Definir rastreamentos e coletar logs no CCE

Contents

Introduction

Este documento descreve como definir e coletar rastreamentos no Cisco Unified Contact Center Enterprise (CCE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Enterprise (UCCE)
- Central de Contatos em Pacotes Enterprise (PCCE)
- Cisco Finesse
- Cisco Customer Voice Portal (CVP)

- Cisco Virtualized Voice Browser (VVB)
- Cisco Unified Border Element (CUBE)
- Cisco Unified Intelligence Center (CUIC)
- Proxy Cisco Unified Session Initiation Protocol (SIP) (CUSP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Finesse versão 12.5
- Servidor CVP versão 12.5
- UCCE/PCCE versão 12.5
- Cisco VB versão 12.5
- CUIC versão 12.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

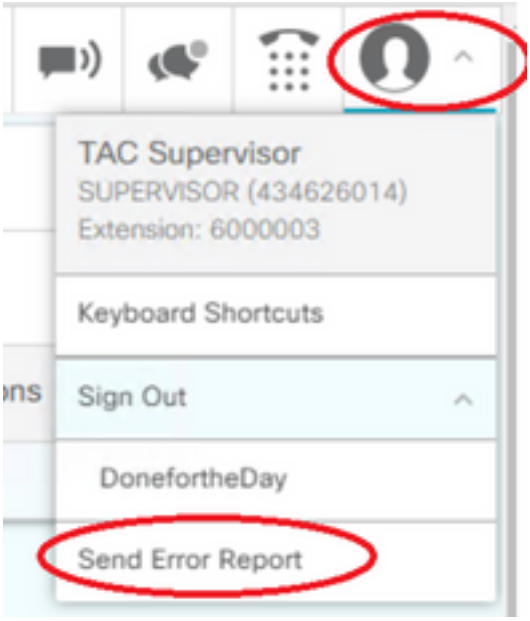
Definir Rastreamentos e Coletar Logs do Finesse

Cliente Finesse

Há várias opções para coletar logs do cliente Finesse.

Opção 1: Colete logs de clientes por meio do relatório de erro de envio.

1. Fazer logon de um agente.
2. Se um agente tiver algum problema durante uma chamada ou evento de mídia, instrua-o a clicar no link **Enviar relatório de erros** no canto superior direito da área de trabalho do finesse.



3. O agente vê os **logs enviados com êxito!** mensagem.
4. Os logs do cliente são enviados ao servidor Finesse. Navegue até https://x.x.x.x/finesse/logs

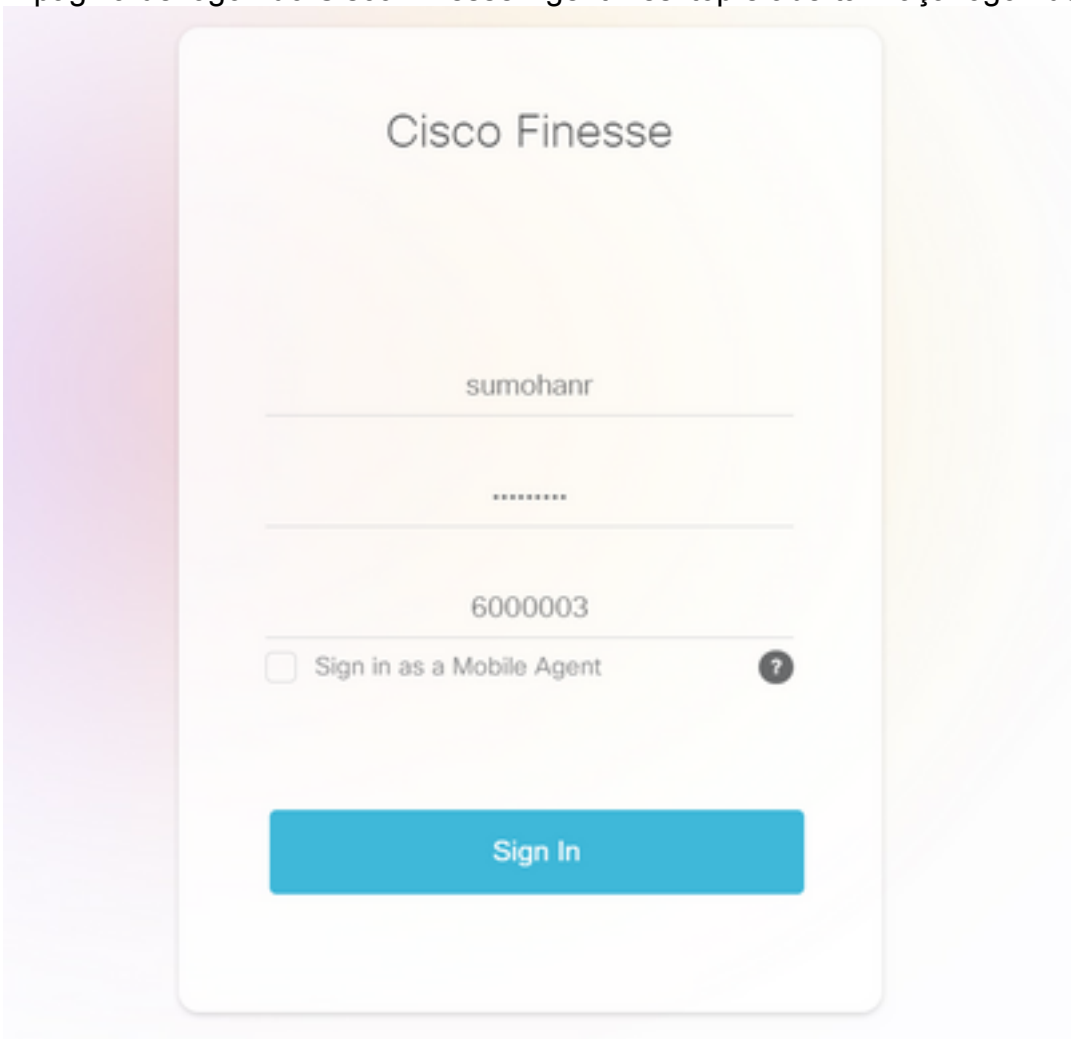
e faça login com uma conta de administração.

5. Colete os logs no diretório **clientlogs/**.

Opção 2: Definir Log Persistente

1. Navegue até https://x.x.x.x:8445/desktop/locallog.
2. Clique Em **Sign In With Persistent Logging**.

3. A página de logon do Cisco Finesse Agent Desktop é aberta. Faça logon do agente.

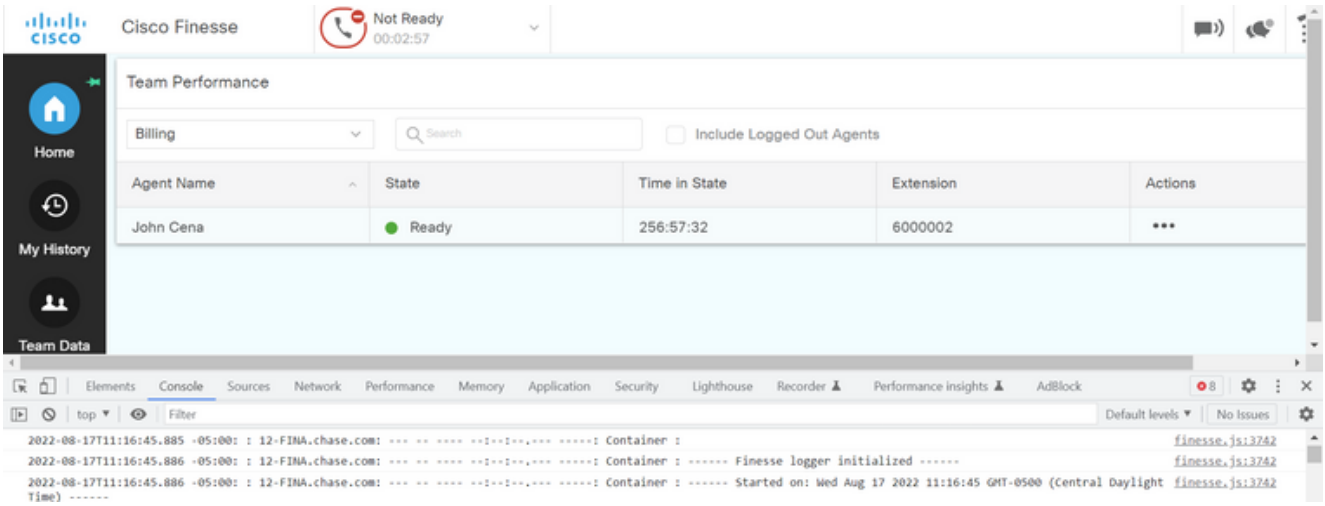


4. Toda a interação do Agent Desktop é registrada e enviada aos logs de armazenamento

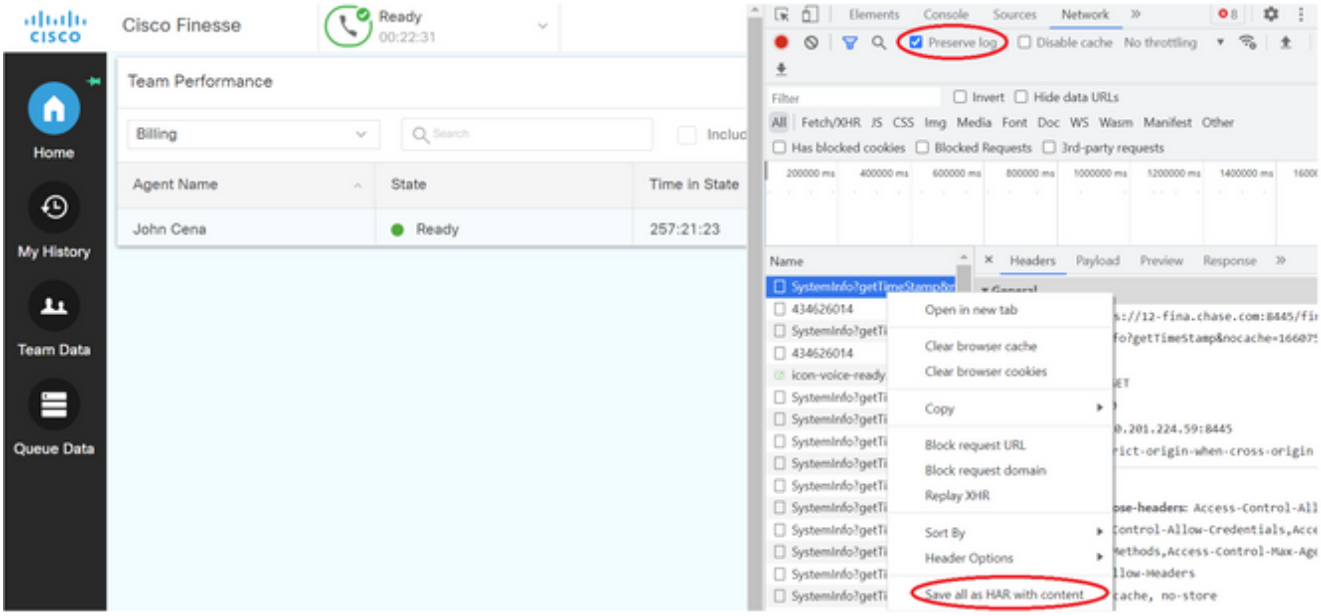
local. Para coletar os logs, navegue até https://x.x.x.x:8445/desktop/locallog e copie o conteúdo em um arquivo de texto. Save o arquivo para análise posterior.

Opção 3: Console do navegador da Web

1. Depois que um agente fizer logon, pressione **F12** para abrir o console do navegador.
2. Selecione a guia **Console**.
3. Verifique os erros no console do navegador. Copie o conteúdo em um arquivo de texto e save o



4. Selecione a guia **Network** e marque a opção Preserve log.
5. Clique com o botão direito do mouse em qualquer evento de nome de rede e selecione **Save** como HAR com conteúdo.



Servidor Finesse

Opção 1: Através da Interface do Usuário (UI) - Serviços Web (obrigatórios) e registros adicionais

1. Navegue até https://x.x.x.x/finesse/logs e faça login com a conta de administração.
2. Expanda o diretório **webservices/**

3. Colete os últimos logs do serviço Web. Selecione o último arquivo unzip. Por Exemplo, **Desktop-Webservices.201X-.log.zip**. Clique no link do arquivo e você verá a opção de save o arquivo.

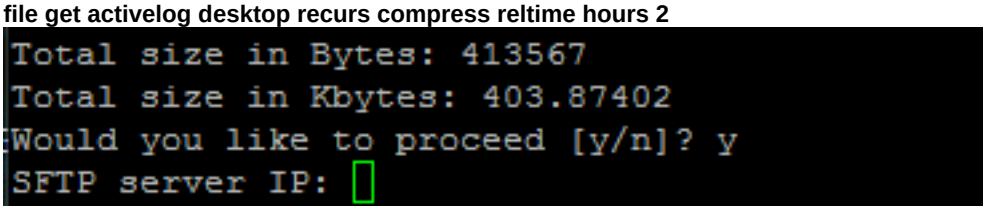
4. Colete os outros logs necessários (dependendo do cenário). Por exemplo, o openfire para problemas de serviço de notificação, logs de realm para problemas de autenticação e logs de tomatlo para problemas de APIs.

Note: O método recomendado para coletar os logs do servidor Cisco Finesse é via Secure Shell (SSH) e Secure File Transfer Protocol (SFTP). Esse método não só permite coletar os logs de serviços da Web, mas também todos os logs adicionais, como, Fippa, openfire, Realm e Clientlogs.

Opção 2: Via SSH e protocolo SFTP - opção recomendada

1. Faça login no servidor Finesse com o SSH.
2. Insira este comando para coletar os logs necessários. O comando coleta os logs por 2 horas. Você é solicitado a identificar o servidor SFTP no qual os logs são carregados.

file get activelog desktop recurs compress reltime hours 2



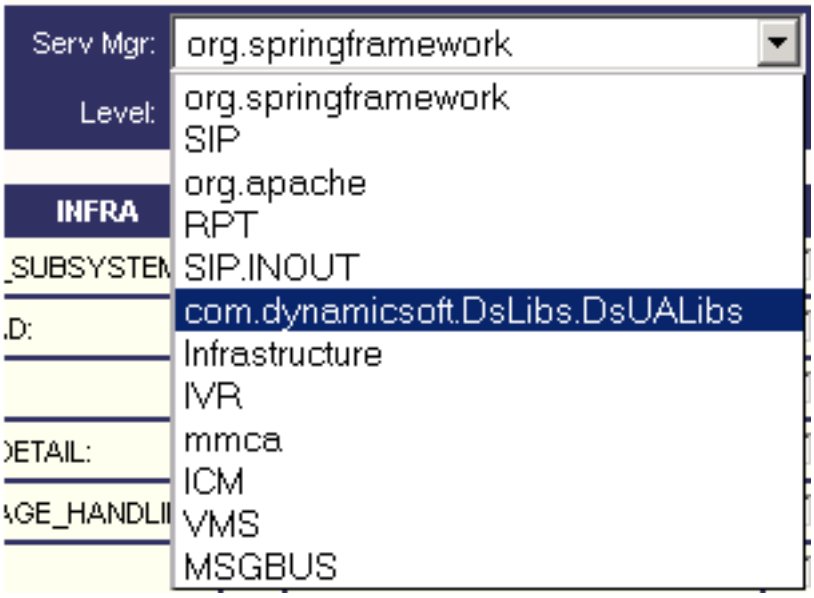
3. Esses logs são armazenados no caminho do servidor SFTP: <endereço IP>\<carimbo de data/hora>\ative_nnn.tgz , onde nnn é carimbo de data/hora em formato longo.
4. Para coletar logs adicionais como tomcat, serviço de contexto, servidor e logs de instalação, consulte a seção Coleta de logs do Guia de Administração do Cisco Finesse Release 12.5(1).

Definir rastreamentos e coletar registros CVP e CVB

Servidor de chamadas CVP

1. O nível padrão de rastreamentos do CVP CallServer é suficiente para solucionar a maioria dos casos. No entanto, quando você precisa obter mais detalhes sobre as mensagens do Session Initiation Protocol (SIP), você precisa definir os rastreamentos de pilha SIP para o nível DEBUG.
2. Navegue até a URL da página da Web CVP CallServer Diag http:/localhost:8000/cvp/diag. **Note**: Esta página fornece boas informações sobre o CVP CallServer e é muito útil para resolver determinados cenários.

3. Selecione **com.dynamicsoft.DsLibs.DsUALibs** no **Serv.** Menu suspenso **Mgr** no canto superior esquerdo

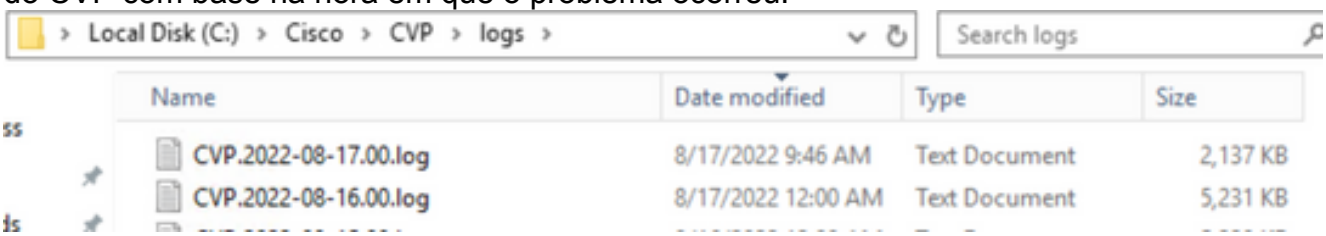


4. Clique no botão **Set**.

5. Role para baixo na janela de rastreamento para garantir que o nível de rastreamentos tenha sido definido corretamente. Estas são suas configurações de depuração.

NAME	LEVEL	MASK
org.springframework	WARN	0
SIP	DEBUG	41
org.apache	ERROR	0
RPT	DEBUG	1
SIP.INOUT	WARN	0
com.dynamicsoft.DsLibs.DsUALibs	DEBUG	0
Infrastructure	INFO	0
IVR	DEBUG	41
mmca	INFO	0
ICM	DEBUG	41
MSGBUS	INFO	0

6. Ao reproduzir o problema, colete os logs de **C:\Cisco\CVP\logs** e selecione o arquivo de log do CVP com base na hora em que o problema ocorreu.

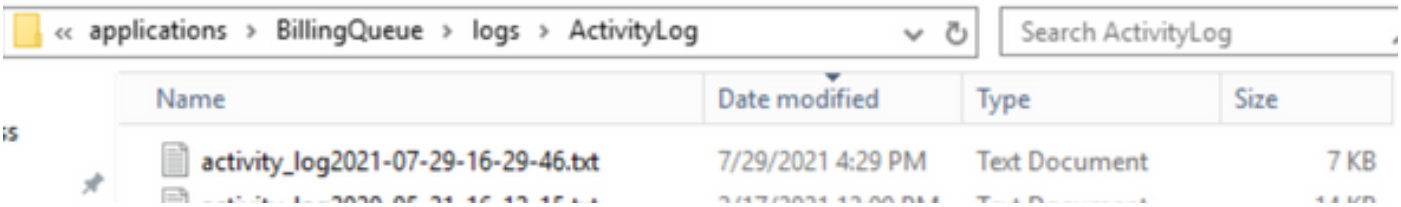


Aplicativo CVP Voice XML (VXML)

Em circunstâncias muito raras, você precisa aumentar o nível de rastreamentos dos aplicativos do servidor VXML. Por outro lado, não é recomendável aumentá-lo, a menos que um engenheiro da

Cisco solicite.

Para coletar os logs de aplicativo do servidor VXML, navegue para o diretório de aplicativo específico no servidor VXML, por exemplo: **C:\Cisco\CVP\VXMLServer\applications\{nome do aplicativo}\logs\ActivityLog** e colete os logs de atividades.



Portal de gerenciamento de operações e administração (OAMP) do CVP

Na maioria dos casos, o nível padrão de rastreamentos de OAMP e ORM é suficiente para determinar a causa raiz do problema. No entanto, se o nível de rastreamentos precisar ser aumentado, estas são as etapas para executar esta ação:

1. Backup **%CVP_HOME%\conf\oamp.properties**

2. Editar **%CVP_HOME%\conf\oamp.properties**

```
omgr.traceMask=-1
omgr.logLevel=DEBUG
org.hibernate.logLevel=DEBUG
org.apache.logLevel=ERROR
net.sf.ehcache.logLevel=ERROR
```

3. Reinicie o OPSConsoleServer após a modificação, conforme mostrado.

Informações do nível de rastreamento

Nível de rastreamento	Descrição	Nível de log	Máscara de rastreamento
0	Instalação padrão do produto. Nenhum ou mínimo impacto esperado no desempenho.	INFORMAÇÕES	Nenhum
1	Mensagens de rastreamento menos detalhadas com um pequeno impacto no desempenho.	DEBUG	DEVICE_CONFIGURATION + DATABASE_MODIFY + GERENCIAMENTO=0x0101000
2	Mensagens de rastreamento detalhadas com impacto médio no desempenho.	DEBUG	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + DATABASE_MODIFY + GERENCIAMENTO=0x0501000
3	Mensagem de rastreamento detalhada com alto impacto no desempenho.	DEBUG	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION

			+ BULK_OPERATIONS + DATABASE_MODIFY + GERENCIAMENTO=0x0511 1000
4	Mensagem de rastreamento detalhada com um impacto de desempenho muito alto.	DEBUG	DIVERSOS + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACK TRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + GERENCIAMENTO + TRACE_METHOD + TRACE_PARAM=0x173710 00
5	Mensagem de rastreamento mais detalhada.	DEBUG	DIVERSOS + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACK TRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + GERENCIAMENTO + TRACE_METHOD + TRACE_PARAM=0x173710 06

Cisco Virtualized Voice Browser (CVB)

No CVB, um arquivo de rastreamento é um arquivo de registro que registra a atividade dos subsistemas e etapas do componente Cisco VB.

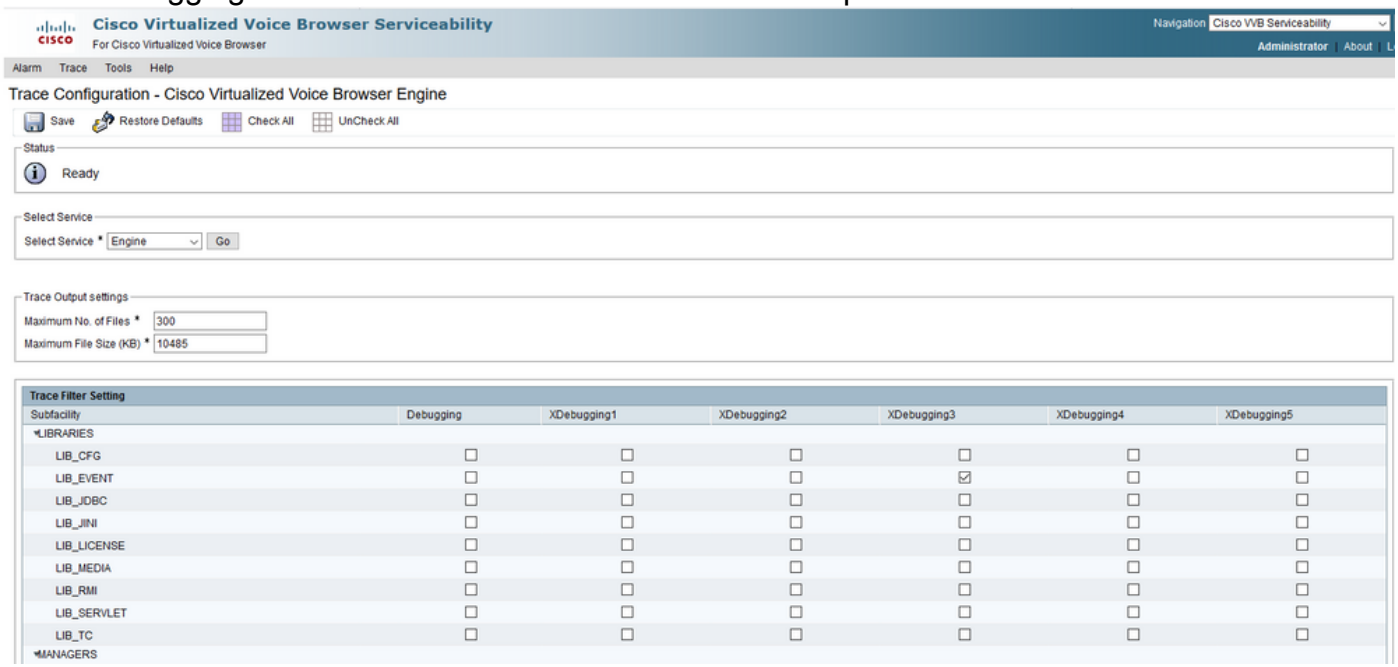
O Cisco VVB tem dois componentes principais:

- Rastreamentos de "administração" do Cisco VB denominados logs MADM
- Rastreamentos de "mecanismo" do Cisco VB denominados logs MIVR

Você pode especificar os componentes para os quais deseja coletar informações e o nível de informações que deseja coletar.

Os níveis de log se estendem de:

- Depuração - Detalhes básicos do fluxo para
- XDebugging 5 - Nível detalhado com rastreamento de pilha



aviso: Xdebugging5 não deve ser habilitado no sistema carregado de produção.

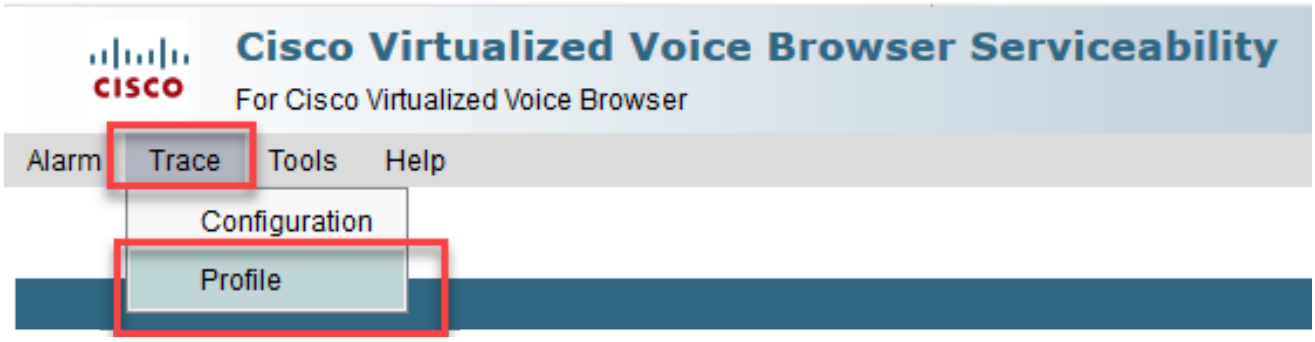
Os logs mais comuns que você precisa coletar são o Mecanismo. O nível padrão de rastreamentos para os rastreamentos do Mecanismo CVB é suficiente para solucionar a maioria dos problemas. No entanto, se você precisar alterar o nível de rastreamentos para um cenário específico, a Cisco recomenda que você use os Perfis de log do sistema predefinidos.

Perfis de log do sistema

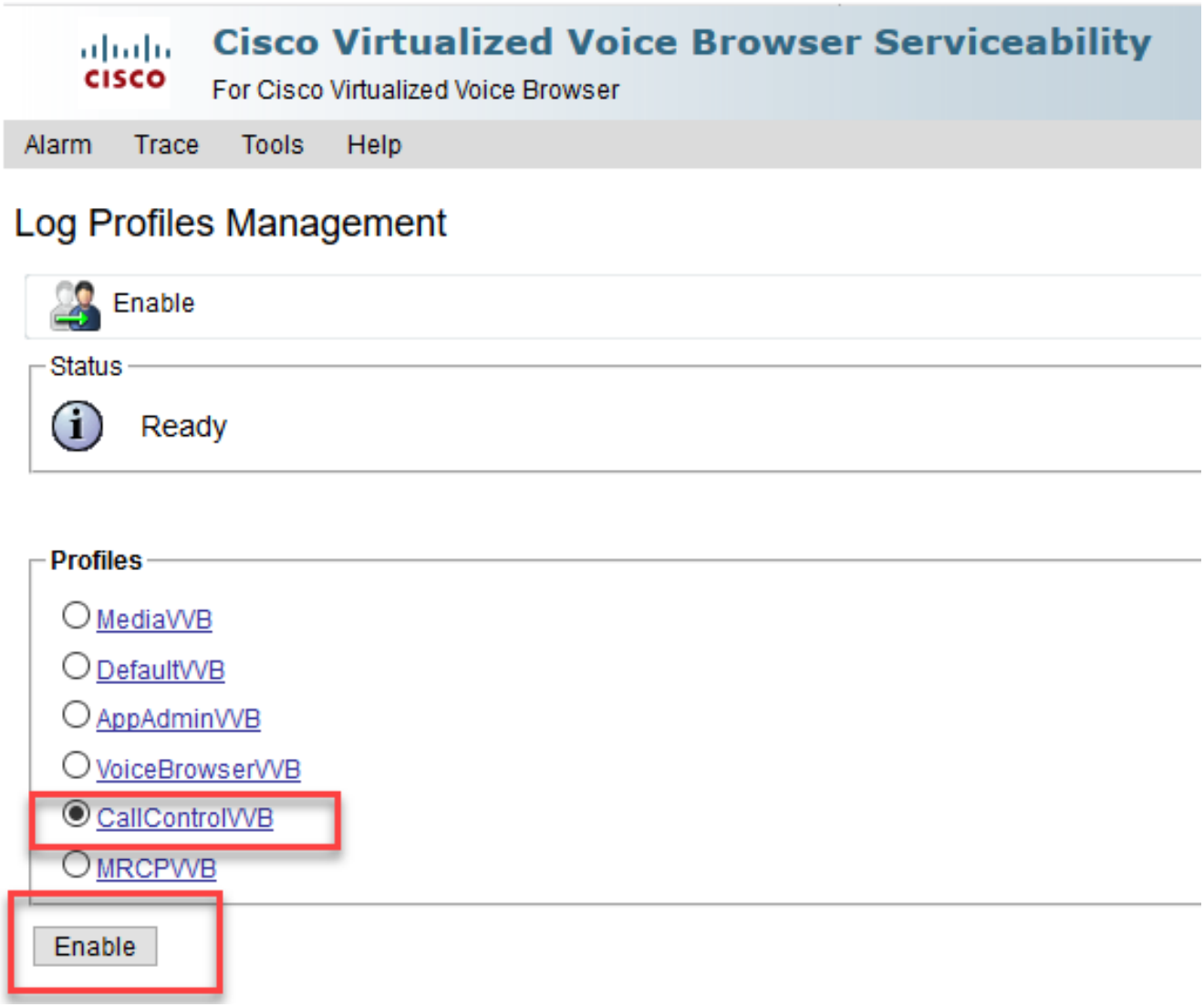
Nome	Cenário no qual este perfil deve ser ativado
VBpadrão	Logs genéricos estão habilitados.
AppAdminVB	Para problemas com a administração da Web através do AppAdmin, Ci VB Serviceability e outras páginas da Web.
MídiaVB	Para problemas de configuração ou transmissão de mídia.
VoiceBrowserVB	Para problemas com tratamento de chamadas.
MRCPVB	Para problemas com ASR/TTS com interação Cisco VVB.
ControleChamadaVVB	Para problemas com sinal SIP relacionado, são publicados no registro.

1. Abra a página principal do CVB (https://X.X.X.X/uccxservice/main.htm) e navegue até a página Cisco VVB Serviceability. Faça login com a conta de administração

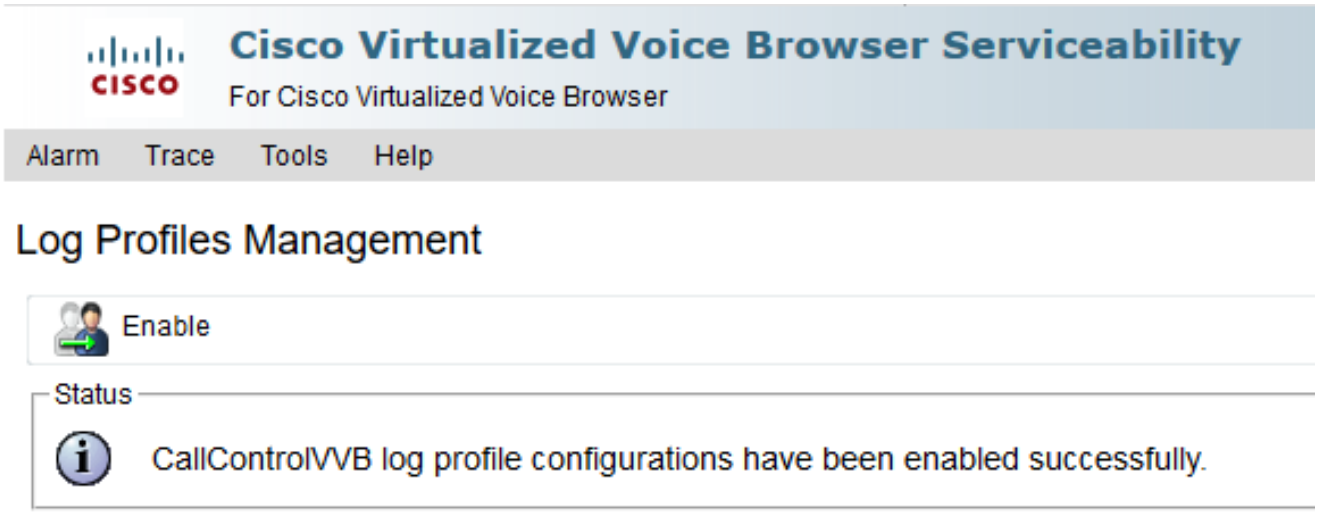
2. Selecionar **Trace -> Profile (Rastrear -> Perfil).**



3. Marque o perfil que deseja ativar para o cenário específico e clique no botão **Ativar**. Por exemplo, habilite o perfil CallControlVVB para problemas relacionados ao SIP ou MRCPVB para problemas relacionados à interação Automatic Speech Recognition and Text to Speech (ASR/TTS).

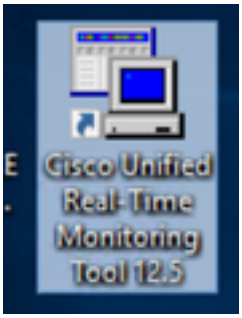


4. Você verá a mensagem de êxito depois de clicar no botão de ativação.

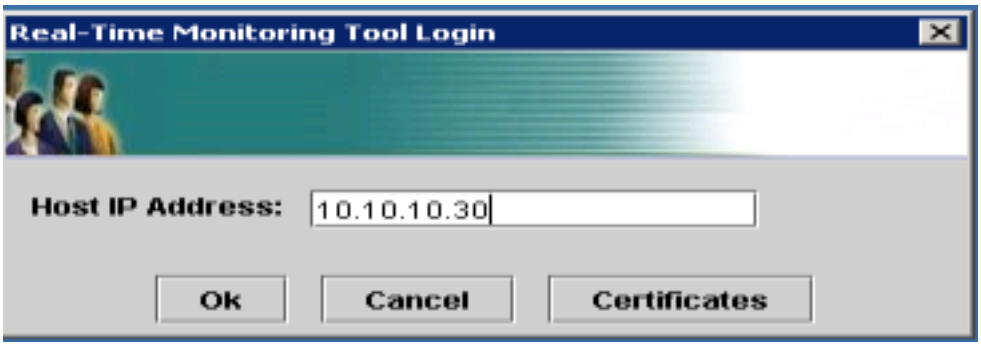


5. Após a reprodução do problema, colete os logs. Use a Real Time Monitor Tool (RTMT) que acompanha o CVB para coletar os logs.

6. Clique no ícone Cisco Unified Real-Time Monitoring Tool em sua área de trabalho (se necessário, baixe essa ferramenta do CVB).

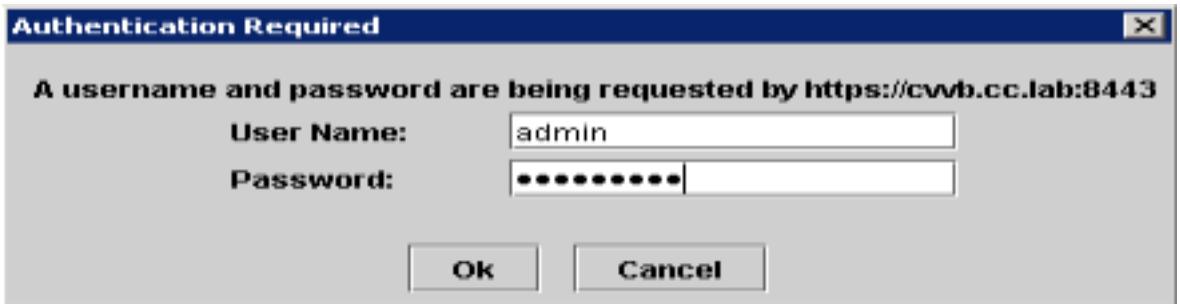


7. Forneça o endereço IP do VVB e clique em **OK**.



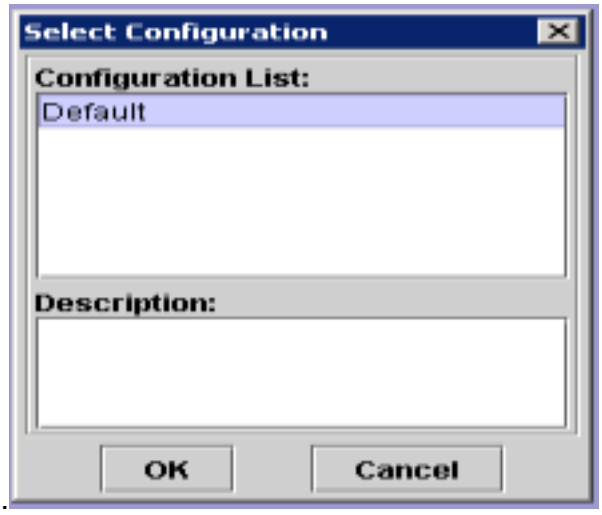
8. Aceitar as informações do certificado se exibidas

9. Forneça a credencial e clique em **OK**.

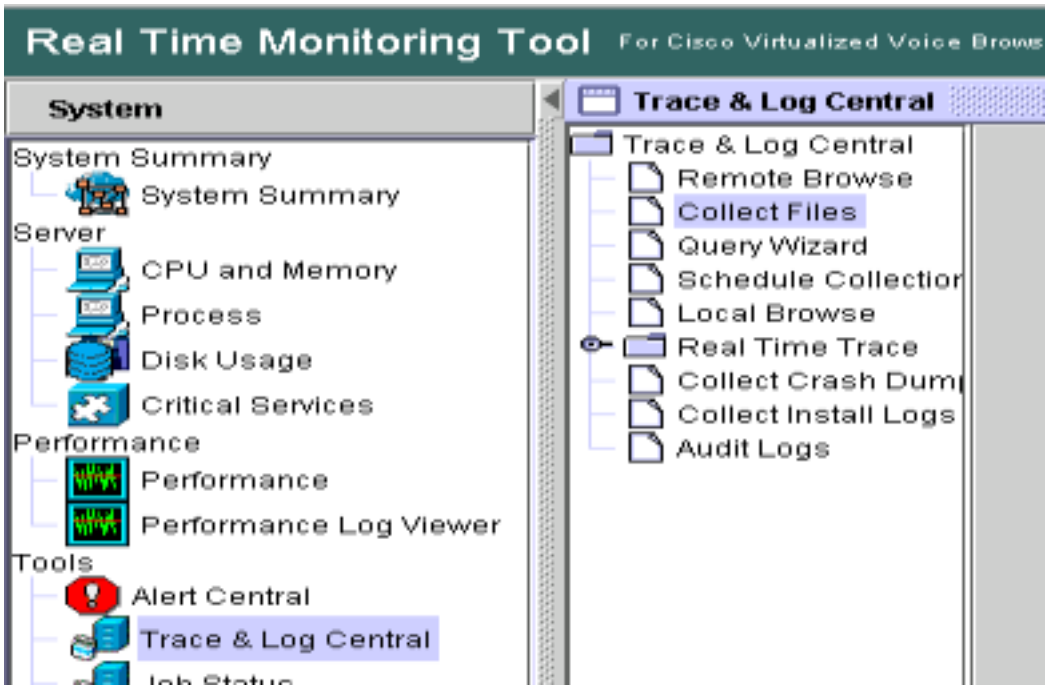


10. Se você recebeu o erro TimeZone, a RTMT pode fechar depois que você clica no botão **Yes**. Reinicie a ferramenta RTMT.

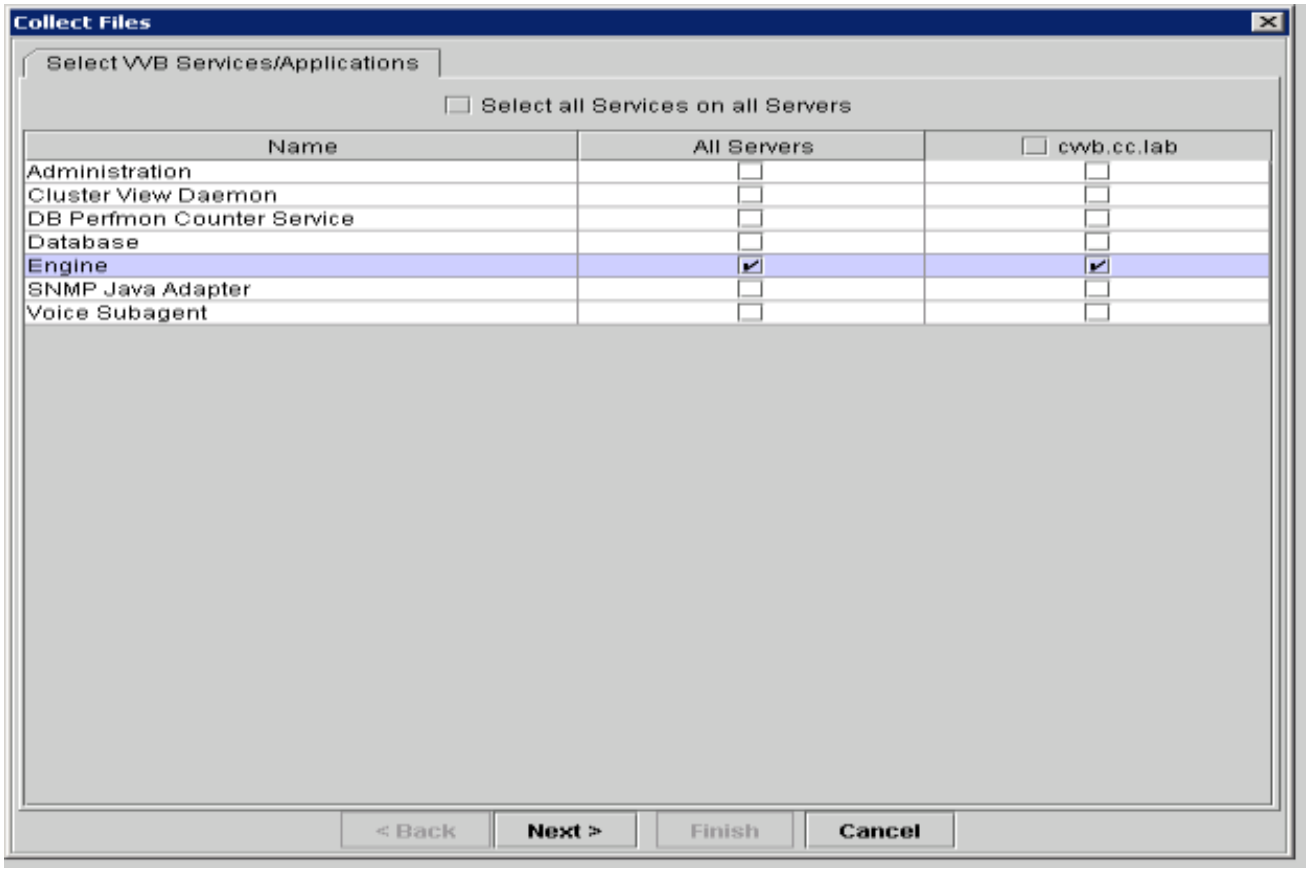
11. Deixe a opção Default configuration selecionada e clique em **OK**.



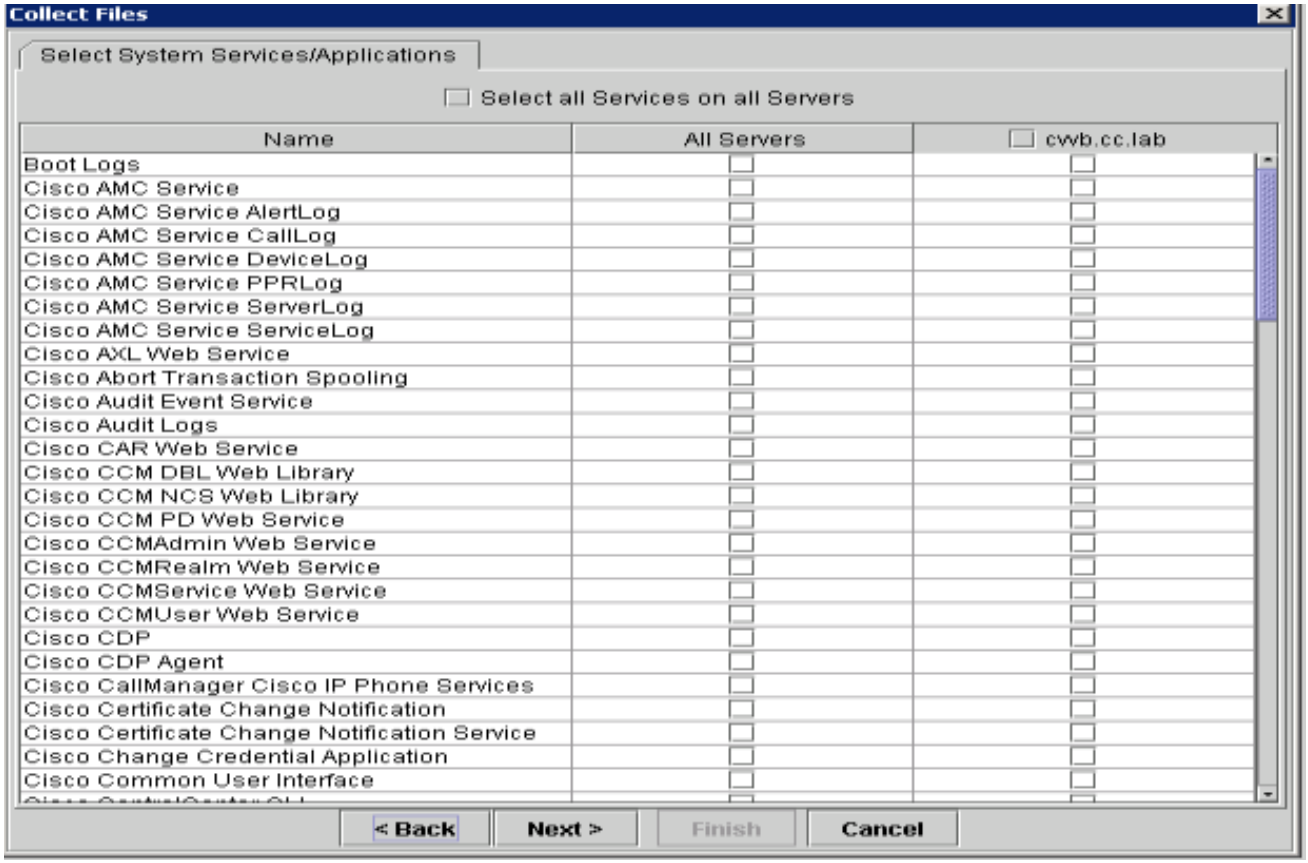
12. Selecione **Trace & Log Central** e clique duas vezes em **Collect Files**.



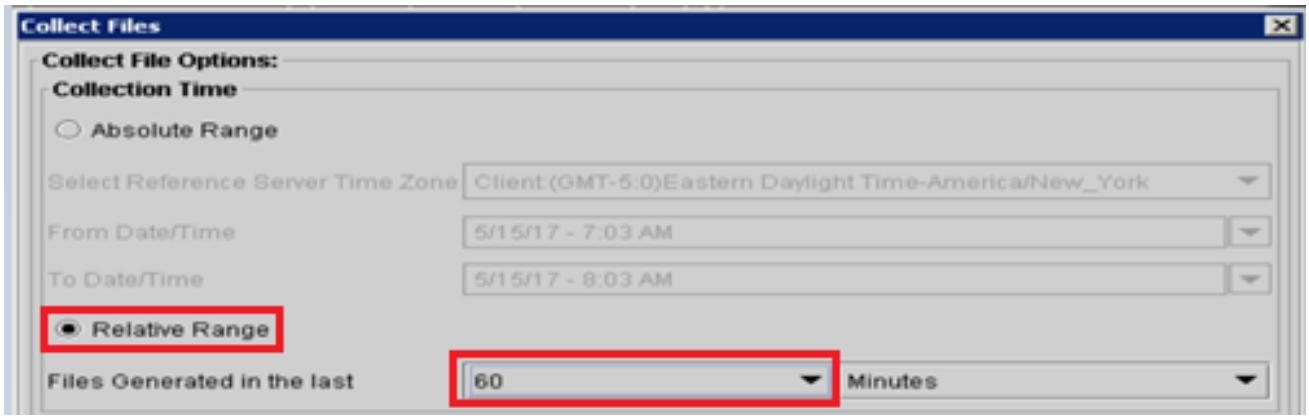
13. Na nova janela aberta, selecione o **Mecanismo** e clique em Avançar.



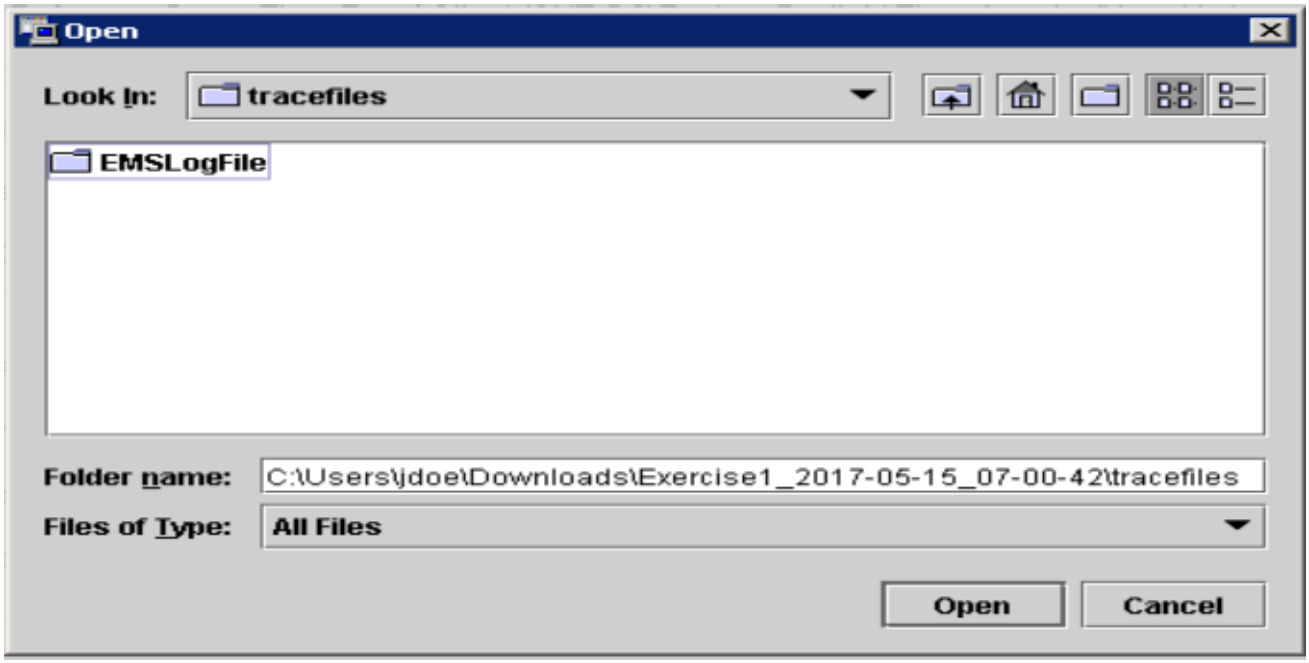
14. Clique em **Avançar** novamente na próxima janela.



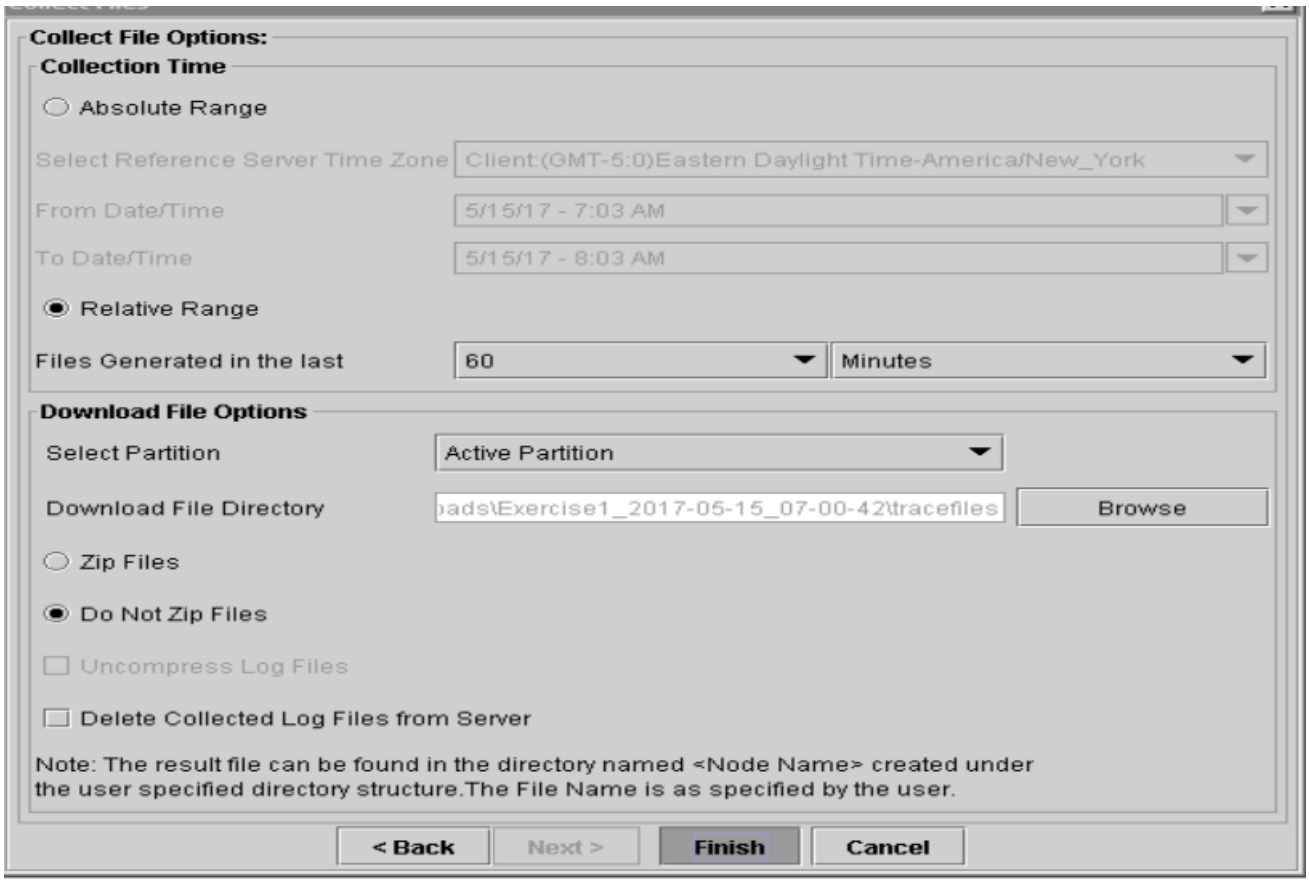
15. Selecione **Intervalo relativo** e certifique-se de selecionar a hora para cobrir a hora da chamada ruim.



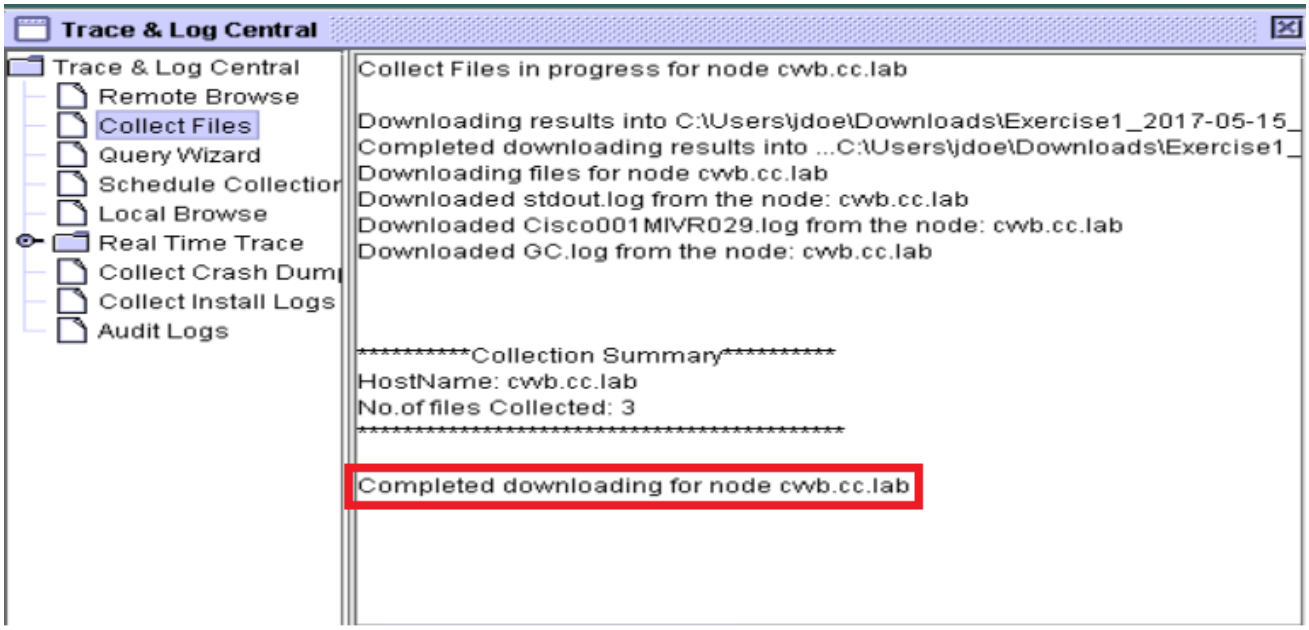
16. Em Download File Options (Opções de download de arquivos), clique em **Browse** e selecione o diretório no qual deseja fazer o download save o arquivo e clique em **Abrir**.



17. Quando tudo estiver selecionado, clique no botão **Concluir**.



18. Coleta os arquivos de log. Aguarde até ver a mensagem de confirmação em RTMT.

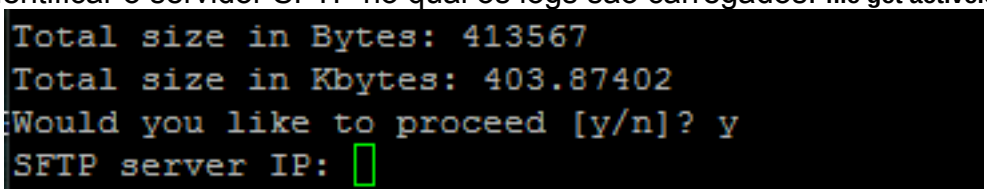


19. Navegue até a pasta onde os rastreamentos são salvos.

20. Os registros do Engine são tudo o que você precisa. Para localizá-los, navegue até a pasta **\<carimbo de data/hora>\uccx\log\MIVR**.

Opção 2: Via SSH e SFTP - opção recomendada

1. Faça login no servidor VVB com o Secure Shell (SSH).
2. Insira este comando para coletar os logs necessários. Os logs são compactados e você é solicitado a identificar o servidor SFTP no qual os logs são carregados. **file get activelog /uccx/log/MIVR/***



3. Esses logs são armazenados no caminho do servidor SFTP: *<endereço IP>\<carimbo de data/hora>\ative_nnn.tgz* , onde nnn é carimbo de data/hora em formato longo.

Definir logs de rastreamento e coleta para CUBE e CUSP

CUBE (SIP)

1. Defina o timestamp dos logs e ative o buffer de registro.

```
#conf  t
service timestamps debug datetime msec
service timestamps log datetime msec
service sequence-numbers
no logging console
no logging monitor
logging buffered 5000000 7
end
clear logging
```

aviso: Qualquer alteração em um GW de produção do Cisco IOS® pode causar uma interrupção.

2. Esta é uma plataforma muito robusta que pode manipular as depurações sugeridas no volume de chamada fornecido sem problemas. No entanto, a Cisco recomenda que você: Envie todos os logs para um servidor syslog em vez de para o buffer de registro.

```
logging <syslog server ip>
logging trap debugs
```

Aplique os comandos debug um de cada vez e verifique a utilização da CPU após cada um.

```
show proc cpu hist
```

aviso: Se a CPU obtém até 70-80% de utilização da CPU, o risco de um impacto no serviço relacionado ao desempenho é muito maior. Portanto, não ative depurações adicionais se o GW atingir 60%.

3. Habilitar estas depurações:

```
debug voip ccapi inout
debug ccsip mess
After you make the call and simulate the issue, stop the debugging:
```

4. Reproduza o problema.
5. Desabilite os rastreamentos.

```
#undebug all
```

6. Colete os logs.

```
term len 0
show ver
show run
show log
```

CUSP

1. Ative os rastreamentos SIP no CUSP.

```
(cusp)> config
(cusp-config)> sip logging
(cusp)> trace enable
(cusp)> trace level debug component sip-wire
```

2. Reproduza o problema.
3. Desligue o sistema quando terminar.

Coletar os logs

1. Configure um usuário no CUSP (por exemplo: teste).
2. Adicione essa configuração no prompt do CUSP.

```
username <userid> create
username <userid> password <password>
username <userid> group pfs-privusers
```

3. Faça FTP para o endereço IP do CUSP. Use o nome de usuário (teste) e a senha conforme definido na etapa anterior.
4. Altere os diretórios para /cusp/log/trace.
5. Obtenha o log_<filename>.

Definir rastreamento e coletar logs UCCE

A Cisco recomenda definir níveis de rastreamento e coletar rastreamentos através do Diagnostics

Framework Portico ou das ferramentas CLI do sistema.

> **Note:** Para obter mais informações sobre o Diagnostic Framework Portico e o System CLI, visite o capítulo Ferramentas de diagnóstico no Guia de manutenção do Cisco Unified ICM/Contact Center Enterprise, Versão 12.5(1).

Ao solucionar a maioria dos cenários de UCCE, se o nível padrão de rastreamentos não fornecer informações suficientes, defina o nível de rastreamentos como 3 nos componentes necessários (com algumas exceções).

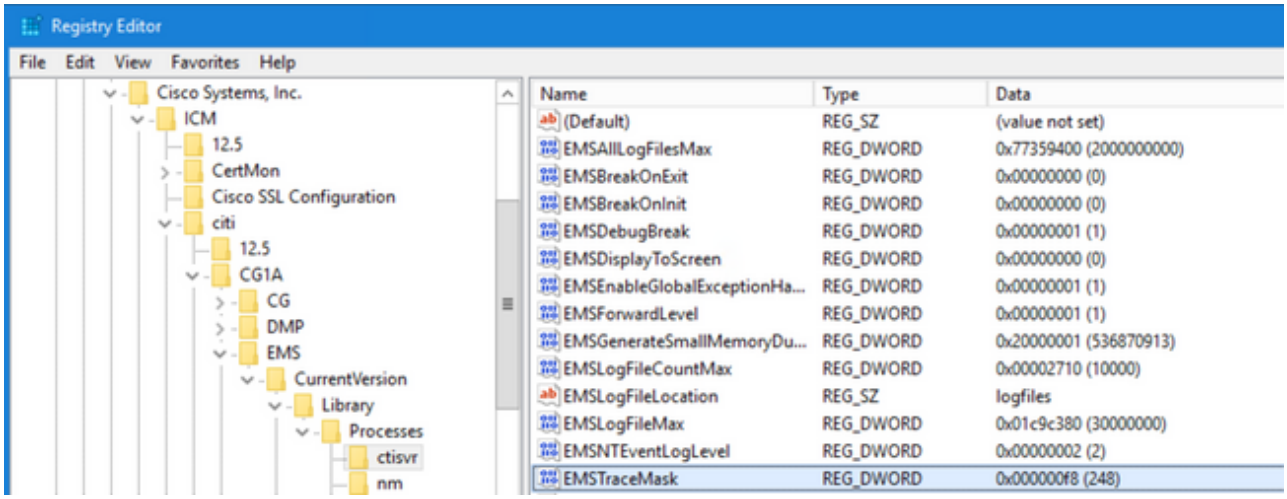
> **Note: Visite a seção** Nível de Rastreamento no Guia de Manutenção do Cisco Unified ICM/Contact Center Enterprise, Versão 12.5(1) para obter mais informações.

Por exemplo, se você solucionar problemas do Outbound Dialer, o nível de rastreamentos deverá ser definido para o nível 2 se o Dialer estiver ocupado.

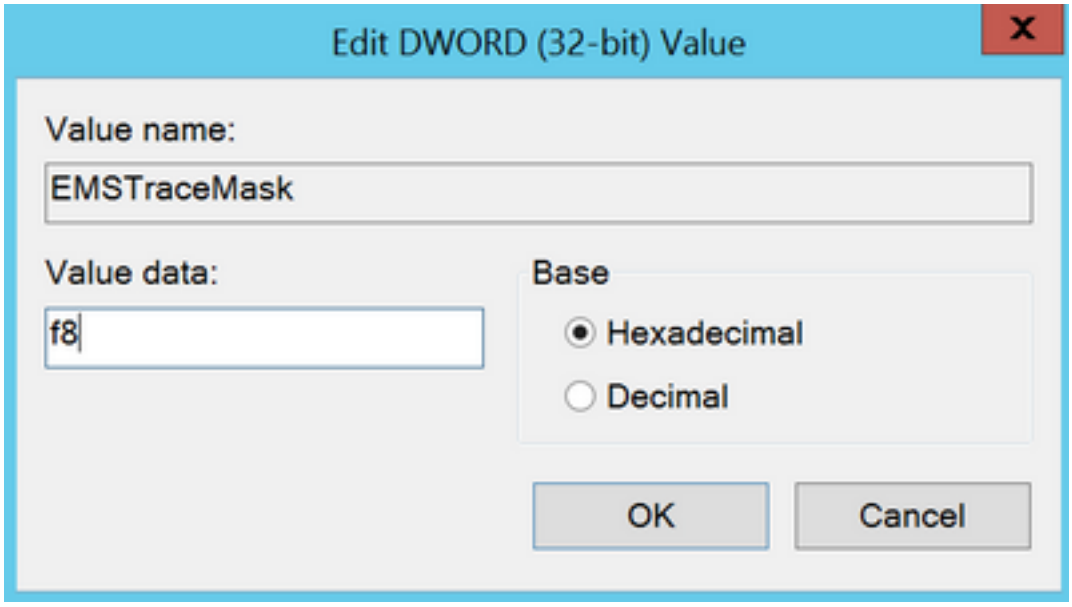
Para CTISVR (CTISVR), o nível 2 e o nível 3 não definem o nível exato de registro recomendado pela Cisco. O registro de rastreamento recomendado para CTISVR é 0XF8.

1. No UCCE Agent PG, abra o Editor do Registro (Regedit).

2. Navegue até HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a e b)\EMS\CurrentVersion\library\Processes\ctisvr.



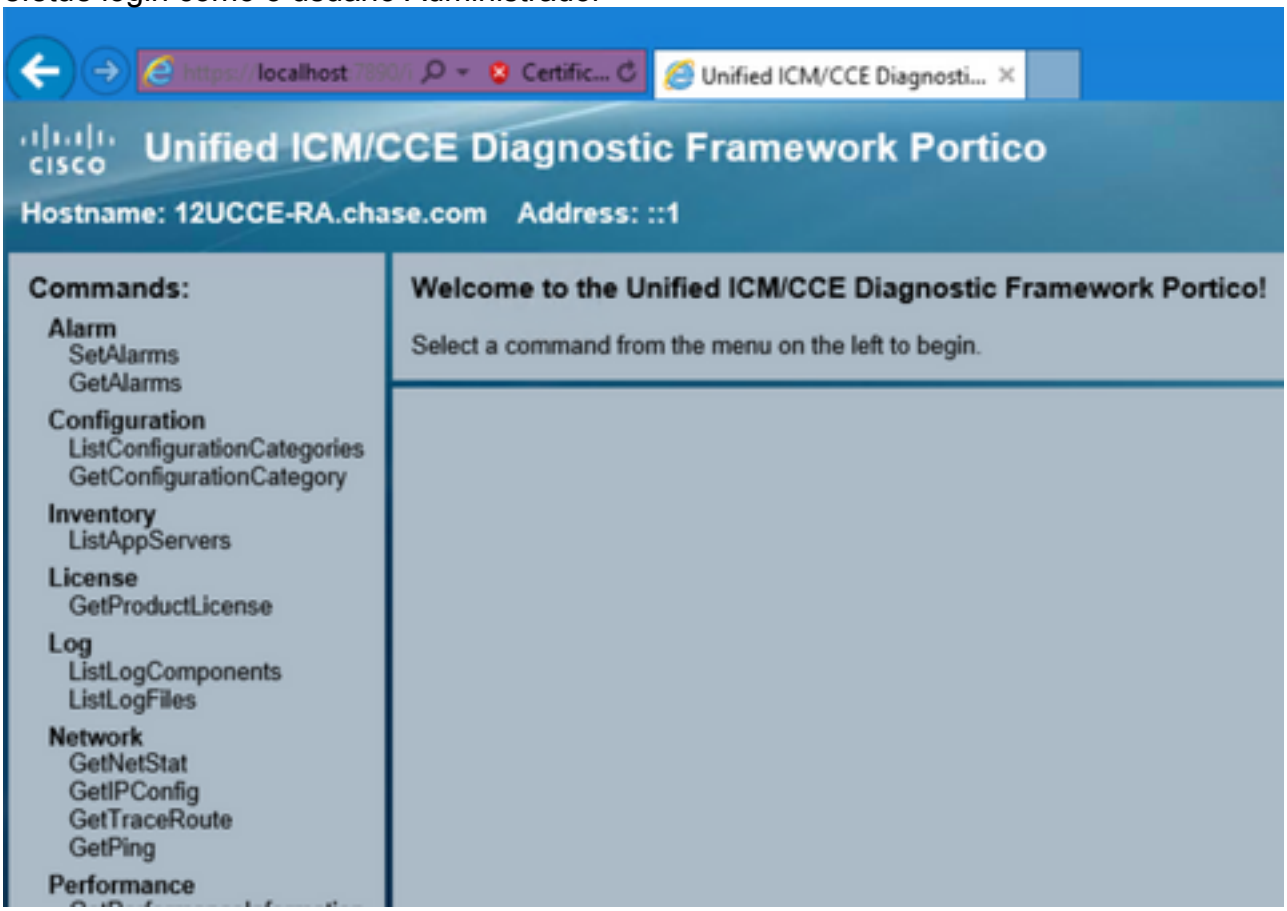
3. Clique duas vezes em **EMSTraceMask** e defina o valor como **f8**.



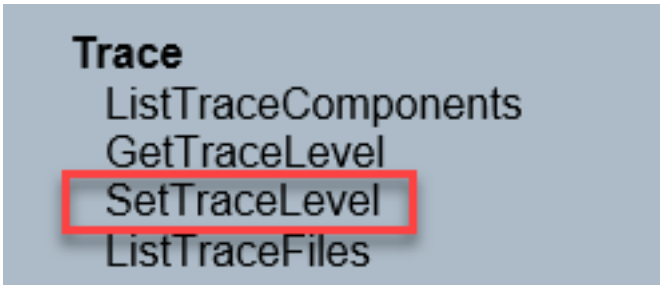
4. Clique em **Ok** e feche o Editor do Registro. Estas são as etapas para definir quaisquer rastreamentos de componente UCCE (o processo RTR é usado como exemplo).

Definir Nível de Rastreamento

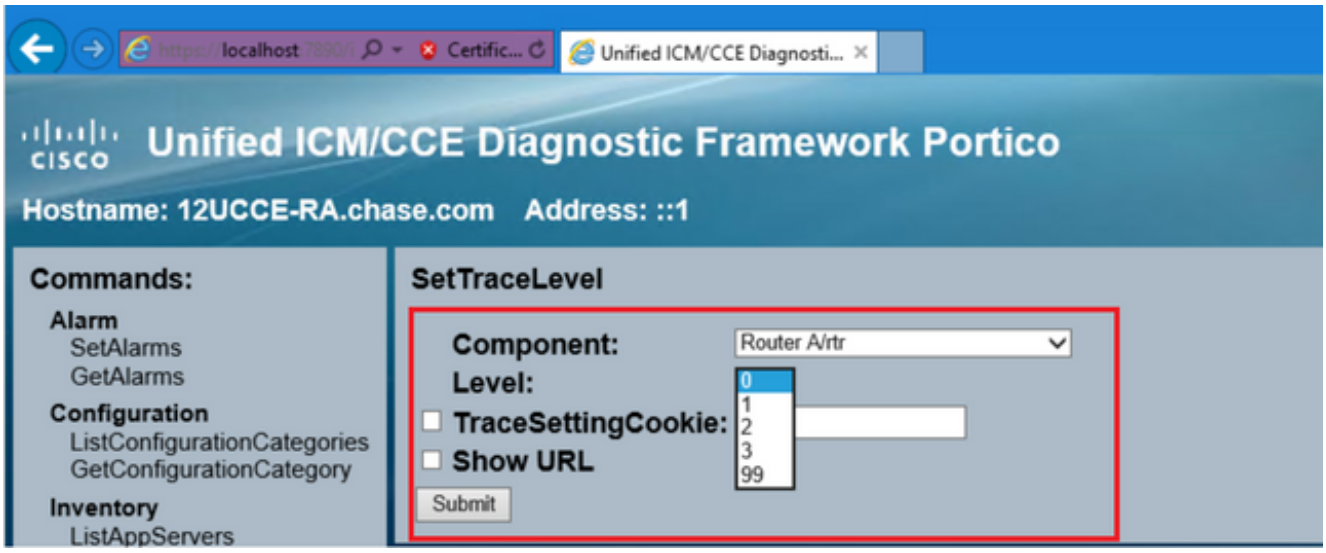
1. Abra o Diagnostic Framework Portico no servidor necessário para definir os rastreamentos e efetue login como o usuário Administrador



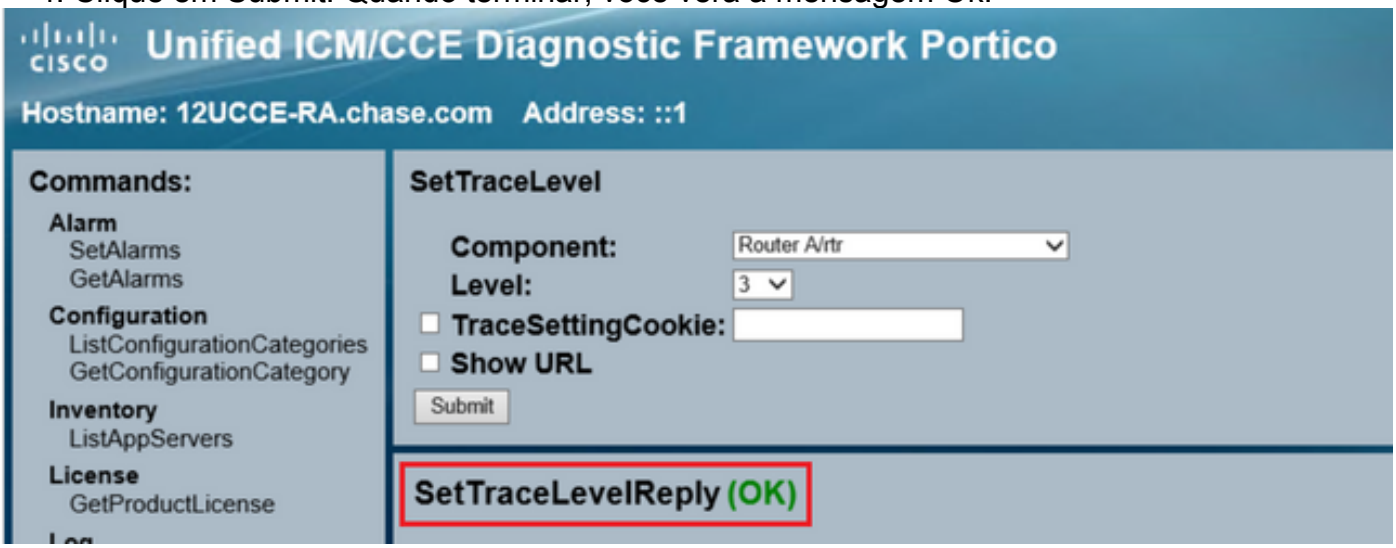
2. Na seção Comandos, navegue até **Rastrear** e selecione **SetTraceLevel.**



3. Na janela **SetTraceLevel**, selecione o componente e o nível.



4. Clique em Submit. Quando terminar, você verá a mensagem Ok.

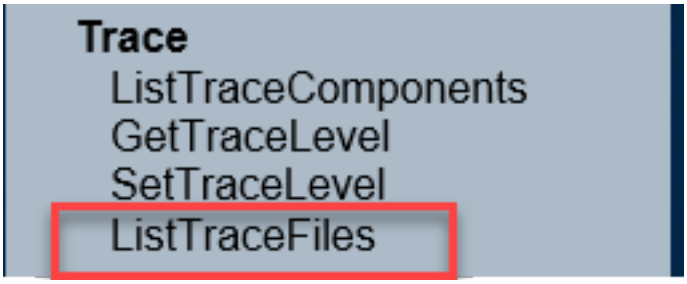


aviso: Defina o nível de rastreamentos como 3 enquanto tenta reproduzir o problema. Depois que o problema for reproduzido, defina o nível de rastreamento como padrão. Tome cuidado especial ao definir os rastreamentos JTAPIGW, já que os níveis 2 e 3 definem os rastreamentos de baixo nível e isso pode causar um impacto no desempenho. Defina o Nível 2 ou o Nível 3 no JTAPIGW durante o tempo de não produção ou em um ambiente de laboratório.

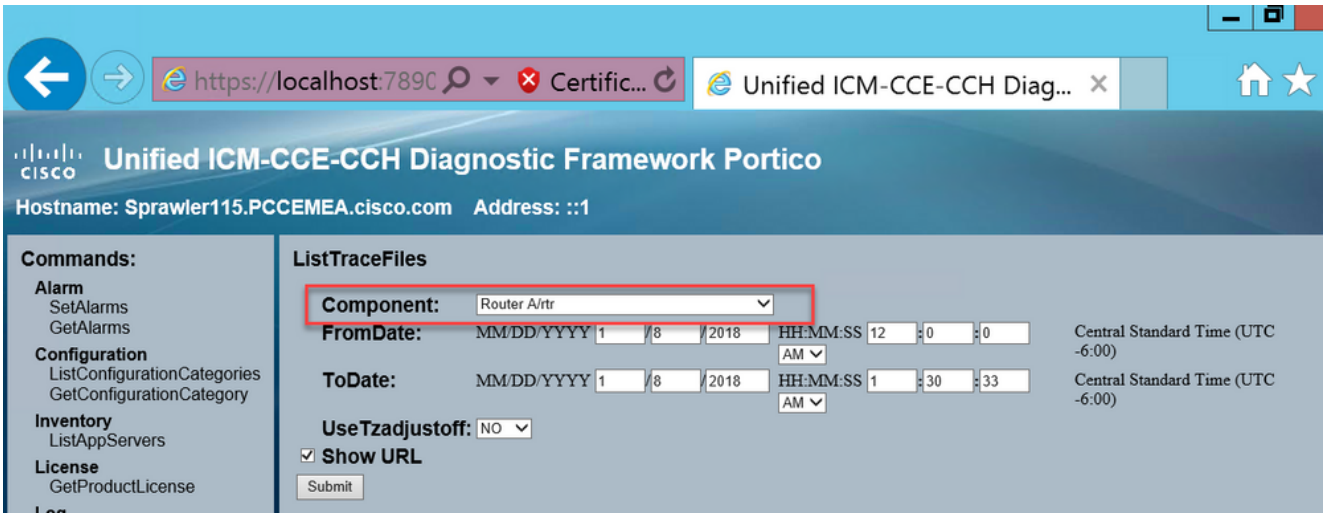
Coleta de logs

1. No Diagnostic Framework Portico, na seção **Commands**, navegue até **Trace** e selecione

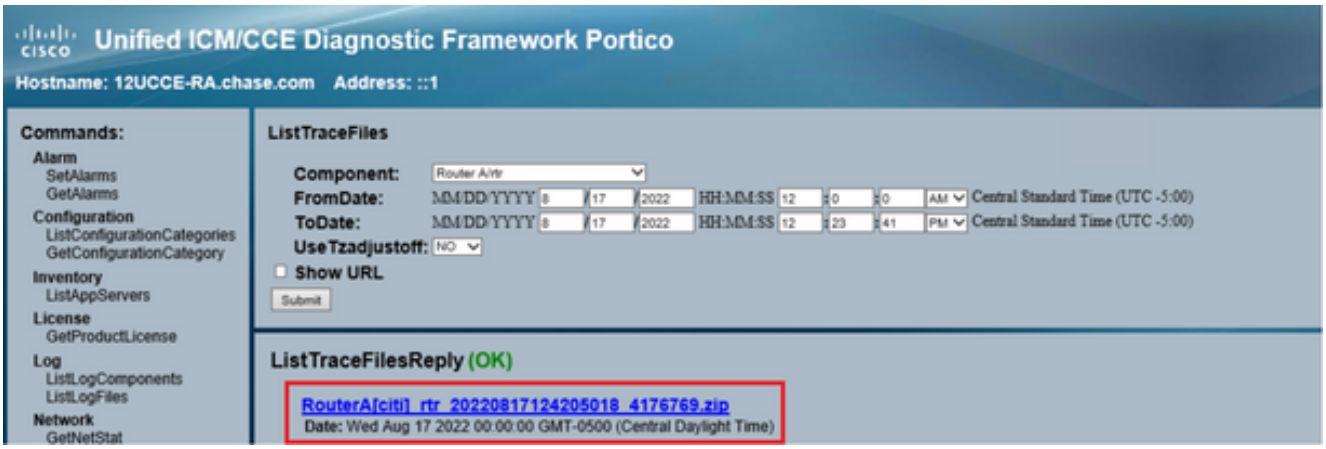
ListTraceFile.



2. Na **janela ListTraceFile**, selecione o **Componente**, **FromDate**e **ToDate**. Marque a caixa **Show URL** e clique em **Submit**.



3. Quando a solicitação terminar, você verá a mensagem OK com o link do arquivo de log ZIP.



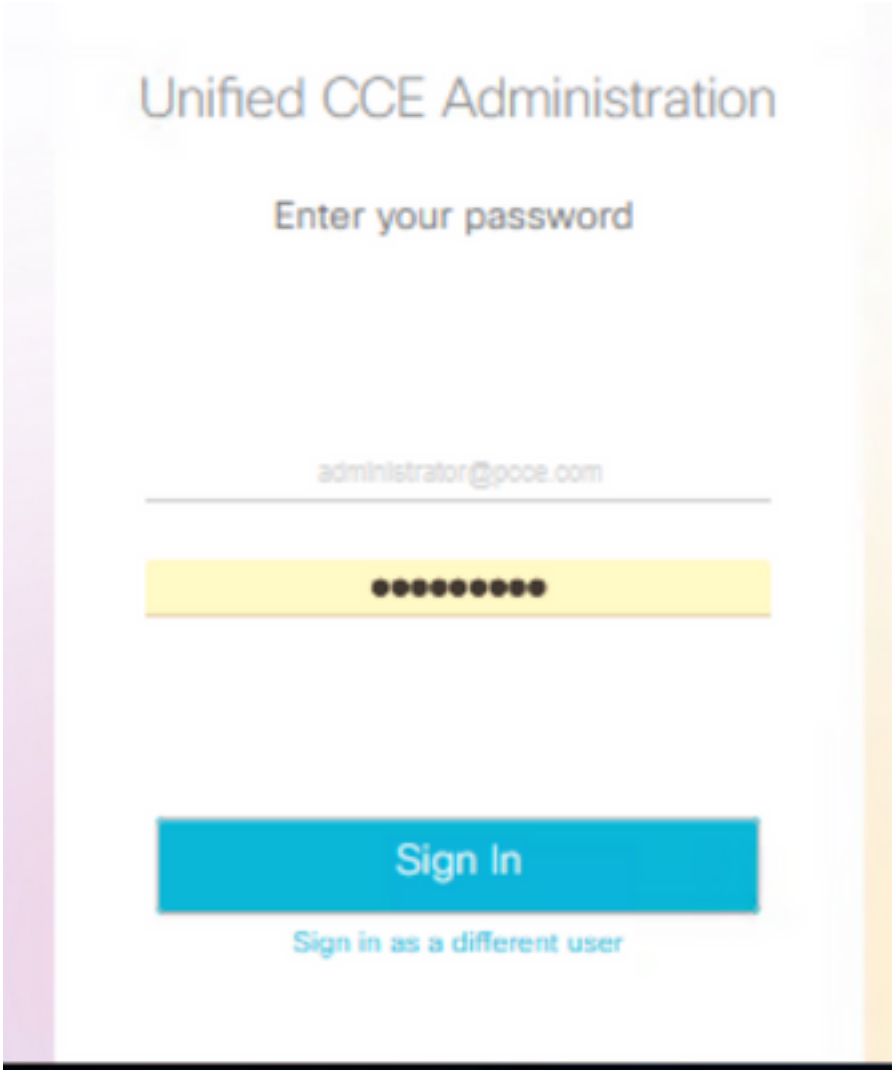
4. Clique no link do arquivo ZIP e save o arquivo no local escolhido.

Definir rastreamento e coletar logs PCCE

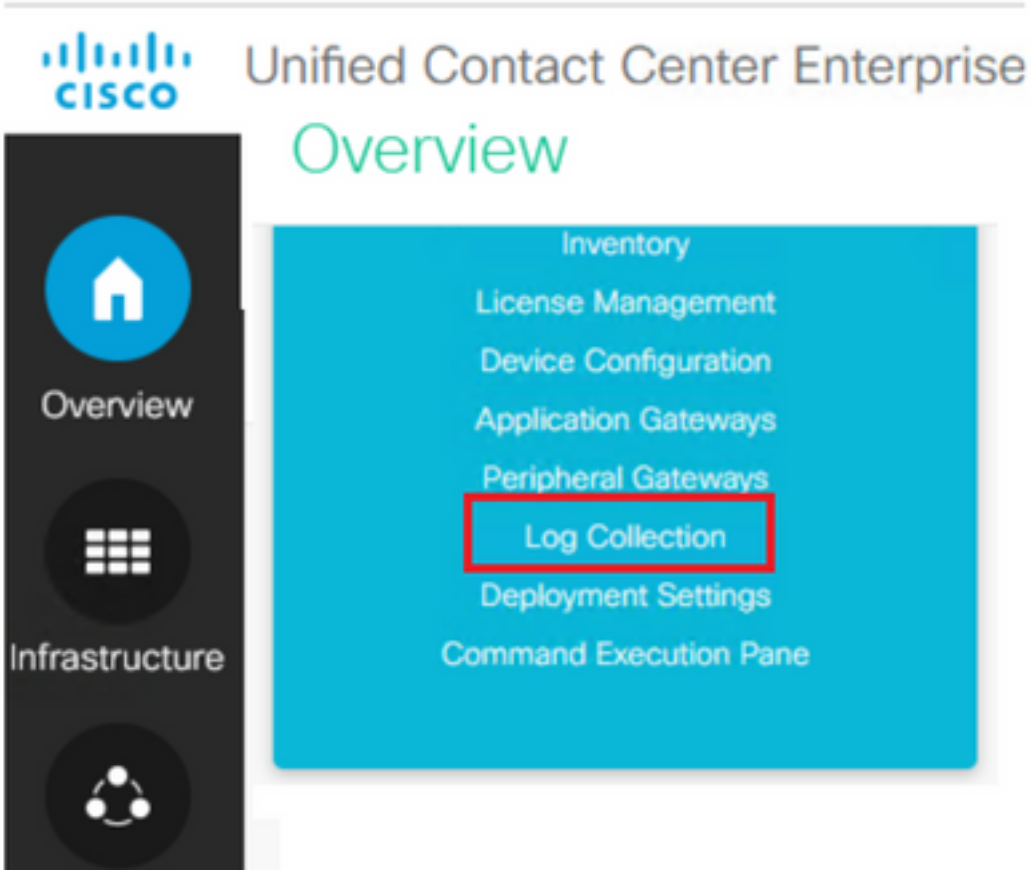
O PCCE tem sua própria ferramenta para configurar níveis de rastreamento. Não é aplicável ao ambiente UCCE, onde o Diagnostic Framework Portico ou o CLI do sistema são as maneiras preferidas de ativar e coletar logs.

1. No servidor PCCE AW, abra a ferramenta Unified CCE Web Administration e faça logon na

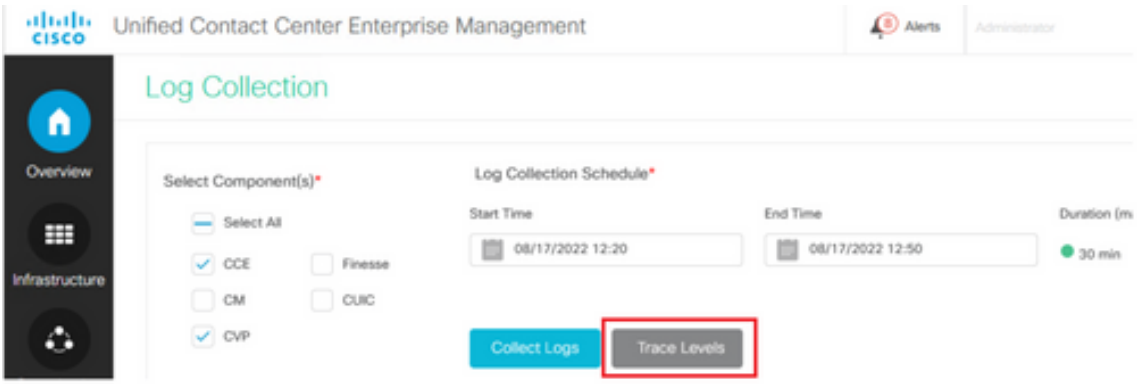
conta de Administrador.



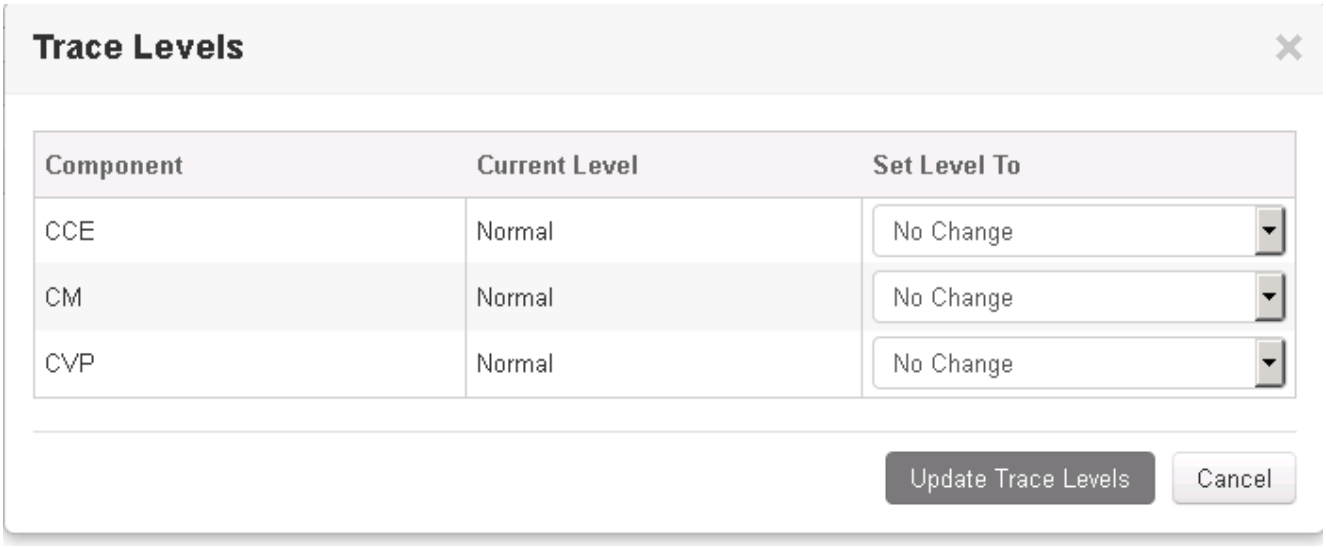
2. Navegue para **Overview->Infrastructure Settings->Log Collection** para abrir a página Log Collection.



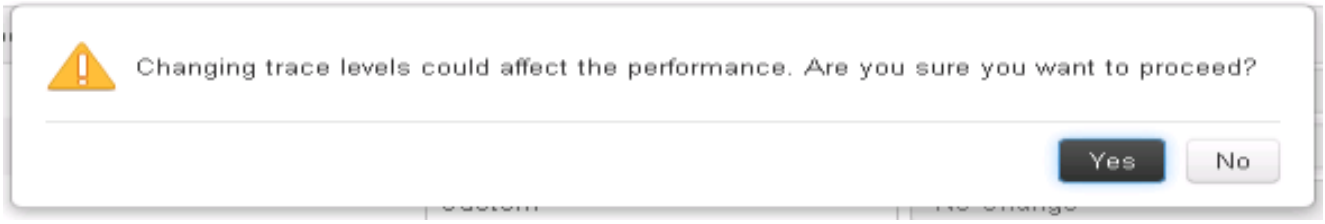
3. Na página Coleta de logs, clique em **Níveis de rastreamento**, que abre a caixa de diálogo **Níveis de rastreamento**.



4. Defina o nível de rastreamento como **detalhado** no CCE e deixe-o como **Sem alteração** para CM e CVP, depois clique em **Atualizar Níveis de Rastreamento.**



5. Clique em **Sim** para confirmar o aviso.



6. Após a reprodução do problema, abra o **Unified CCE Administration** e navegue de volta para **System > Coleta de logs.**
7. Selecione **CCE** e **CVP** no painel Componentes.
8. Selecione o Tempo de Coleta de Log apropriado (o default são os últimos 30 min).
9. Clique em **Collect Logs** e em **Yes** para o aviso da caixa de diálogo. A coleta de logs é iniciada. Aguarde alguns minutos antes que termine.

10. Quando terminar, clique no botão **Download** na coluna **Actions** para fazer o download de um arquivo zipado com todos os logs contidos nele. Save o arquivo **zip** em qualquer local que você achar apropriado.

Definir rastreamento e coletar registros CUIC/Live Data/IDS

Baixar logs com SSH

1. Faça login na linha de comando (CLI) SSH do CUIC, LD e IDS.

2. Execute o comando para coletar logs relacionados ao CUIC.

```
file get activelog /cuic/logs/cuic/*.* recurs compress reltime hours 1
file get activelog /cuic/logs/cuicsrvr/*.* recurs compress reltime hours 1
file get activelog tomcat/logs/*.* recurs compress
```

3. Execute o comando para coletar logs relacionados ao LD.

file get activelog livedata/logs/*.*

4. Execute o comando para coletar logs relacionados ao IdS.

file get activelog ids/log/*.* recurs compress reltime days 1

5. Esses logs são armazenados no caminho do servidor SFTP: <endereço IP>\<carimbo de data/hora>\ative_nnn.tgz , onde nnn é carimbo de data/hora em formato longo.

Baixar logs com RTMT

1. Faça o download da RTMT na página OAMP. Faça login em https://<HOST ADDRESS>/oamp, onde HOST ADDRESS é o endereço IP do servidor.

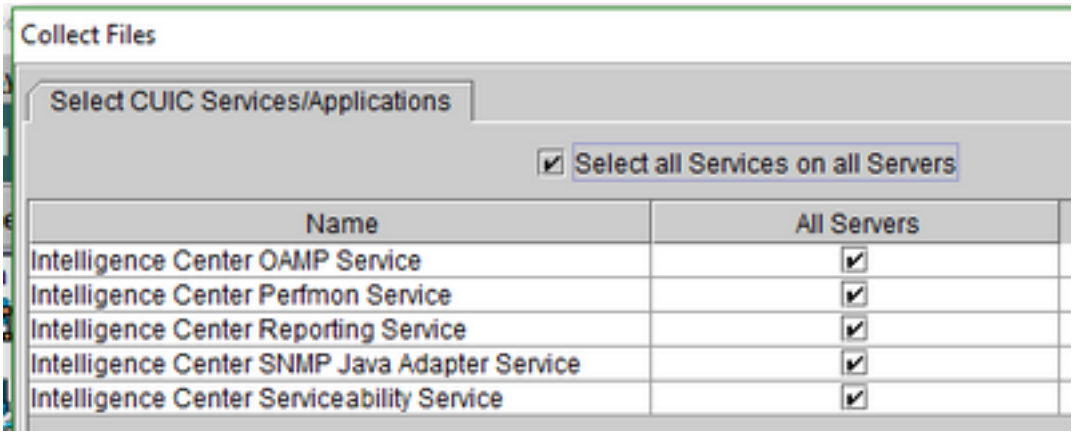
2. Navegue para **Ferramentas > RTMT** download plugin. Baixe e instale o plug-in.

3. Inicie a RTMT e faça logon no servidor com credenciais de administrador.

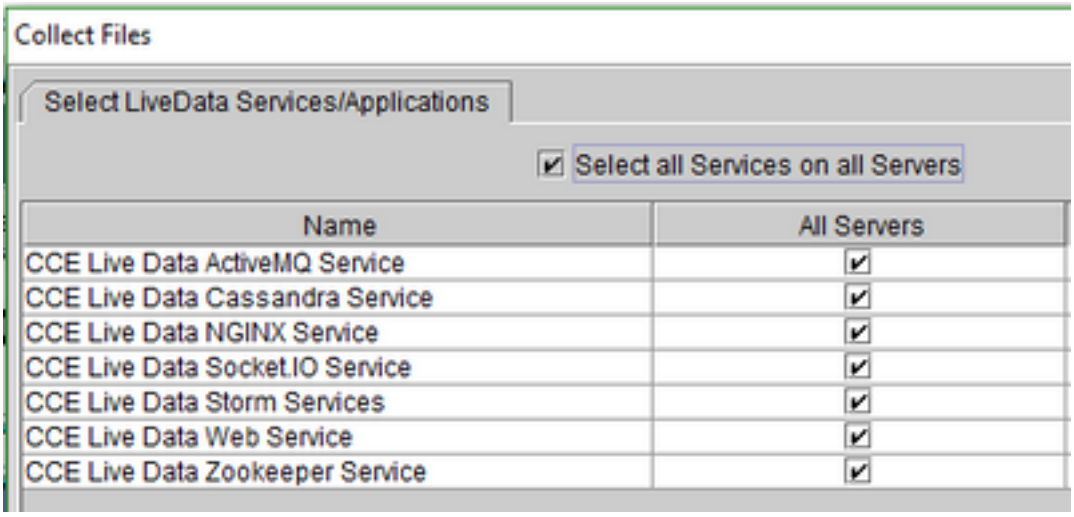
4. Clique duas vezes em **Trace and Log Central** e clique duas vezes em **Collect Files**.

5. Você pode ver essas guias para os serviços específicos. Você deve selecionar todos os serviços/servidores para CUIC, LD e IDS.

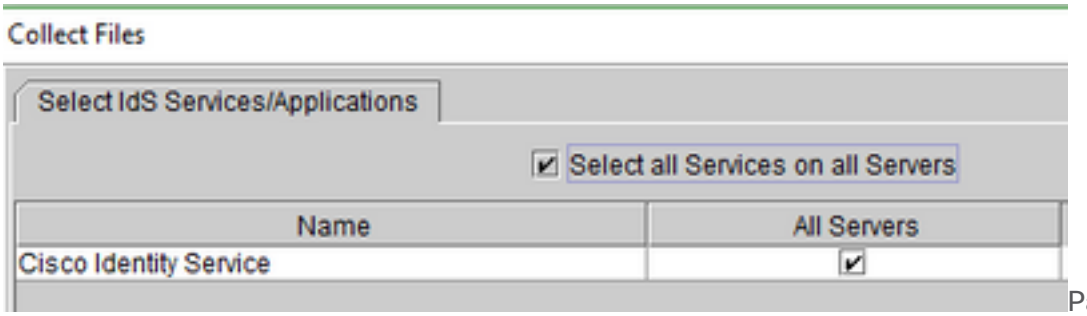
Para CUIC:



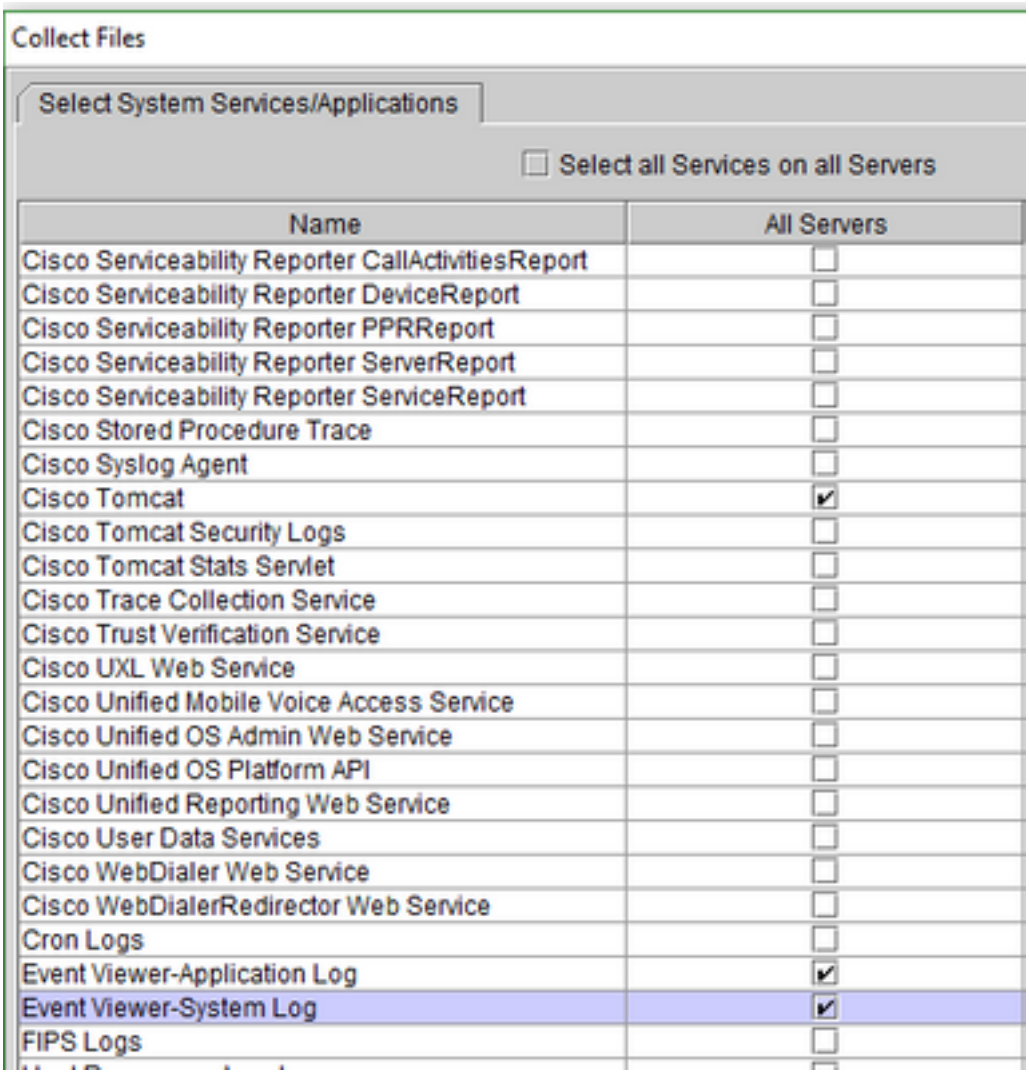
Para LD:



Para IDS:

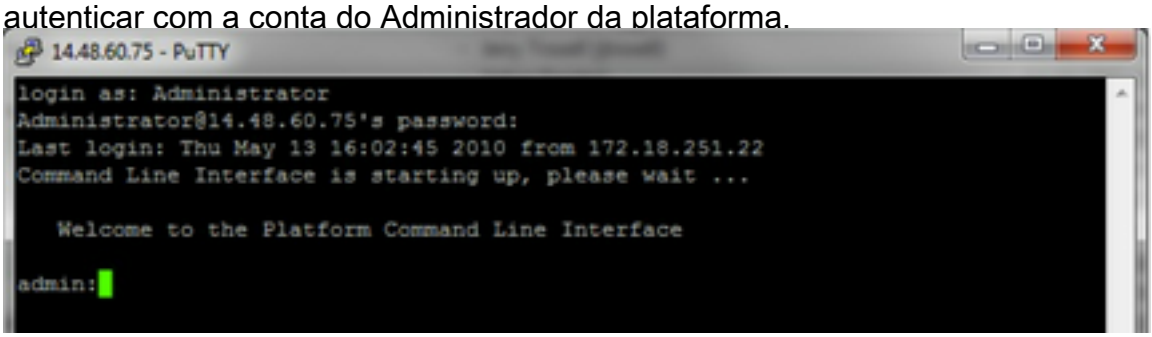


Para serviços de plataforma, geralmente é uma boa ideia selecionar registros do Tomcat e do visualizador de eventos:



6. Selecione a **Data e a Hora** junto com a pasta de destino para save os registros.

Captura de pacotes em VoS (Finesse, CUIC, VVB)

1. Iniciar a captura Para iniciar a captura, estabeleça uma sessão SSH para o servidor VOS autenticar com a conta do Administrador da plataforma.
2. 

1 bis. Sintaxe do comando

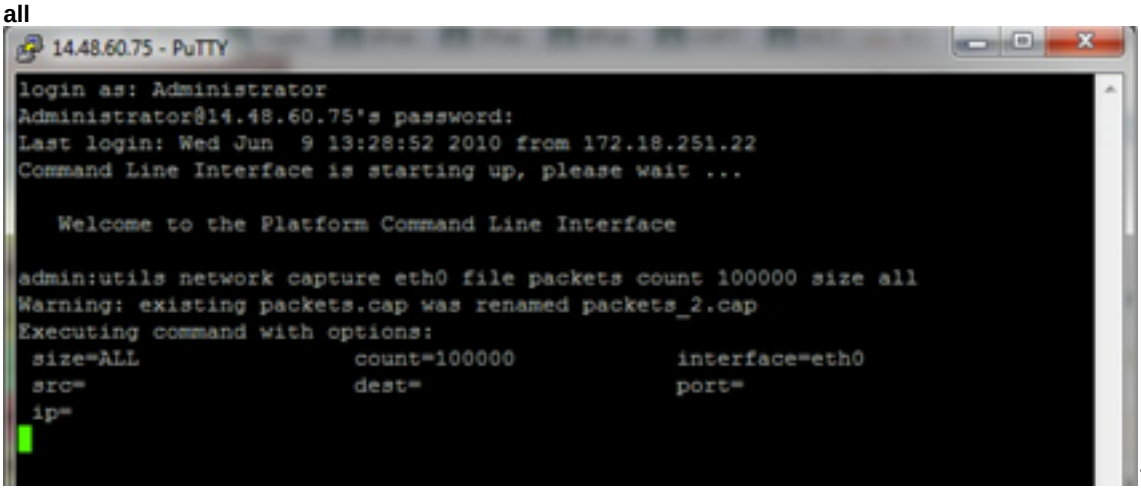
O comando é **utils network capture**e a sintaxe é a seguinte:

```
Syntax:
utils network capture [options]
options  optional
page,numeric,file fname,count num,size bytes,src addr,dest addr,port
```

```
num,host protocol addr
options are:
page
- pause output
numeric               - show hosts as dotted IP
addresses
file fname            - output the information to a file

Note: The file is saved in platform/cli/fname.cap

fname should not contain the "." character
count num             - a
count of the number of packets to capture
   Note: The maximum count
for the screen is 1000, for a file is 100000
size bytes            -
the number of bytes of the packet to capture
   Note: The maximum
number of bytes for the screen is 128
         For a file it can be
any number or ALL
src addr              - the source address of the
packet as a host name or IPV4 address
dest addr             - the
destination address of the packet as a host name or IPV4 address
port
num              - the port number of the packet (either src or dest)
host
protocol addr    - the protocol should be one of the following:
ip/arp/rarp/all. The host address of the packet as a host name or IPV4
address. This option  will display all packets to and from that address.

Note: If "host" is provided, do not provide "src" or "dest"
```

1-B. Capturar todos os tráfegos

Para uma captura típica, é possível coletar TODOS os pacotes de TODOS os tamanhos de e para TODOS os endereços em um arquivo de captura chamado **packets.cap**. Para fazer isso, basta executar na CLI do administrador **utils network capture eth0 file packets count 100000 size all**

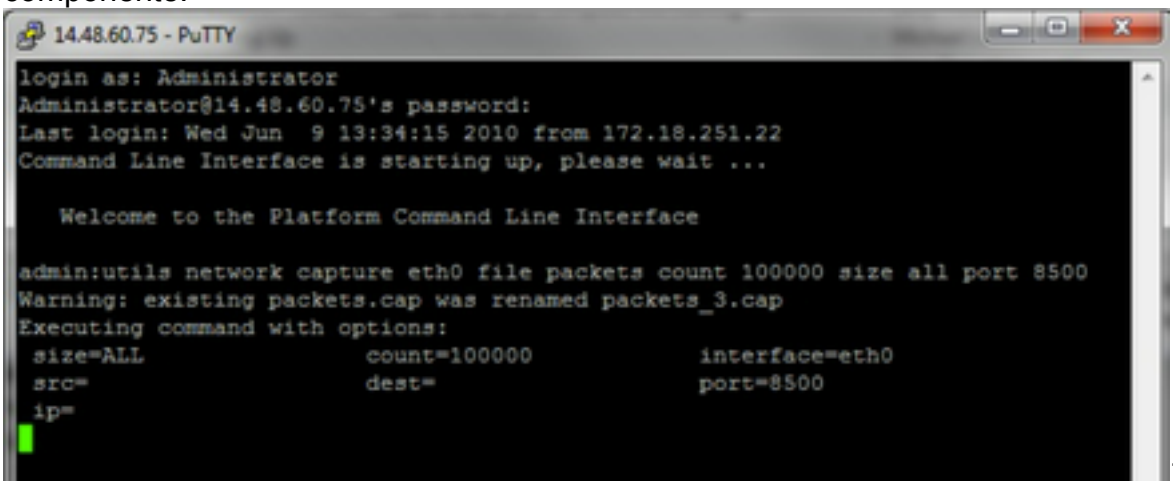


1 quater. Captura baseada no número da porta

Para solucionar um problema de comunicação com o Cluster Manager, pode ser desejável usar a opção de porta para capturar com base em uma porta específica (8500).

Para obter mais informações sobre quais serviços exigem comunicações em cada porta,

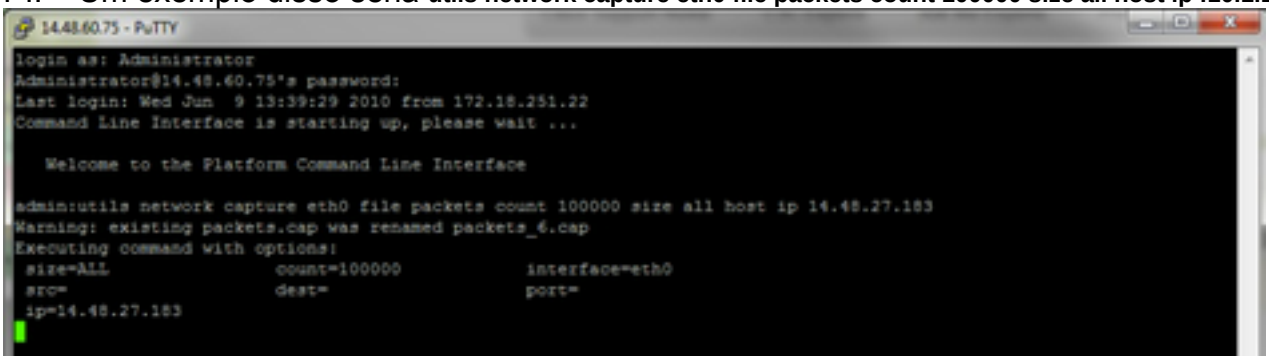
consulte oGuia de Uso de Portas TCP e UDP para obter a versão aplicável do respectivo componente.



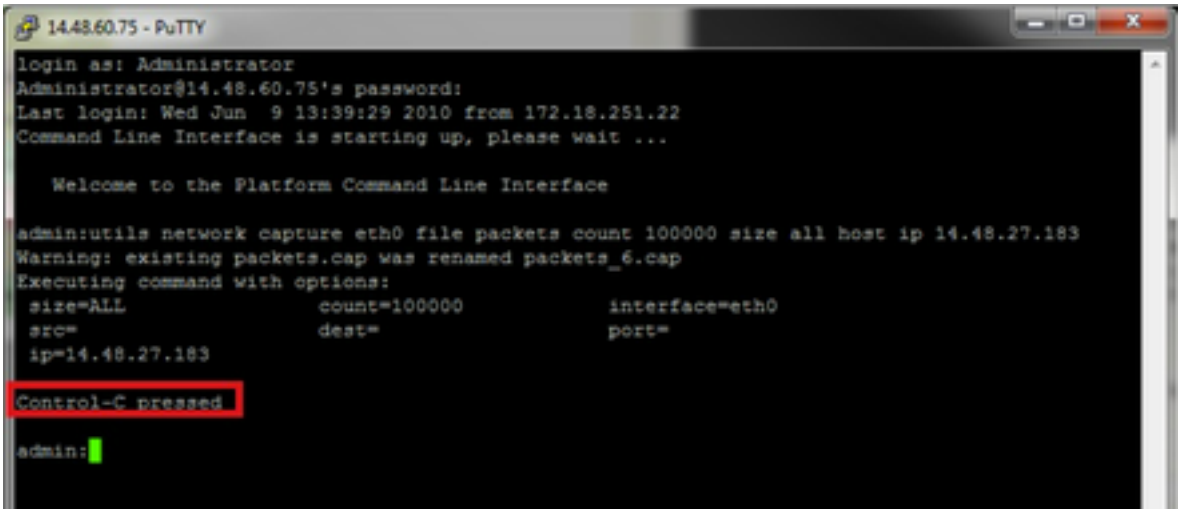
1d. Captura baseada no host

Para solucionar um problema com o VOS e um host específico, pode ser necessário usar a opção 'host' para filtrar o tráfego de e para um host específico.

Também pode ser necessário excluir um host específico, nesse caso, use um "!" antes do PI. Um exemplo disso seria **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**

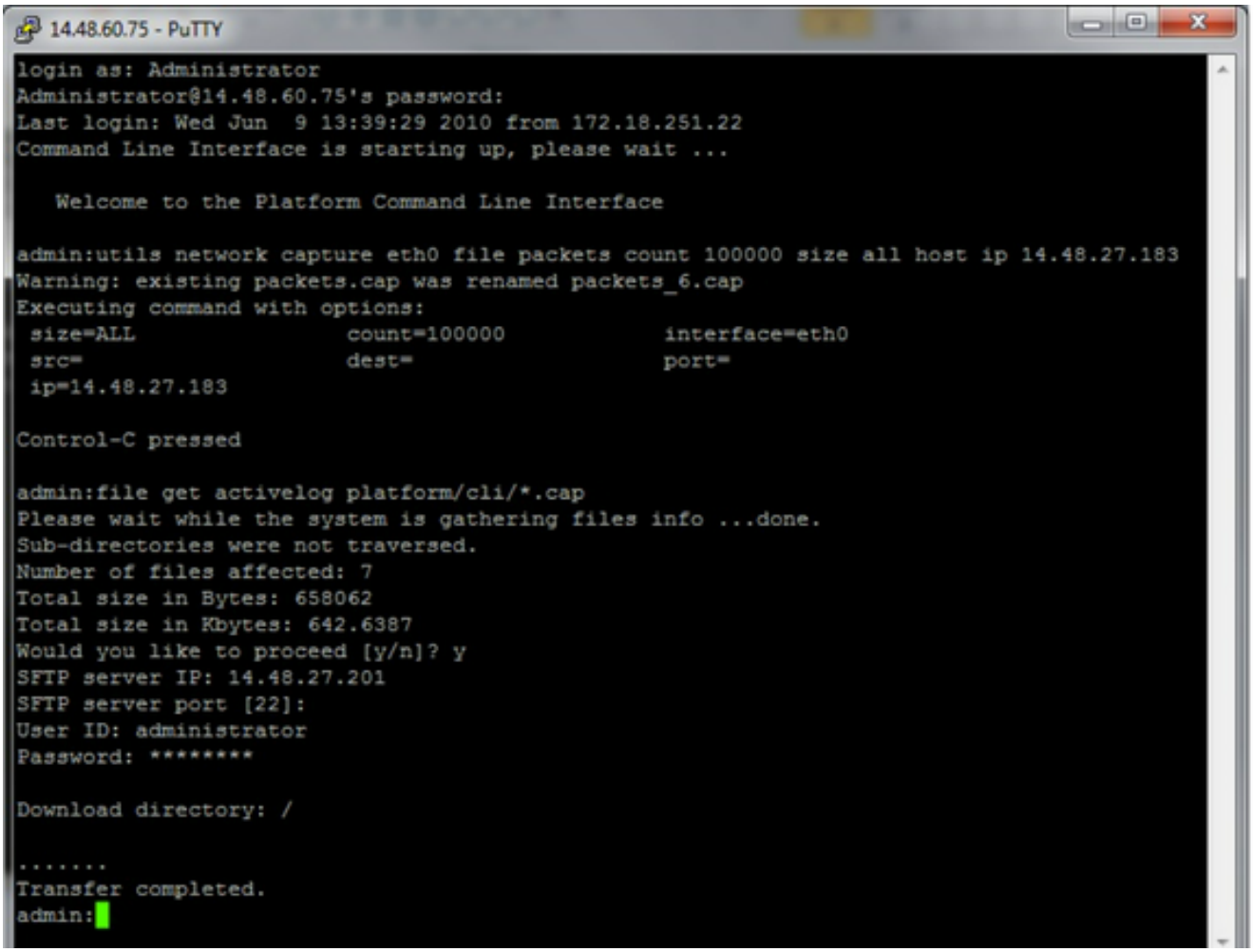


3. Reproduzir o sintoma do problema Enquanto a captura é iniciada, reproduza o sintoma ou condição do problema para que os pacotes necessários sejam incluídos na captura. Se o problema for intermitente, pode ser necessário executar a captura por um longo período. Se a captura for encerrada, é porque o buffer está preenchido, reinicie a captura e a captura anterior será renomeada automaticamente para que a captura anterior não seja perdida. Se uma captura for necessária por um longo período de tempo, use uma sessão de monitor em um switch para capturar no nível de rede.
4. Parar a captura Para interromper a captura, mantenha pressionada a tecla **Control** e pressione **C** no teclado. Isso faz com que o processo de captura termine e nenhum pacote novo seja adicionado ao dump de captura.
5.



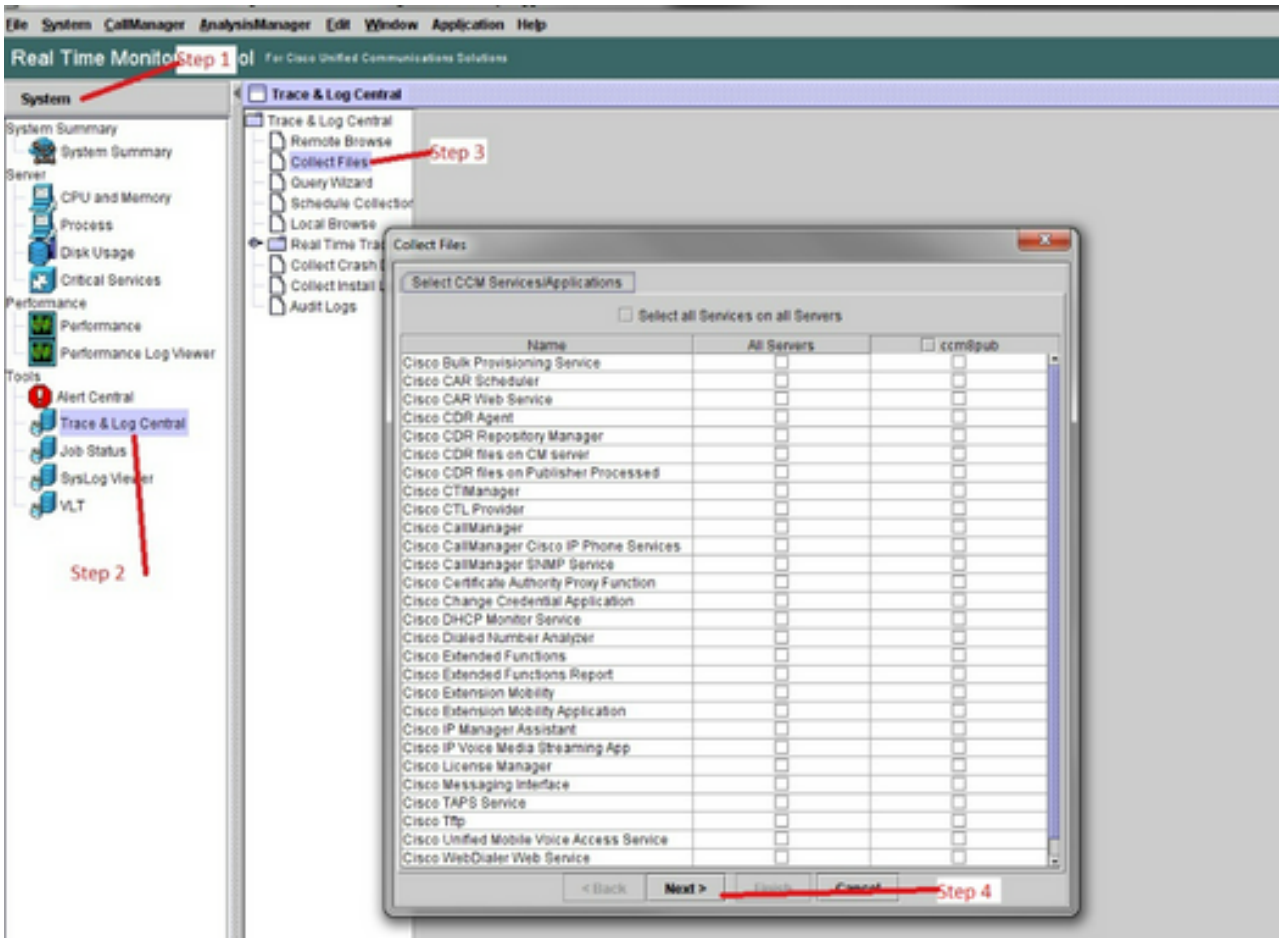
Quando isso for concluído, um arquivo de captura será armazenado no servidor no local 'ativelog platform/cli/'

6. Coletar a captura do servidor
   Os arquivos de captura são armazenados na localização "ativelog platform/cli/" no servidor. Você pode transferir os arquivos por meio da CLI para um servidor SFTP ou para o PC local com o RTMT. 4 bis. Transferir o arquivo de captura através do CLI para um servidor SFTP
   Use o comando **file get activelog platform/cli/packets.cap** para coletar o arquivo packets.cap para o servidor SFTP.
   Como alternativa, para coletar todos os arquivos .cap armazenados no servidor, use 'file get ativelog platform/cli/*.cap
   Por fim, preencha as informações de IP/FQDN, porta, nome de usuário, senha e diretório do servidor SFTP:

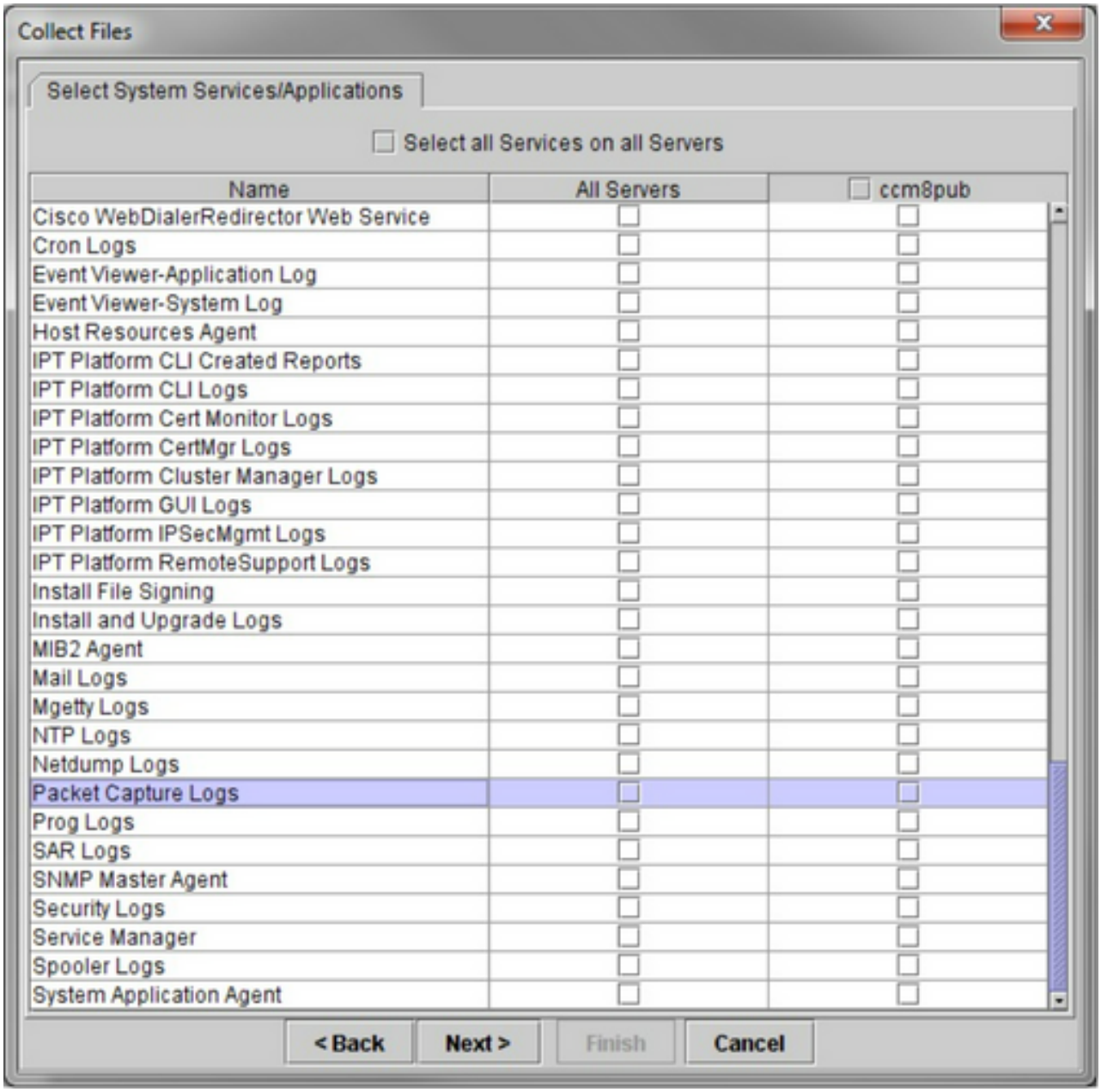


A CLI indica êxito ou falha na transferência de arquivos para o servidor SFTP.

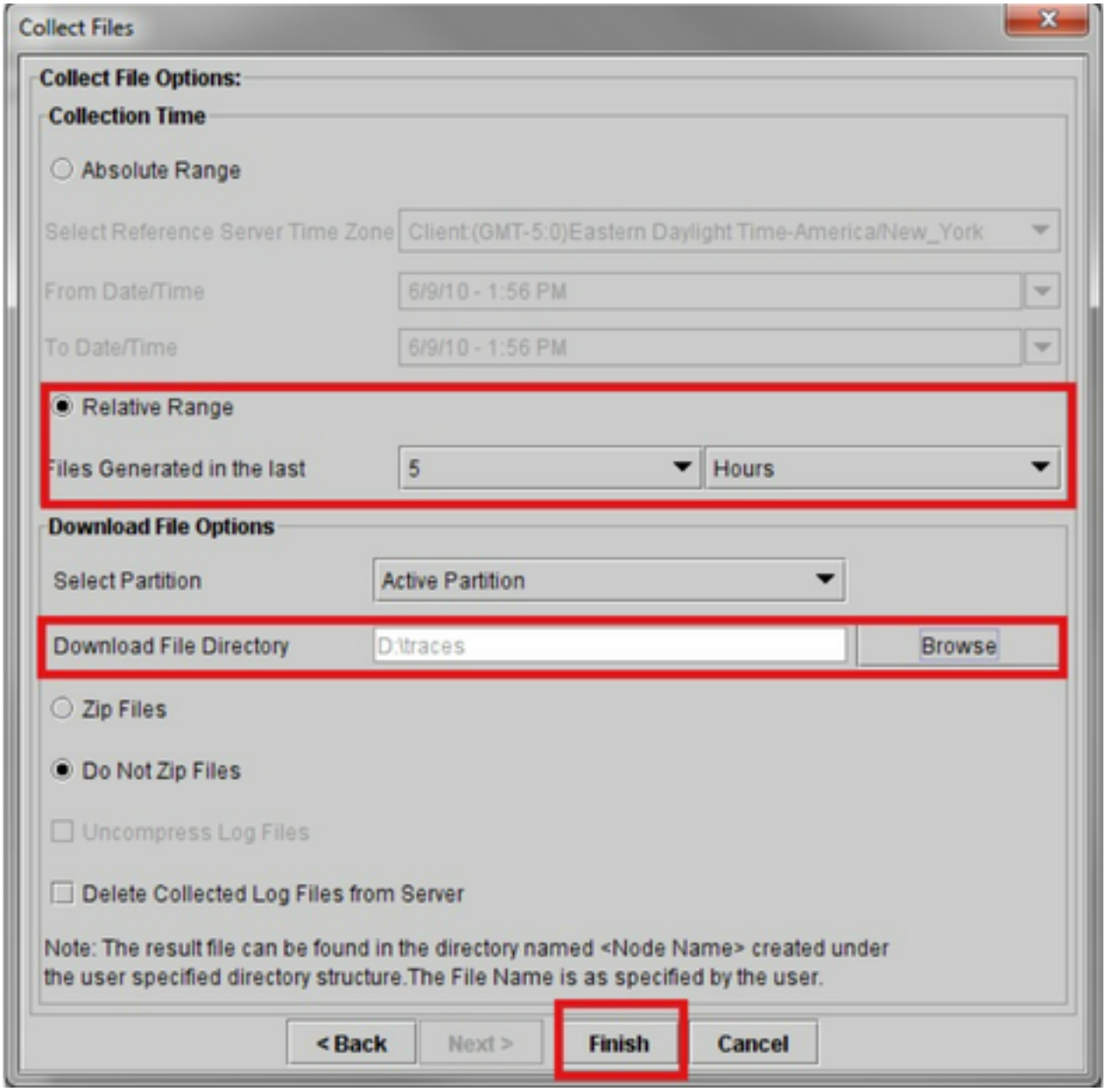
4-B. Use RTMT para transferir um arquivo de captura para um PC local.
Inicie o RTMT. Se ele não estiver instalado no PC local, instale a versão apropriada na página VOS Administration (Administração do VOS) e vá para o menu **Applications->Plugins**. Clique em **System**, em **Trace & Log Central** e clique duas vezes em **Coletar arquivos.** Clique em **Avançar** no primeiro menu.



No segundo menu, escolha a caixa de seleção para **Packet Capture Logs** no servidor em que a captura foi realizada e clique em **Next**.



Na tela final, escolha um intervalo de tempo quando a captura foi realizada e um diretório de download no PC local.



O RTMT fecha essa janela e continua coletando o arquivo e armazenando-o no PC local no local especificado.

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.