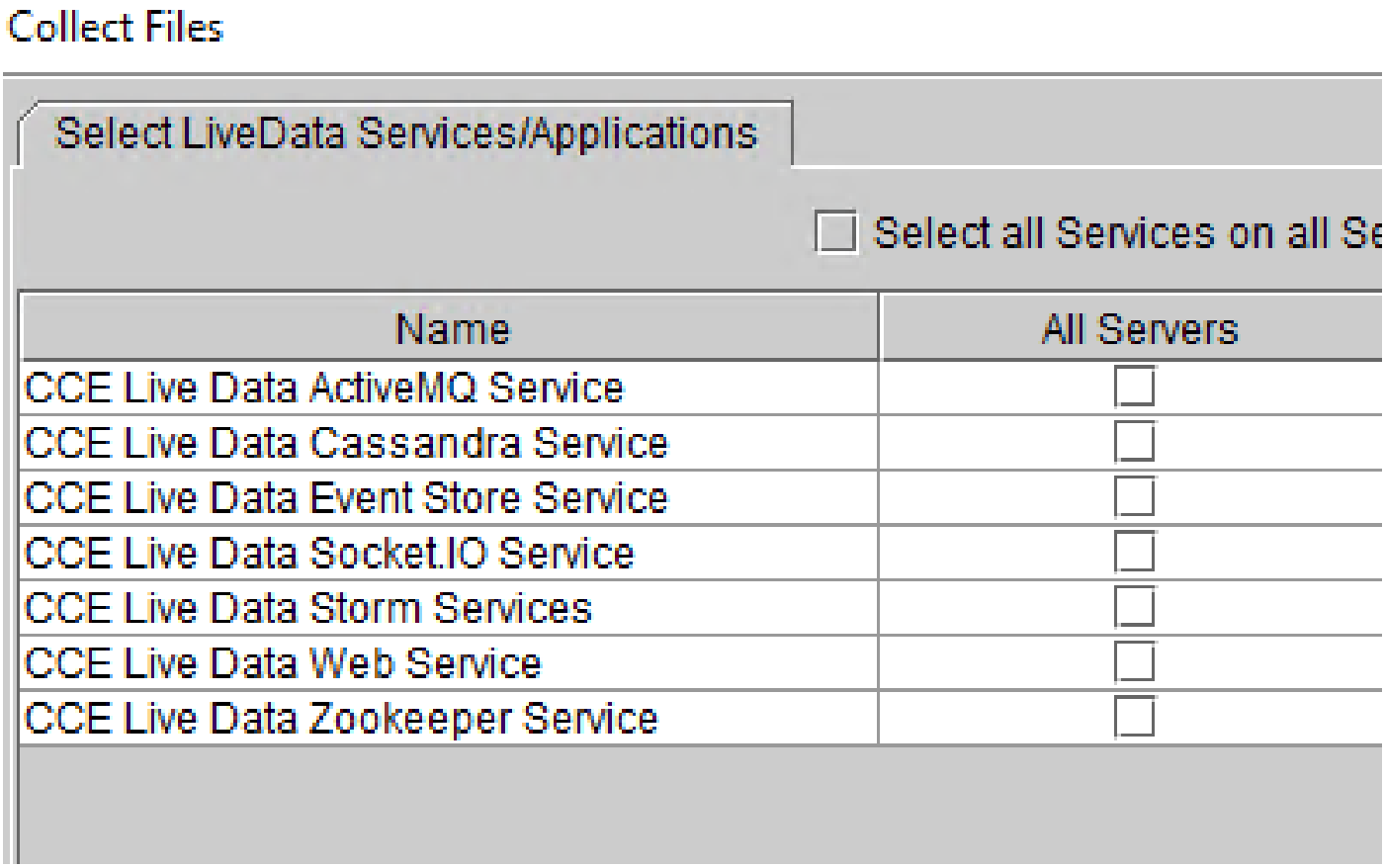
- rtr logs

PG

- logs de opc

Nos servidores LiveData

Usando RTMT



Captura de tela do LD

Usando 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
```

Este comando coleta logs de todos os componentes de Dados dinâmicos

Como alternativa, você também pode coletar logs para os componentes individuais do 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

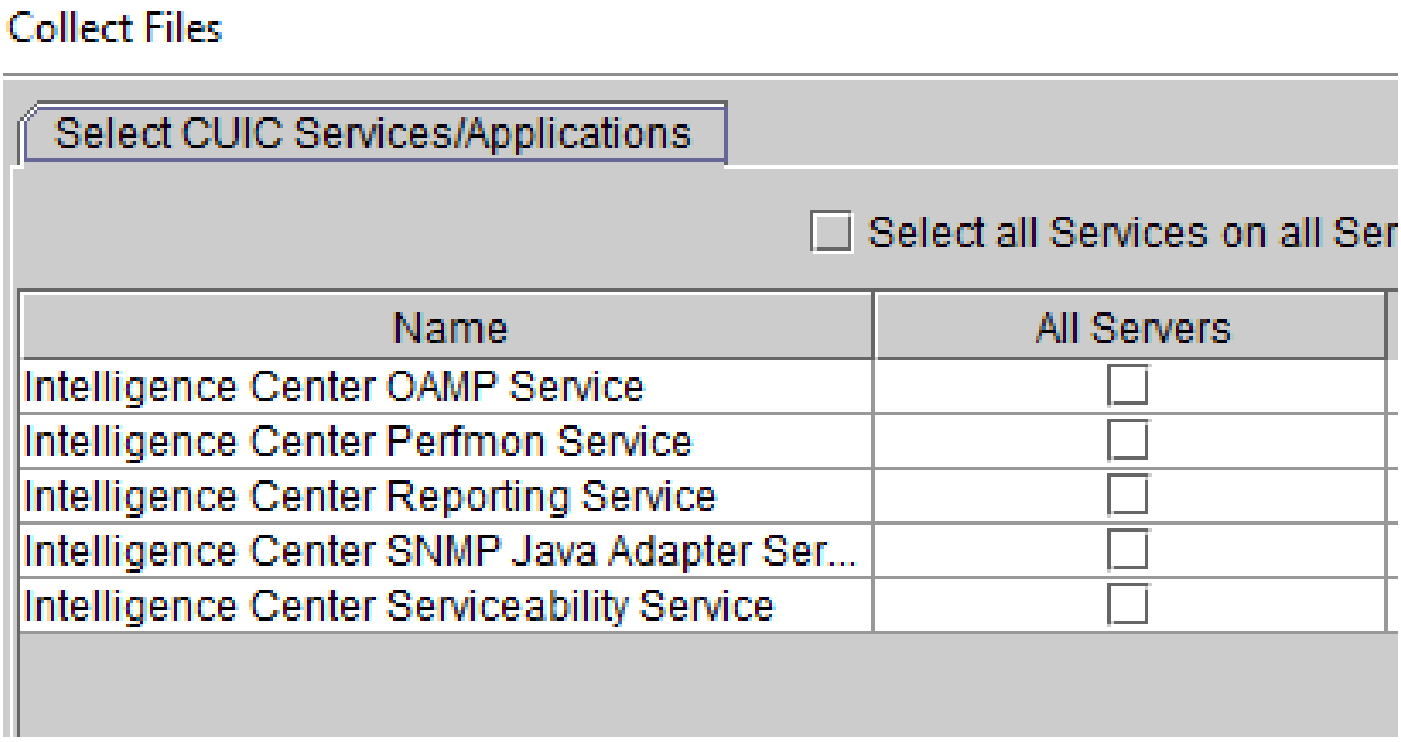
```
file get activelog livedata/logs/livedata-web
```

CCE Live Data Zookeeper Service

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

Dos servidores CUIC

Usando RTMT



Usando CLI

<#root>

```
Intelligence Center Reporting Service
```

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

Console do navegador e registros de rede

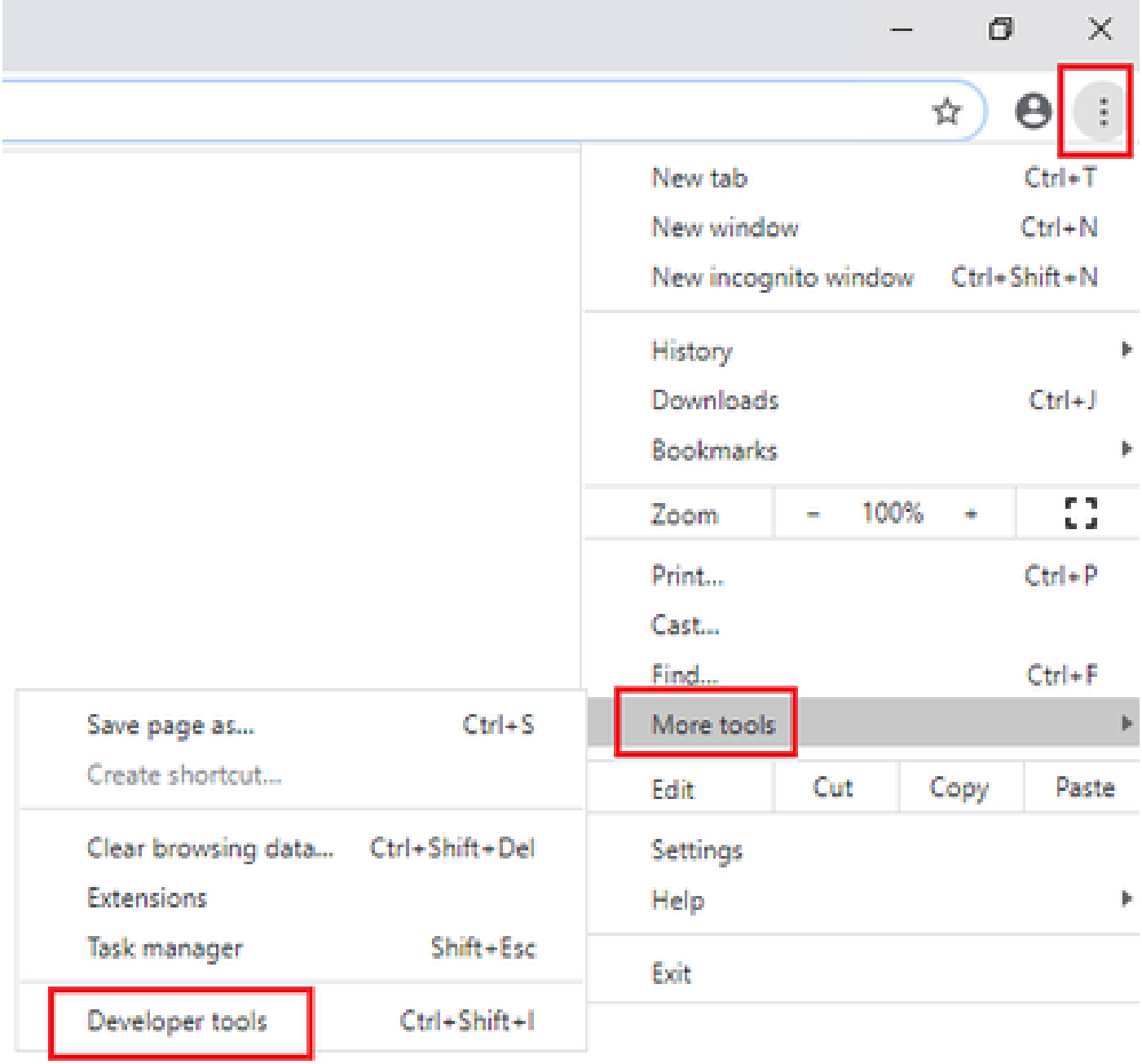
Colete o Console do navegador e os logs de rede para o problema de duração. Comece limpando o Cache, reinicie o navegador e capture os logs a partir do tempo de logon, cobrindo a tentativa feita para reproduzir o problema

Para o navegador Chrome/Edge:

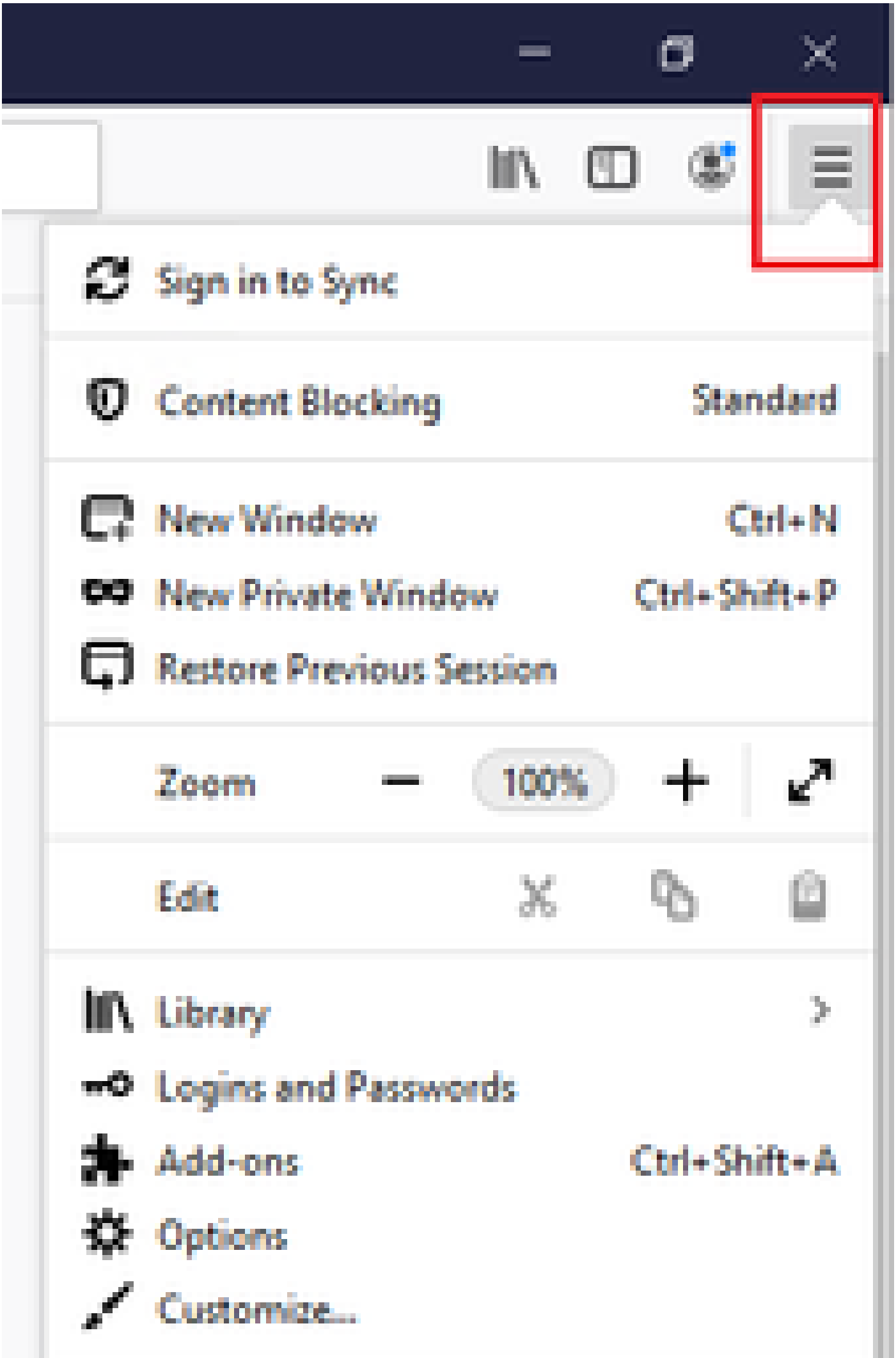
- Clique no ícone Configurações e navegue para Ferramentas do desenvolvedor > Mais ferramentas > Ferramentas do desenvolvedor.
- Em Developer tools > Console tab, clique no símbolo da engrenagem e verifique as opções: Preservar log, Mostrar carimbos de data/hora, Registrar XMLHttpRequests.
- Em Developer tools > Network tab, clique no símbolo gear e marque a opção: Preservar log.
- Feche a página configurações.
- O console e os registros de rede agora podem ser coletados clicando com o botão direito nas respectivas guias e selecionando Salvar tudo como.

Para o navegador Firefox:

- Clique no ícone do menu Aplicativos e navegue para Mais ferramentas > Ferramentas para Desenvolvedor da Web.
- Na guia Rede, clique no símbolo engrenagem e selecione a opção: Logs de Persistência.
- O console e os registros de rede agora podem ser coletados clicando com o botão direito do mouse nas respectivas guias e selecionando Salvar tudo como.



Cromo


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...

Guia de design da solução
Guia de instalação e atualização

12.6(2)
Guia de design da solução
Guia de instalação e atualização

Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.