

Definir e coletar registros de rastreamento UCCE

Contents

[Introduction](#)

[Requirements](#)

[Configurações de rastreamento e coleta de logs](#)

[Finesse](#)

[Cisco Agent Desktop](#)

[Cisco Supervisor Desktop](#)

[Desktops cliente CTIOS](#)

[Problemas relacionados ao cliente com rastreamento e logon no PG](#)

[Depurar serviço de sincronização do CAD](#)

[Depurar o servidor RASCAL do CAD 6.0\(X\)](#)

[Debug Chat Server](#)

[Outros registros e rastreamento relacionados ao PG](#)

[Habilitar rastreamento de PIM do CallManager](#)

[Habilitar rastreamento no CUCM](#)

[Habilitar Gateway JGW \(Java Telephony Application Programming Interface\)](#)

[Ativar Rastreamento de Servidor CTI \(CTISVR\) no Lado Ativo](#)

[Habilitar rastreamento de PIM da URV](#)

[Habilitar rastreamento de servidor CTIOS em ambos os servidores CTIOS](#)

[Ativar Rastreamento OPC \(Open Peripheral Controller, Controlador de Periférico Aberto\) no PG ativo](#)

[Habilitar rastreamento Eagtpim no PG ativo](#)

[Use o utilitário Dumplog para puxar registros](#)

[Habilitar rastreamento em servidores CVP](#)

[Rastreamento e coleta de logs relacionados ao discador de saída](#)

[Logs de recebimento](#)

[Sobre o importador](#)

[No Campaignmanager](#)

[Ativar os logs do roteador no processo do roteador](#)

[Receber logs do roteador](#)

[Rastreamentos de gateway \(SIP\)](#)

[Rastreamento de CUSP](#)

[Uso de CLI para rastreamento](#)

[Exemplo de CLI](#)

Introduction

Este documento descreve como definir o rastreamento no Cisco Unified Contact Center

Enterprise (UCCE) para clientes, serviços de gateway periférico (PG), Cisco Customer Voice Portal (CVP), Cisco UCCE Outbound Dialer, Cisco Unified Communications Manager (CallManager) (CUCM) e gateways Cisco.

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Agent Desktop (CAD)
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Cisco Unified Communications Manager (CallManager) (CUCM)
- Gateways Cisco

Configurações de rastreamento e coleta de logs

Notas:

Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

A [ferramenta Output Interpreter \(exclusiva para clientes registrados\)](#) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Consulte [Informações Importantes sobre Comandos de Depuração antes de usar comandos debug](#).

Finesse

Faça login no servidor Finesse com o Shell Seguro (SSH) e insira esses comandos para coletar os registros necessários. Você é solicitado a identificar um servidor FTP SSH (SFTP) em que os registros serão carregados.

Logs

Instalar logs

Logs da área de trabalho

Logs do servm

Logs do Platform Tomcat

Logs de instalação do sistema operacional de voz (VOS)

Comando

```
arquivo get install desktop-install.log
```

```
arquivo get ativelog desktop recurse
```

```
compress
```

```
arquivo get ativelog platform/log/servm*.*
```

```
compress
```

```
arquivo get ativelog tomcat/logs compress
```

```
file get install install.log
```

Cisco Agent Desktop

Este procedimento descreve como criar e coletar arquivos de depuração:

1. No computador do agente, vá para o arquivo C:\Program Files\Cisco\Desktop\Config directory and open the Agent.cfg.
2. Altere o limite de depuração de OFF para **DEBUG**. O TRACE pode ser usado para um nível mais profundo.

```
[Debug Log]
Path=..\log\agent.dbg
Size=3000000
Threshold=DEBUG
```

3. Verifique o tamanho=3000000 (seis zeros).
4. Salve o arquivo de configuração.
5. Interrompa o programa do agente.
6. Exclua todos os arquivos no diretório C:\Program Files\Cisco\Desktop\log directory.
7. Inicie o programa do agente e recrie o problema.
8. Esses arquivos de depuração são criados e colocados em C:\Program Files\Cisco\Desktop\log:

agent0001.dbgctiosclientlog.xxx.log

Cisco Supervisor Desktop

Este procedimento descreve como criar e coletar arquivos de depuração:

1. No computador do agente, vá para o arquivo C:\Program Files\Cisco\Desktop\Config directory and open the supervisor.cfg.
2. Altere o LIMITE de depuração de OFF para **DEBUG**. O TRACE pode ser usado para um nível mais profundo.

```
[Debug Log]
Path=..\log\supervisor.dbg
Size=3000000
THRESHOLD=DEBUG
```

3. Verifique o tamanho=3000000 (seis zeros).
4. Salve o arquivo de configuração.
5. Interrompa o programa do agente.

6. Exclua todos os arquivos no diretório C:\Program Files\Cisco\Desktop\log directory.

7. Inicie o programa do agente e recrie o problema. Um arquivo de depuração chamado supervisor0001.dbg é criado e colocado em C:\Program Files\Cisco\Desktop\log.

Desktops cliente CTIOS

No PC cliente onde o cliente CTIOS está instalado, use Regedt32 para ativar o rastreamento. Altere estas configurações:

Versão	Localização do Registro	Valor padrão	alteram
Versões anteriores à versão 7.x	HKEY_LOCAL_MACHINE\Software\Cisco Systems\Ctios\Logging\TraceMask	0x07	Aumente o valor para 0xfff.
Versão 7.x e posterior	HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS Tracing	0x40000307	Defina o valor como 0xfff para a solução de problemas.

A saída padrão é criada e colocada em um arquivo de texto chamado CtiosClientLog na pasta c:\Program Files\Cisco Systems\CTIOS Client\CTIOS Desktop Phones\install directory.

Problemas relacionados ao cliente com rastreamento e logon no PG

Depurar serviço de sincronização do CAD

Estas são as configurações para depurar o serviço de sincronização do CAD:

Configuração	Valor
Arquivo de configuração	DirAccessSynSvr.cfg
Localização padrão	C:\Program Files\Cisco\Desktop\config
Problemas gerais	Limite=DEBUG
Arquivos de saída	DirAccessSynSvr.log

Depurar o servidor RASCAL do CAD 6.0(X)

Estas são as configurações para depurar o servidor RASCAL do CAD 6.0(X):

Configuração	Valor
Arquivo de configuração	FCRasSvr.cfg
Localização padrão	C:\Program Files\Cisco\Desktop\config
Problemas gerais	Intervalo = 1-4, 50, 3000-8000
Problemas relacionados ao LDAP:	Intervalo = 4000-4999

Problemas relacionados ao LRM:	Intervalo = 1999-2000
Problemas relacionados ao banco de dados	Intervalo = 50-59
Arquivos de saída	FCRasSvr.log, FCRasSvr.dbg
Localização padrão	C:\Program Files\Cisco\Desktop\log

Debug Chat Server

Estas são as configurações para depurar o servidor de bate-papo:

Configuração	Valor
Arquivo de configuração	FCCServer.cfg
Localização padrão	C:\Program Files\Cisco\Desktop\config
Problemas gerais	Limite=DEBUG
Arquivos de saída	FCCServer.log, FCCServer.dbg
Localização padrão	C:\Program Files\Cisco\Desktop\log

Outros registros e rastreamento relacionados ao PG

Consulte [Usar utilitário Dumplog para puxar registros](#) para coleta de logs.

Habilitar rastreamento de PIM do CallManager

Use o utilitário de monitoramento de processo (procmon) para ativar e desativar níveis de rastreamento. Esses comandos ativam o rastreamento do gerenciador de interface periférica (PIM) do CallManager:

```
C:\>procmon <Customer_Name> <PG_Name> <ProcessName>
>>>trace tp* !-- Turns on third party request tracing
>>>trace precall !-- Turns on precall event tracing
>>>trace *event !-- Turns on agent and call event tracing
>>>trace csta* !-- Turns on CSTA call event tracing
>>>ltrace !-- Output of all trace bits
>>>q !-- Quits
```

Este comando procmon desativa o rastreamento PIM do CallManager:

```
>>>trace * /off
```

Habilitar rastreamento no CUCM

Este procedimento descreve como ativar o rastreamento CUCM:

1. Vá para Call Manager Unified Serviceability.
2. Selecione **Trace/Configuration**.
3. Selecione **Serviços CM**.

4. Selecione **CTIManager (Ativo)**.
5. Na parte superior direita, selecione **SDL Configuration**.
6. Habilite tudo, exceto Desabilitar impressão direta do rastreamento SDL.
7. Deixe o número de arquivos e seus tamanhos nos valores padrão.
8. Na Real-Time Monitoring Tool (RTMT), reúna o Cisco Call Manager e o Cisco Computer Telephony Integration (CTI) Manager. Ambos têm registros de interface de diagnóstico do sistema (SDI) e camada de distribuição de sinal (SDL).

Habilitar Gateway JGW (Java Telephony Application Programming Interface)

Esses comandos procmon ativam o rastreamento JGW:

```
C:\procmon <Customer_Name> <node> process
>>>trace JT_TPREQUESTS !-- Turns on third-party request traces
>>>trace JT_JTAPI_EVENT_USED !-- Turns on traces for the JTAPI Events the PG uses
>>>trace JT_ROUTE_MESSAGE !-- Turns on routing client traces
>>>trace JT_LOW* !-- Traces based on the underlying JTAPI and CTI layers
```

Um comando de exemplo é **procmon ipcc pg1a jgw1**.

Ativar Rastreamento de Servidor CTI (CTISVR) no Lado Ativo

Este procedimento descreve como ativar o rastreamento CTISVR no lado ativo:

1. Use o editor do Registro para editar HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a e b)\EMS\CurrentVersion\library\Processes\ctisvr.
2. Defina EMSTraceMask = f8.

Habilitar rastreamento de PIM da URV

Note: Os comandos diferenciam maiúsculas e minúsculas. O Gateway Periférico da Unidade de Resposta de Voz (URV) é diferente do Gateway Periférico do Cisco CallManager (CCM).

Esses comandos procmon ativam o rastreamento para VRU PIM:

```
C:\procmon <Customer_Name> <PG_Name> <ProcessName>
procmon>>>trace *.* /off !-- Turns off
procmon>>>trace !-- Verifies what settings are on/off
procmon>>>trace cti* /onprocmon>>>trace opc* /on
procmon>>>trace *ecc* /onprocmon>>>trace *session* /off
procmon>>>trace *heartbeat* /off
procmon>>>ltrace /traceprocmon>>>quit
```

Este comando procmon desativa o rastreamento do PIM da URV:

```
>>>trace * /off
```

Habilitar rastreamento de servidor CTIOS em ambos os servidores CTIOS

Este procedimento descreve como ativar o rastreamento em ambos os servidores CTIOS:

1. Anote a máscara de rastreamento atual para uso posterior.
2. Use o editor do registro para editar HLKM >> Software\Cisco Systems Inc.\ICM\<cust_inst>\CTIOS\EMS\CurrentVersion\library\Processes\ctios.
3. Configurado:
 - Máscara de corrida EMST = 0x60A0F
 - EMSTraceMask para um destes valores, dependendo da versão:
 - 0x0A0F para Versão 6.0 e anterior
 - 0x20A0F para as versões 7.0 e 7.1(1)
 - 0x60A0F para a versão 7.1(2) e posterior

A máscara de rastreamento padrão é 0x3 em todas as versões, exceto a versão 7.0(0), onde é 0x20003.

Se a máscara de rastreamento tiver um alto valor (0xf ou superior), haverá um grande impacto no desempenho do servidor CTIOS e na taxa de conclusão de chamada. Defina a máscara de rastreamento com um valor alto somente quando estiver depurando um problema; depois de coletar os registros necessários, você deve definir a máscara de rastreamento de volta ao valor padrão.

Para fins de solução de problemas, defina a máscara de rastreamento do servidor CTIOS como:

- 0x0A0F para Versão 6.0 e anterior
- 0x20A0F para as versões 7.0 e 7.1(1)
- 0x60A0F para a versão 7.1(2) e posterior

Ativar Rastreamento OPC (Open Peripheral Controller, Controlador de Periférico Aberto) no PG ativo

Esses comandos opctest ativam o rastreamento OPC em um PG ativo:

```
opctest /cust <cust_inst> /node <node>  
opctest:debug /agent /routing /cstacer /tpmsg /closedcalls
```

Este é um exemplo de um ambiente de laboratório:

```
C:\Documents and Settings\ICMAdministrator>opctest /cust ccl /node pgl  
OPCTEST Release 8.0.3.0 , Build 27188  
opctest: debug /agent /routing /cstacer /tpmsg /closedcalls !-- Use debug /on in  
order to restore default tracing levels  
opctest: quit
```

Exemplos adicionais são:

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg
!-- General example
```

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /NCT
!-- Network transfer example
```

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /task /passthru
!-- Multimedia example
```

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /passthru
!-- VRU PG example
```

Habilitar rastreamento Eagtpim no PG ativo

Esses comandos procmon ativam o rastreamento eagtpim em um PG ativo:

```
C:\>procmon <cust_inst> <node> pim<pim instance
>>>>trace tp* /on
>>>trace precall /on
>>>trace *event /on
>>>trace csta* /on
```

Este é um exemplo de um ambiente de laboratório:

```
C:\Documents and Settings\ICMAdministrator>procmon ccl pgl pml
>>>>trace tp* /on
>>>>trace precall /on
>>>>trace *event /on
>>>>trace csta* /on
>>>>quit
```

Use o utilitário Dumplog para puxar registros

Consulte [Como usar o utilitário Dumplog](#) para obter detalhes adicionais. Use o comando **cdlog** para chegar ao diretório logfiles, como mostrado neste exemplo:

```
c:\cdlog <customer_name> pgl !-- Or, pgXa to depending on the PG number (X)
c:\icm\<customer_name>\<<PG#>>\logfiles\
```

Estes exemplos mostram como colocar a saída no arquivo padrão; em todos os casos, você pode usar **/de** para definir um nome específico para o arquivo de saída:

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog pml /bt <HH:MM> /et <HH:MM> /ms /o
!-- This PIM example places output in a default pml.txt file
```

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog opc /bt <HH:MM> /et <HH:MM> /ms /o
!-- This OPC example places output in a default opc.txt file
```

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog jgw1 /bt <HH:MM> /et <HH:MM> /ms /o
c:\cdlog <customer_name> cgl
c:\icm\<customer_name>\<cg#>\logfiles\
!-- This JTAPI example places output in a default jgw1.txt file
```

```
c:\icm\<customer_name>\cg#\logfiles\dumplog ctisvr /bt <HH:MM> /et <HH:MM> /ms /o
!-- This CTI server example places output in a default ctisvr.txt file
```



```
c:\ icm\\ctios\logfiles\dumplog ctios /bt <HH:MM> /et <HH:MM> /ms /o
!-- This CTIOS server example places output in a default ctios.txt file
```

Habilitar rastreamento em servidores CVP

SIP

Este procedimento descreve como ativar o rastreamento em servidores CVP com o software do Telefone IP Cisco SIP:

1. No(s) servidor(es) de chamadas, vá para a ferramenta de diagnóstico CVP ([http://localhost\(CallServer\):8000/cvp/diag](http://localhost(CallServer):8000/cvp/diag)) para obter a pilha do Session Initiation Protocol (SIP).
2. Adicione com.dynamicsoft.Dslibs.DsUAlibs com debug.
3. Clique em **Definir**.
4. Clique em **DEBUG/41**.

H323

Este procedimento descreve como ativar o rastreamento em servidores CVP com um gateway H323:

1. No(s) servidor(es) de chamadas, faça login no VBAAdmin.
2. Ative estes rastreamentos para o navegador de voz CVP:

```
setcalltrace on
setinterfacetrace on
```

Receber registros CVP de servidores de chamada

Colete os arquivos CVP *.log e Error.log durante o período de teste. Esses arquivos estão no diretório C:\Cisco\CVP\logs directory on both CVP servers.

Estes são os locais dos arquivos de log do Unified CVP, onde CVP_HOME é o diretório em que o software Unified CVP está instalado.

Tipo de registro

Registros do servidor de chamadas e/ou do servidor de relatórios
Logs do console de operações
Logs do servidor XML de voz (VXML)
Logs de agente do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol)
Logs do gerenciador de recursos do Unified CVP

Local

CVP_HOME\logs\
CVP_HOME\logs\C
CVP_HOME\logs\V
CVP_HOME\logs\S
CVP_HOME\logs\C

Um exemplo de local é C:\Cisco\CVP.

Logs do VXML Server

Para aplicativos XML de voz personalizados, como um aplicativo auxiliar implantado, você pode ativar um depurador de log.

Adicione esta linha à seção <loggers> (a última seção) do arquivo de configuração settings.xml no diretório C:\Cisco\CVP\VXMLServer\applications\APP_NAME\data\application\ directory:

```
<logger_instance name="MyDebugLogger"  
class="com.audium.logger.application.debug.ApplicationDebugLogger"/>
```

Em tempo de execução, este logger envia um registro VoiceXML detalhado para o diretório \Cisco\CVP\VXMLServer\applications\APP_NAME\MyDebuggerLogger directory.

Note: Você pode alterar o nome do logger no arquivo de configuração settings.xml de MyDebugLogger para qualquer nome escolhido.

Rastreamento e coleta de logs relacionados ao discador de saída

Este procedimento descreve como aumentar os registros de processo do badialer no Outbound Dialer (que geralmente é encontrado em um PG).

1. Verifique se EMSDisplaytoScreen = 0.
2. Use o editor do registro para editar HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialer.
3. Configurado:
 - Máscara de corrida EMST = 0xff
 - EMSUserData = ff (quatro f's no modo binário)
4. Use o editor do registro para editar HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer.
5. Defina DebugDumpAllEvents = 1.

Logs de recebimento

Execute o utilitário dumplog do diretório /icm/<instance>/dialer/logfiles:

```
dumplog badialer /bt hh:mm:ss /et hh:mm:ss /o
```

Sobre o importador

Este procedimento descreve como aumentar o log do processo de importação básica.

1. Use o editor do registro para editar HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\- 2. Configurado:
 - Máscara de corrida EMST = 0xff
 - EMSUserData = ff (quatro f's no modo binário)
- 3. Execute o utilitário dumplog do diretório /icm/<instance>/la/logfiles:

```
dumplog balmport /bt hh:mm:ss /et hh:mm:ss /o
```

No Campaignmanager

Este procedimento descreve como aumentar o registro de processo do gerenciador de campanhas.

1. Use o editor do registro para editar HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\- 2. Configurado:
 - Máscara de corrida EMST = 0xff
 - EMSUserData = ff (quatro f's no modo binário)
- 3. Execute o utilitário dumplog do diretório /icm/<instance>/la/logfiles:

```
dumplog campaignmanager /bt hh:mm:ss /et hh:mm:ss /o
```

No Avaya Communications Manager (ACD) PG, use o utilitário **opctest** para aumentar o seguinte para o CallManager e a Avaya.

```
C:\opctest /cust <instance> /node <pgname>
opctest: type debug /agent /closedcalls /cstacer /routing
opctest: q !-- Quits
```

Este procedimento descreve como aumentar o rastreamento para o processo ctisvr.

1. Use o editor de registro para editar HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr.
2. Defina EMSTraceMask = f8. Você pode deixar o valor em f0 se desejar.

Ativar os logs do roteador no processo do roteador

Este procedimento descreve como ativar os logs do roteador:

1. No roteador, navegue até **Start > Run** e digite **trtrtrace**.
2. digite o nome do cliente.
3. Clique em Conectar.
4. Selecione estas opções:

alterações de agentesolicitações de roteadoresscriptselectsnetworkvrutracingrota de traduçãoenfileiramento de chamadascalltyperealtime

5. Clique em Apply.

6. Saia do utilitário.

Para o opctest Versão 8.5, use o Diagnostic Framework Portico.

```
debug level 3 component "icm:Router A" subcomponent icm:rtr
```

Receber logs do roteador

Use o utilitário dumplog para extrair os logs do roteador de qualquer um dos roteadores durante o período dos testes. Consulte [Como usar o utilitário Dumplog](#) para obter detalhes adicionais.

Este é um exemplo de uma solicitação de log para logs em 21/10/2011 entre 9:00:00 e 9:30:00 (no formato de 24 horas). Esta saída vai para o arquivo C:/router_output.txt:

```
C:\Documents and Settings\ICMAdministrator>cdlog u7x ra
C:\icm\u7x\ra\logfiles>dumplog rtr /bd 10/21/2011 /bt 09:00:00 /ed 10/21/2011
/et 09:30:00 /ms /of C:/router_output.txt
```

Envie o arquivo de saída (C:/router_output.txt) para a Cisco para solução de problemas, se necessário.

Rastreamentos de gateway (SIP)

Esses comandos ativam o rastreamento em servidores CVP com SIP:

```
#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
```

Note: Qualquer alteração em um GW do software Cisco IOS[®] de produção pode causar uma interrupção.

Essa é uma plataforma muito robusta que pode lidar com as depurações sugeridas no volume de chamadas fornecido sem problemas. No entanto, a Cisco recomenda que você:

- Enviar todos os registros 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
```

Note: Se a CPU obtiver até 70 a 80% de utilização da CPU, o risco de um impacto de serviço relacionado ao desempenho aumentará muito. Portanto, não habilite depurações adicionais se o GW atingir 60%.

Ative estas depurações:

```
debug isdn q931
debug voip ccapi inout
debug ccsip mess
debug http client all
debug voip application vxml all
debug vtsp all
debug voip application all
```

Depois de fazer a chamada e simular o problema, pare a depuração:

```
#undebug all
```

Coletar esta saída:

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

Rastreamento de CUSP

Esses comandos ativam o rastreamento SIP no Cisco Unified SIP Proxy (CUSP):

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

Lembre-se de desligar o login quando terminar.

Este procedimento descreve como coletar os registros:

1. Configure um usuário no CUSP (por exemplo, teste).

2. Adicione esta configuração no prompt do CUSP:

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

3. FTP para o endereço IP do CUSP. Use o nome de usuário (teste) e a senha conforme definido na etapa anterior.

4. Altere diretórios para /cusp/log/trace.

5. Obtenha o log_<filename>.

Uso de CLI para rastreamento

No UCCE Versão 8 e posterior, você pode usar a Interface de Linha de Comando (CLI - Command-Line Interface) do Unified System para coletar rastreamentos. Comparado aos utilitários de dumplog, o CLI é um método muito rápido e eficiente para obter um conjunto inteiro de registros de um servidor, como um PG ou Rogger.

Este procedimento descreve como iniciar a análise de problemas e como determinar qual rastreamento ativar. O exemplo coleta registros desses servidores:

- ROTEADOR A/ROTEADOR B
- LOGGER-A/LOGGER-B
- PGXA/PGXB
- Todos os servidores de chamada CVP
- Todos os servidores CVP VXML/Media (se presentes)

1. Em cada sistema na lista, abra o Unified System CLI em cada servidor e execute este comando:

```
show tech-support absdatetime mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm redirect
dir c:\temp
```

Substitua primeira string *mm-dd-aaaa:hh:mm* por uma data e hora aproximadamente 15 minutos antes do evento.

Substitua segunda string *mm-dd-aaaa:hh:mm* por uma data e hora aproximadamente 15 minutos após o evento ser resolvido. Se o evento ainda estiver ocorrendo, reúna pelo menos 15 minutos. Isso produz um arquivo chamado clioutputX.zip, em que X é o próximo número na sequência.

2. Exporte os registros de aplicativos/segurança/sistema do Windows de cada sistema no formato CSV (valores separados por vírgula) e salve no diretório C:\Temp directory.

3. Adicione os registros CSV do Windows ao zip da etapa 1 e renomeie o arquivo zip neste formato:

<SERVERNAME>-SystCLILogs-EvntOn-YYYYMMDD_HMMSS.zip

4. Em qualquer PG do agente, colete os logs no diretório C:\Program Files\Cisco\Desktop\logs every time the failure is seen. Envie os logs para um arquivo com um nome neste formato:

<SERVERNAME>-CADLogs-EvntOn-YYYYMMDD_HHMMSS.zip

Se você estiver usando o CAD-Browser Edition (CAD-BE) ou qualquer produto da Web CAD, reúna os logs do diretório C:\Program Files\Cisco\Desktop\Tomcat\logs directory e adicione-os ao mesmo arquivo zip.

Se você estiver executando em qualquer um dos produtos Windows 2008 x64, o diretório de log está em C:\Program Files (x86)\Cisco\Desktop\...

5. Anexe esses arquivos à solicitação de serviço ou carregue-os no FTP se forem muito grandes para enviar e-mail ou anexar.

Reúna essas informações adicionais, se possível:

- A hora de início e de término do evento.
- Vários exemplos de ANI/DNIS/AgentID envolvidos no evento. No mínimo, a Cisco precisa de pelo menos um desses para ver o evento.
- RouteCallDetail (RCD) e TerminationCallDetail (TCD) para o período de tempo que envolve o evento. A consulta RCD é:

```
SELECIONE * FROM Route_Call_Detail WHERE DbDateTime > 'AAAA-MM-DD
```

```
HH:MM:SS.MMM' e DbDateTime < 'AAAA-MM-DD HH:MM:SS.MMM'
```

```
A consulta TCD é:
```

```
SELECIONE * FROM Termination_Call_Detail WHERE DbDateTime > 'AAAA-MM-DD
```

```
HH:MM:SS.MMM' e DbDateTime < 'AAAA-MM-DD HH:MM:SS.MMM'
```

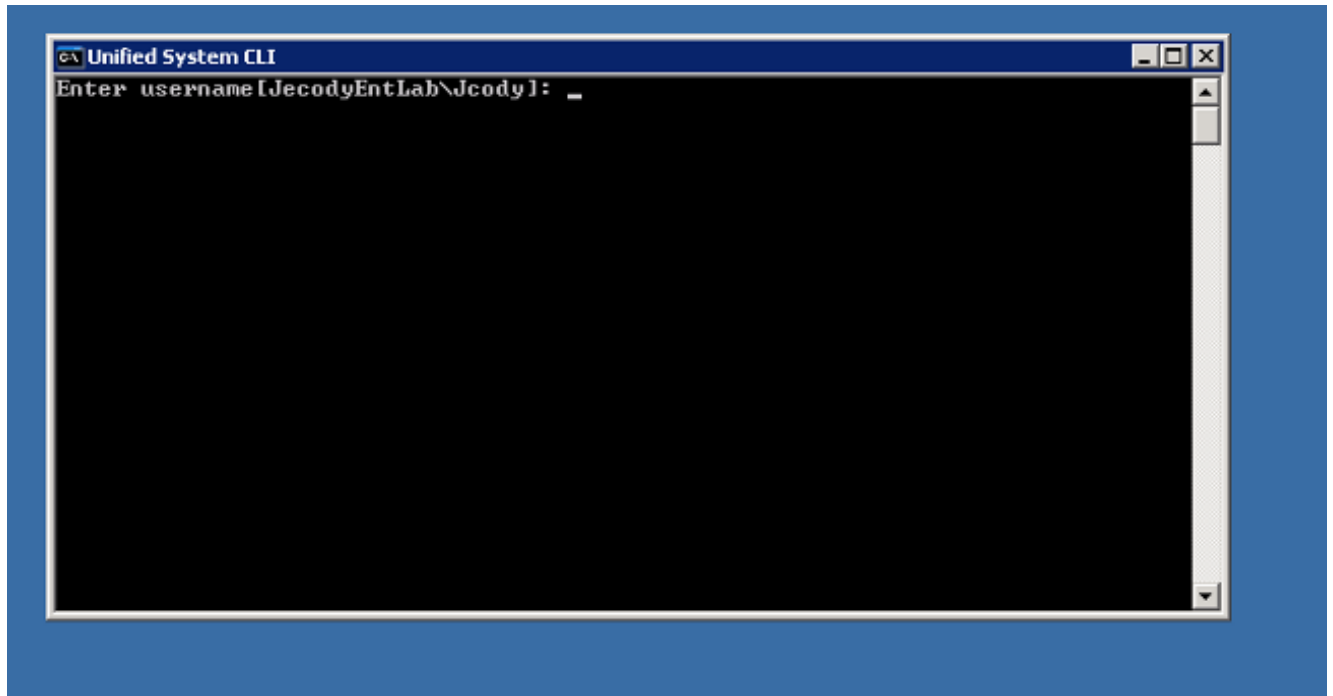
Exemplo de CLI

Note: Você é avisado de que essas ações podem afetar o sistema, portanto, talvez seja conveniente fazer esse trabalho durante horas de folga ou durante um tempo lento.

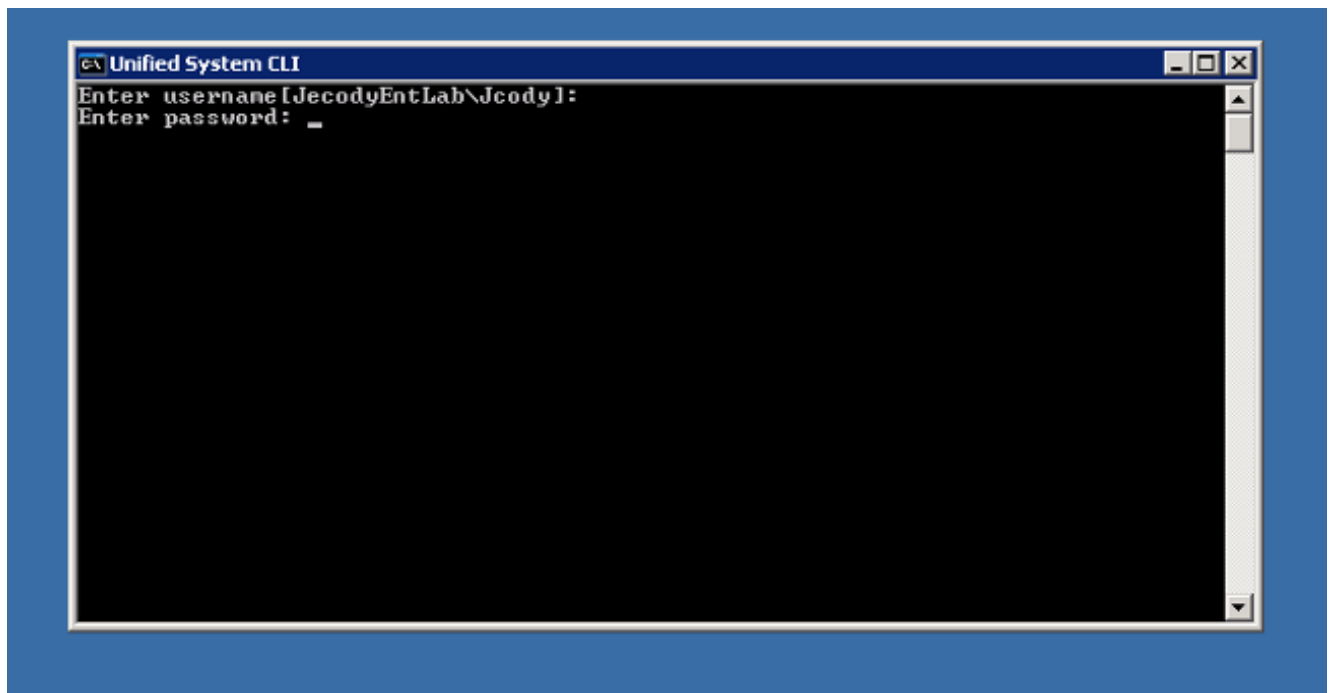
Há duas ferramentas: uma ferramenta Estrutura de diagnóstico e a ferramenta CLI do sistema. Ambos são ícones na área de trabalho ou no diretório Programas de cada servidor.

Este procedimento descreve como usar a CLI do Unified System para rastreamento.

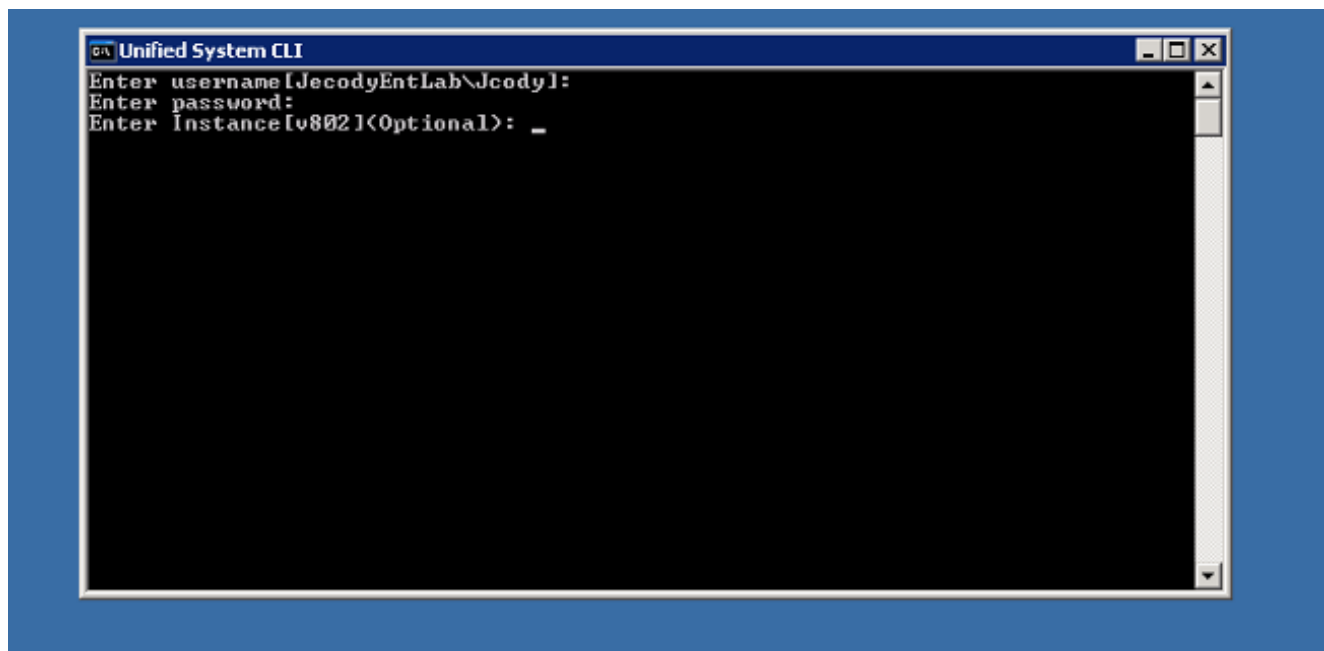
1. Clique no ícone da CLI do Unified System e faça login com o domínio e o nome de usuário. (Neste exemplo, o administrador do domínio já fez logon antes, portanto, a CLI já conhece o domínio (JecodyEntLab) e o nome de usuário (Jcody).



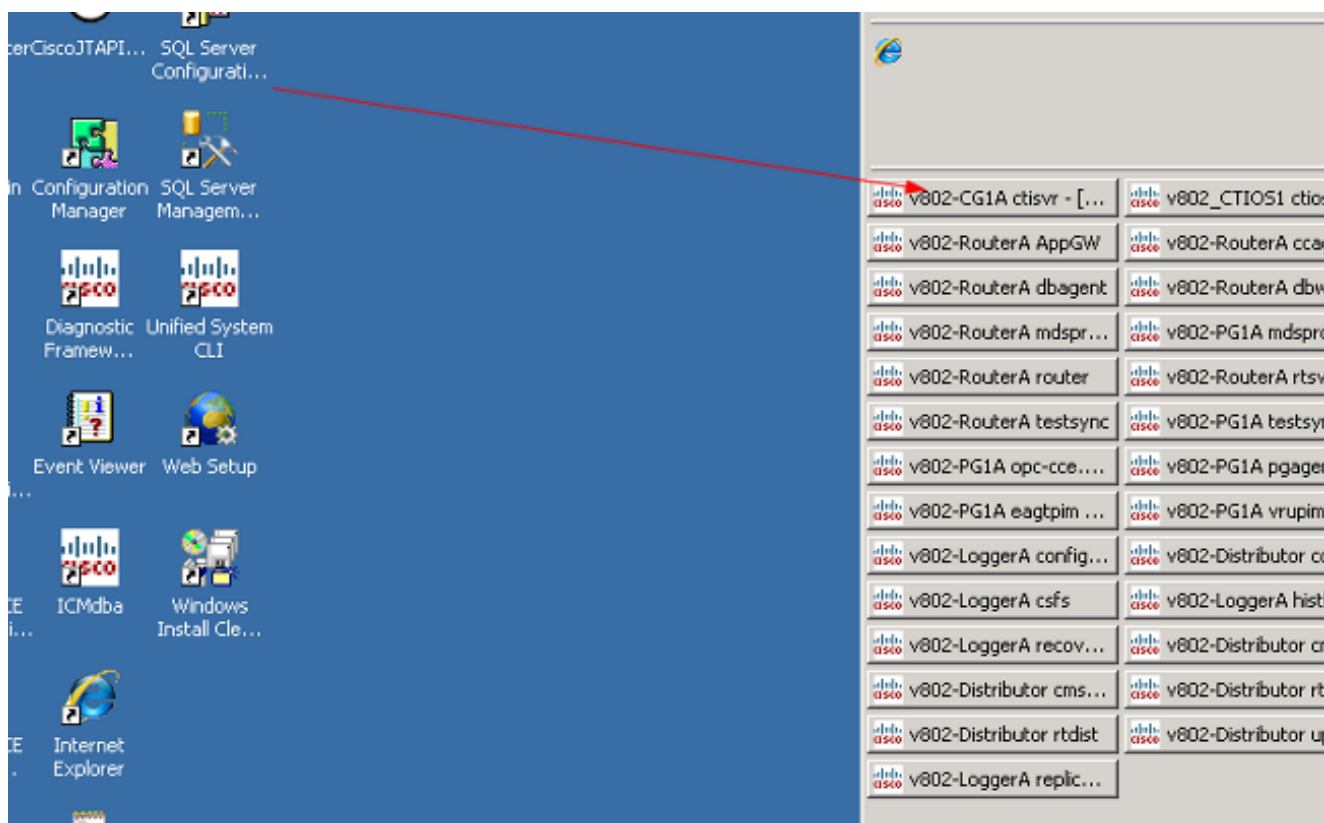
2. Digite a senha.



3. Digite o nome da instância; neste exemplo, é v802. Veja o PG em um dos serviços; o nome da instância é a primeira parte do nome do serviço.



4. Uma maneira simples de encontrar o nome da instância é observar os serviços que estão sendo executados no servidor.



5. Depois de ver a mensagem de boas-vindas, digite este comando:

```
show tech-support absdatetime mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm redirect dir c:\temp
```

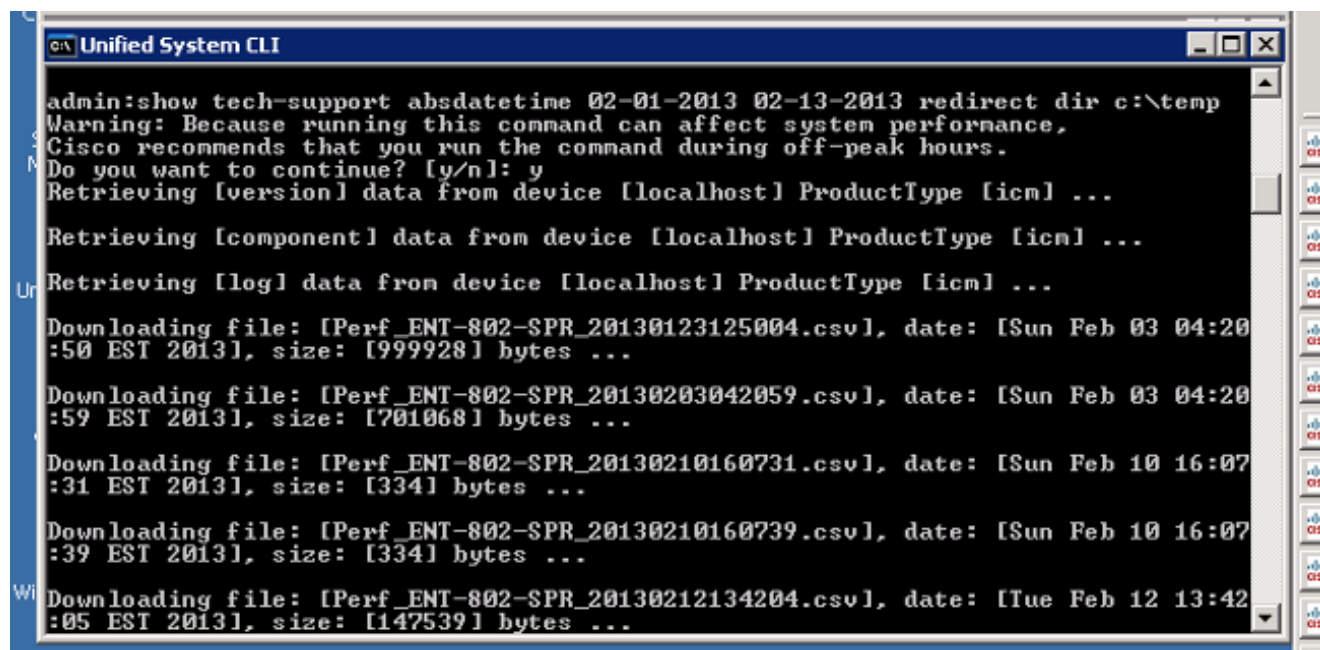
Substitua primeira string *mm-dd-aaaa:hh:mm* por uma data e hora aproximadamente 15 minutos antes do evento.

Substitua segunda string *mm-dd-aaaa:hh:mm* por uma data e hora aproximadamente 15

minutos após o evento ser resolvido.

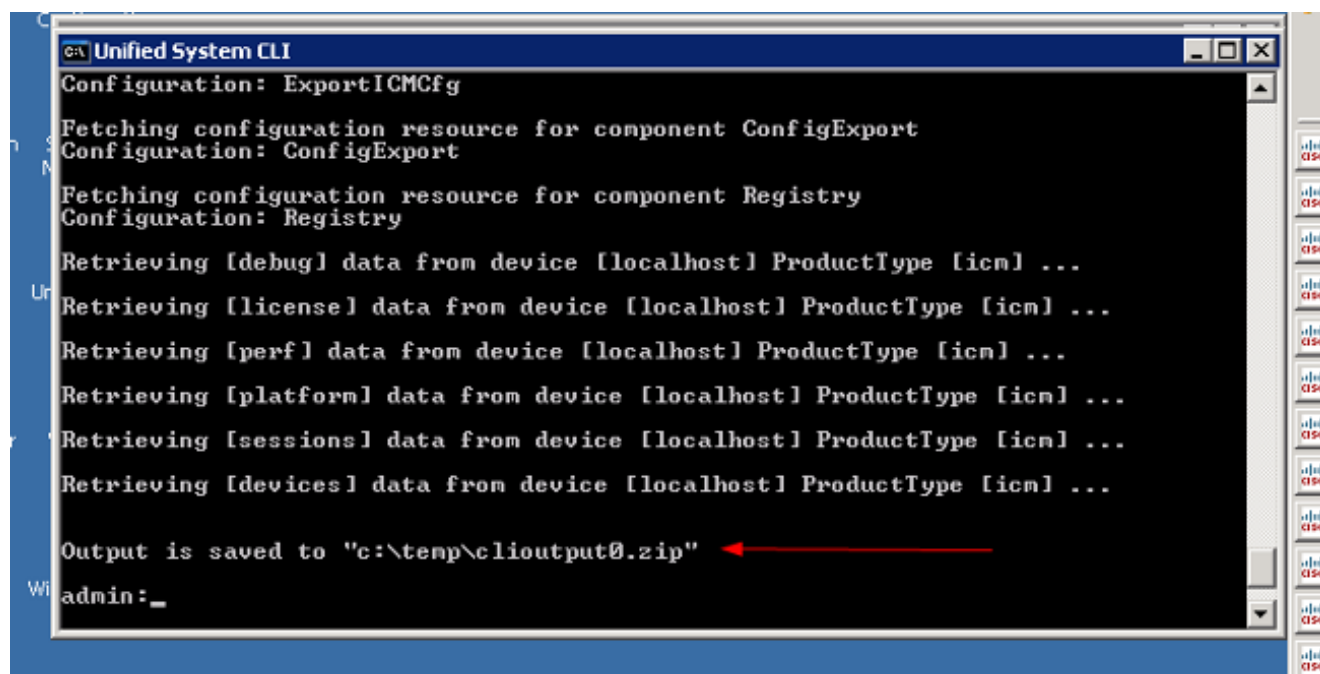
Se o evento ainda estiver ocorrendo, reúna pelo menos 15 minutos.

Isso produz um arquivo chamado *clioutputX.zip*, onde *X* é o próximo número na sequência.



```
Unified System CLI
admin:show tech-support absdatetime 02-01-2013 02-13-2013 redirect dir c:\temp
Warning: Because running this command can affect system performance,
Cisco recommends that you run the command during off-peak hours.
Do you want to continue? [y/n]: y
Retrieving [version] data from device [localhost] ProductType [icm] ...
Retrieving [component] data from device [localhost] ProductType [icm] ...
Retrieving [log] data from device [localhost] ProductType [icm] ...
Downloading file: [Perf_ENT-802-SPR_20130123125004.csv], date: [Sun Feb 03 04:20
:50 EST 2013], size: [999928] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130203042059.csv], date: [Sun Feb 03 04:20
:59 EST 2013], size: [701068] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130210160731.csv], date: [Sun Feb 10 16:07
:31 EST 2013], size: [334] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130210160739.csv], date: [Sun Feb 10 16:07
:39 EST 2013], size: [334] bytes ...
Downloading file: [Perf_ENT-802-SPR_20130212134204.csv], date: [Tue Feb 12 13:42
:05 EST 2013], size: [147539] bytes ...
```

6. Quando o processo terminar, procure o arquivo *clioutputX.zip* no diretório:



```
Unified System CLI
Configuration: ExportICMcfg
Fetching configuration resource for component ConfigExport
Configuration: ConfigExport
Fetching configuration resource for component Registry
Configuration: Registry
Retrieving [debug] data from device [localhost] ProductType [icm] ...
Retrieving [license] data from device [localhost] ProductType [icm] ...
Retrieving [perf] data from device [localhost] ProductType [icm] ...
Retrieving [platform] data from device [localhost] ProductType [icm] ...
Retrieving [sessions] data from device [localhost] ProductType [icm] ...
Retrieving [devices] data from device [localhost] ProductType [icm] ...
Output is saved to "c:\temp\clioutput0.zip"
admin: _
```

Note: Normalmente, esse arquivo é muito grande porque contém todos os arquivos relacionados ao UCCE para todos os serviços neste servidor.

7. Se precisar de apenas um registro, talvez seja mais fácil usar o utilitário *dumplog* mais antigo ou usar o *Diagnostic Framework Portico*:

Unified ICM-CCE-CCH Diagnostic Framework Portico

Hostname: ENT-802-SPR.JecodyEntLab.com Address: 14.10.150.108

Commands:

- Alarm**
 - SetAlarms
 - GetAlarms
- Configuration**
 - ListConfigurationCategories
 - GetConfigurationCategories
- Inventory**
 - ListAppServers
- License**
 - GetProductLicense
- Log**
 - ListLogComponents
 - ListLogFiles
- Network**
 - GetNetStat
 - GetPConfig
 - GetTraceRoute
 - GetPing
- Performance**
 - GetPerformanceSummary

ListTraceFiles

Component: CTI Server 1A/ctisvr

FromDate: MM/DD/YYYY 5 / 7 / 2013 HH:MM:SS 12 : 0 : 0 AM

ToDate: MM/DD/YYYY 5 / 7 / 2013 HH:MM:SS 9 : 17 : 13 AM

Show URL

Submit

Trusted sites 100%