在CCE中设置跟踪和收集日志

目录

简介

本文档介绍如何在Cisco Unified Contact Center Enterprise(CCE)中设置和收集跟踪。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科统一联系中心企业版(UCCE)
- 套装联络中心企业版(PCCE)
- 思科Finesse
- 思科客户语音门户(CVP)
- 思科虚拟化语音浏览器(VVB)

- 思科统一边界元素(CUBE)
- 思科统一情报中心(CUIC)
- 思科统一会话初始协议(SIP)代理(CUSP)

使用的组件

本文档中的信息基于以下软件版本：

- 思科Finesse版本12.5
- CVP服务器版本12.5
- UCCE/PCCE版本12.5
- 思科VVB版本12.5
- CUIC版本12.5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

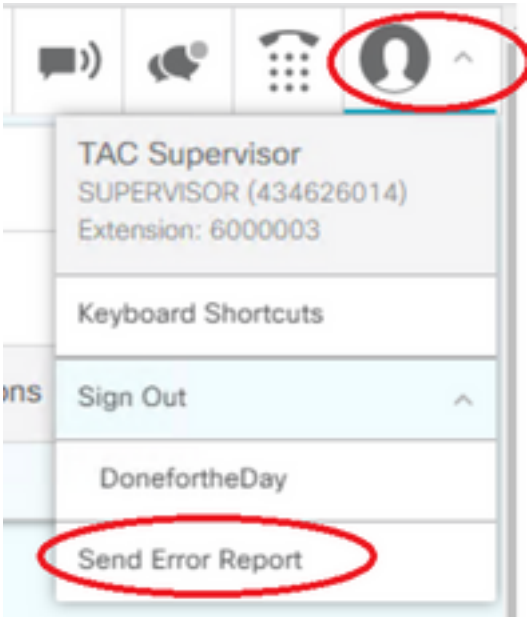
设置跟踪和收集Finesse日志

Finesse客户端

有几种选项可用于收集Finesse客户端日志。

选项 1：通过发送错误报告收集客户端日志。

1. 登录代理。
2. 如果座席在呼叫或媒体事件期间遇到任何问题，指示座席单击finesse桌面右上角的**发送错误报告**链接。

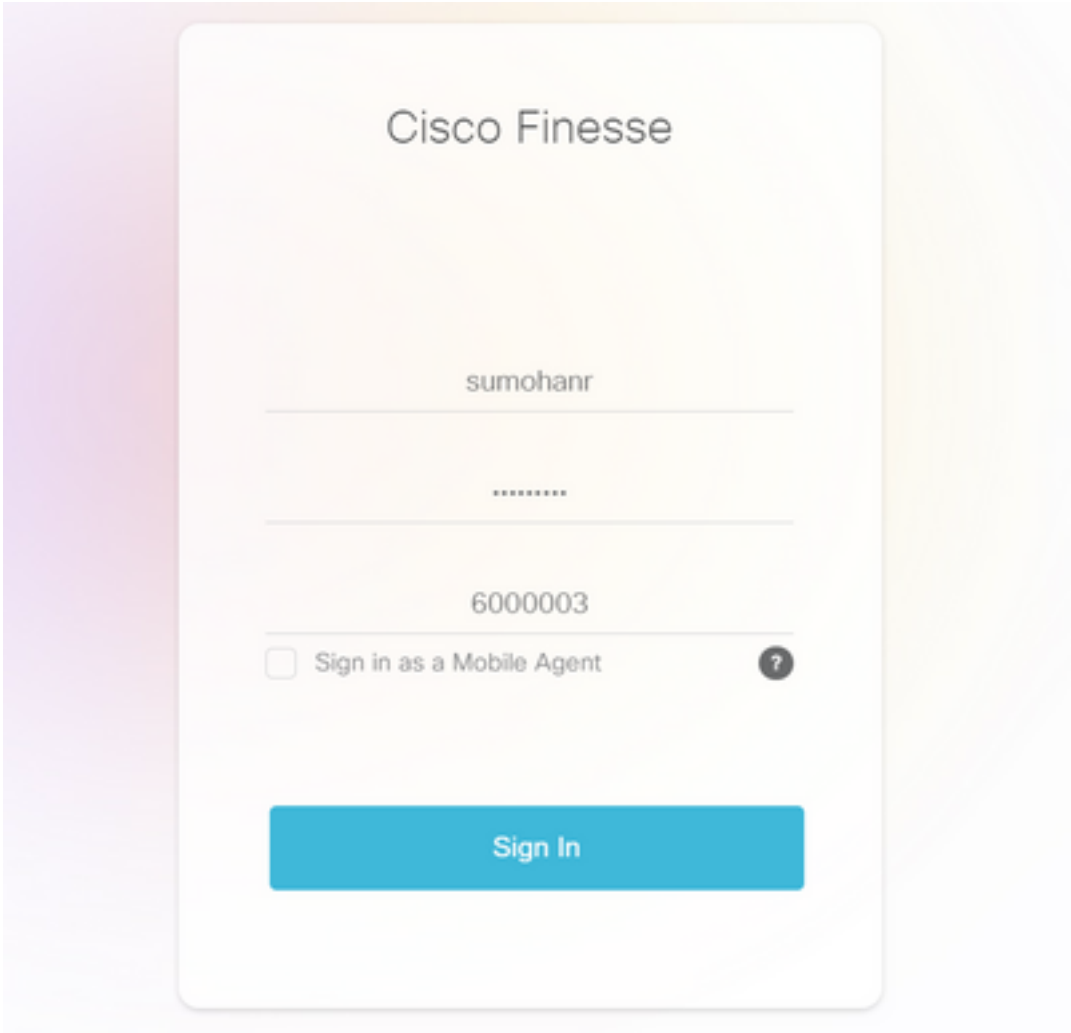


3. 代理看到**Logs Successfully Sent!**邮件.
4. 客户端日志将发送到Finesse服务器。导航到https://x.x.x.x/finesse/logs并使用管理帐户登录。
5. 收集**clientlogs/**目录下的日志。

选项 2：设置持久日志记录

1. 导航至 https://x.x.x.x:8445/desktop/locallog。
2. 单击Sign In With Persistent Logging。

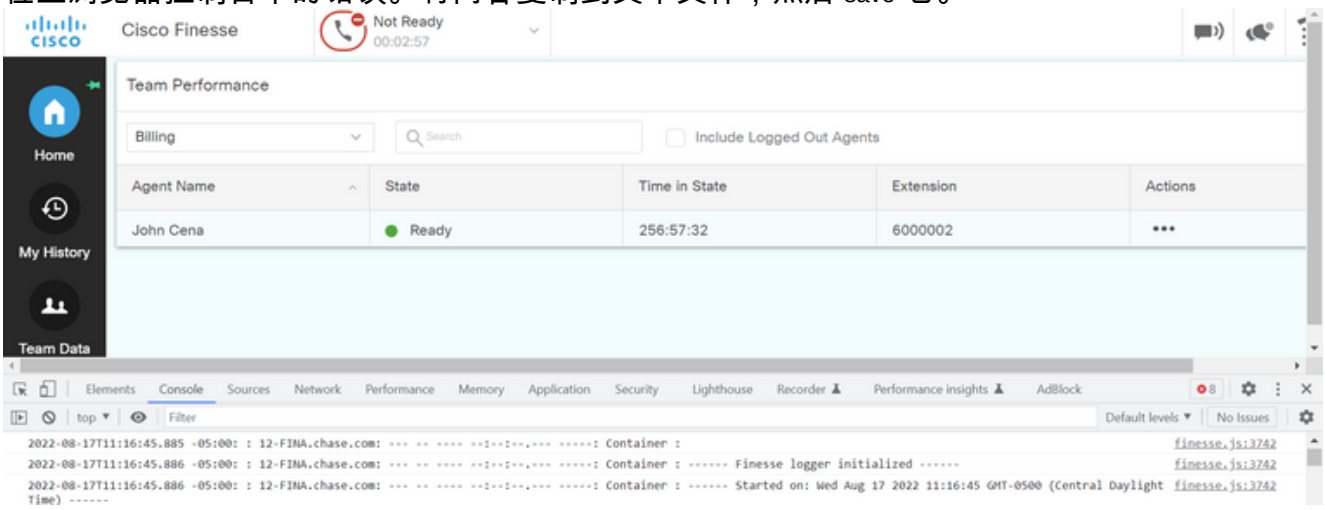
3. 系统将打开Cisco Finesse座席桌面登录页面。登录代理。



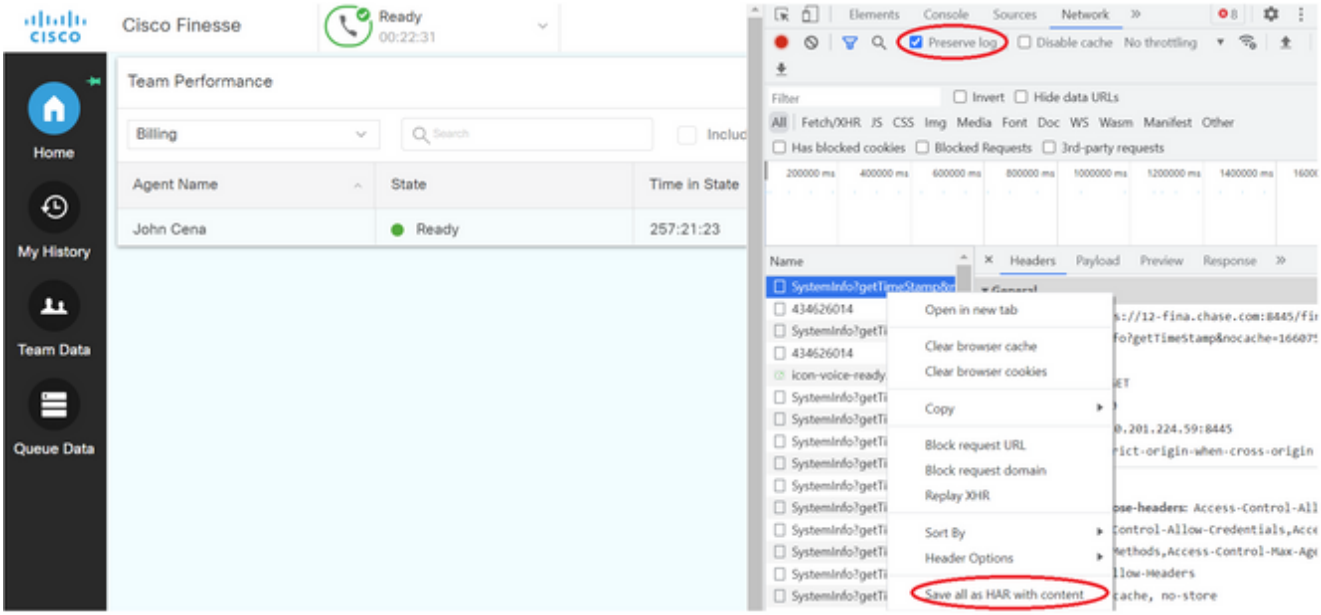
4. 所有Agent Desktop交互都将注册并发送到本地存储日志。要收集日志，请导航至 https://x.x.x.x:8445/desktop/locallog，并将内容复制到文本文件中。 Save 文件以供进一步分析。

选项 3：Web浏览器控制台

1. 代理登录后，按F12打开浏览器控制台。
2. 选择Console选项卡。
3. 检查浏览器控制台中的错误。将内容复制到文本文件，然后 save 它。



4. 选择Network选项卡，并选中Preserve log选项。
5. 右键单击任何网络名称事件并选择 Save 在内容方面如类比。



Finesse服务器

选项 1：通过用户界面(UI)- Web服务（必需）和其他日志

1. 导航到https://x.x.x.x/finesse/logs并使用管理帐户登录。
2. 展开目录webservices/

3. 收集上一个Web服务日志。选择最后一个解压缩文件。例如Desktop-Webservices.201X-..log.zip。点击文件链接，您会看到以下选项 save 文件。

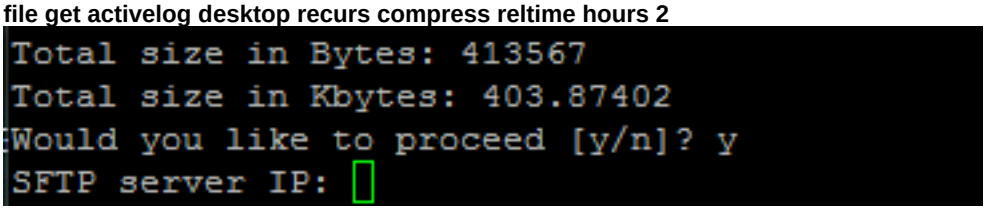
4. 收集其他所需的日志（取决于场景）。 例如，用于通知服务问题的openfire、用于身份验证问题的领域日志以及用于API问题的tomcatlogs。

   注意：建议通过安全外壳(SSH)和安全文件传输协议(SFTP)收集Cisco Finesse服务器日志。此方法不仅允许您收集Web服务日志，还允许您收集其他所有日志，如Fippa、openfire、领域和Clientlogs。

选项 2：通过SSH和安全文件传输协议(SFTP) — 推荐选项

1. 使用SSH登录Finesse服务器。
2. 输入此命令以收集所需的日志。该命令将收集2小时的日志。系统将提示您标识日志上传到的SFTP服务器。

   file get activelog desktop recurs compress reltime hours 2

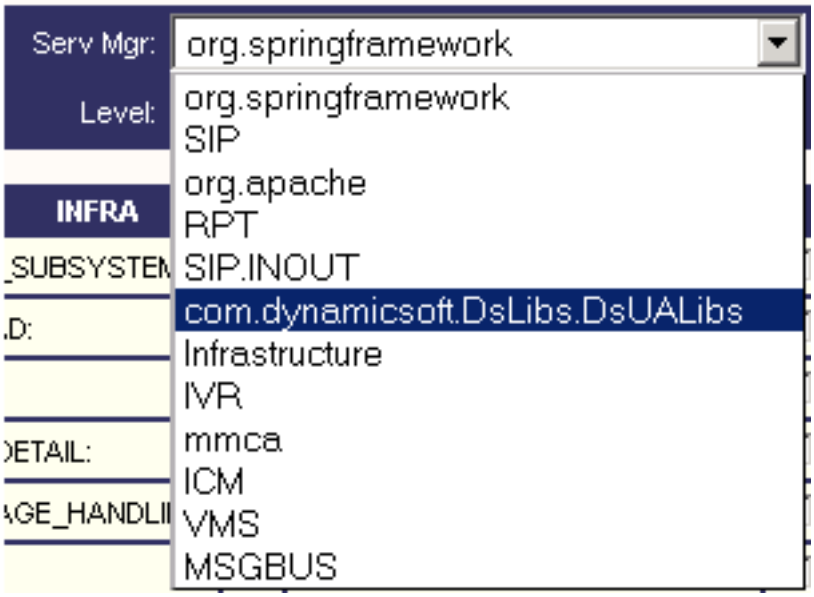


3. 这些日志存储在SFTP服务器路径上：<IP地址>\<日期时间戳>\active_nnn.tgz ，其中nnn是长格式的时间戳。
4. 要收集其他日志，如tomcat、情景服务、服务和安装日志，请查看Cisco Finesse管理指南12.5(1)版的“日志收集”部分。

设置跟踪并收集CVP和CVVB日志

CVP呼叫服务器

1. CVP CallServer默认跟踪级别足以对大多数情况进行故障排除。但是，如果您需要获得有关会话发起协议(SIP)消息的更多详细信息，则需要将SIP字符串跟踪设置为DEBUG级别。
2. 导航至CVP CallServer Diag网页URL http:/localhost:8000/cvp/diag。
   注意：此页提供有关CVP CallServer的良好信息，对特定场景进行故障排除非常有用。
3. 从服务器中选择**com.dynamicsoft.DsLibs.DsUALibs**。**左**上角的Mgr下拉菜单

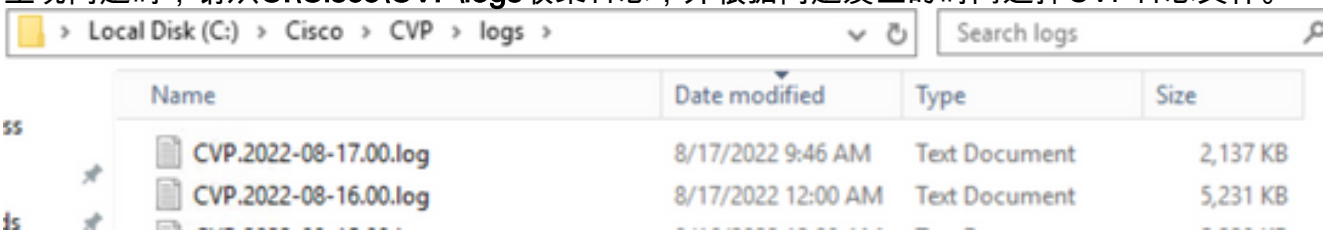


4. 单击Set按钮。

5. 在跟踪窗口中向下滚动，以确保已正确设置跟踪级别。这些是您的调试设置。

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

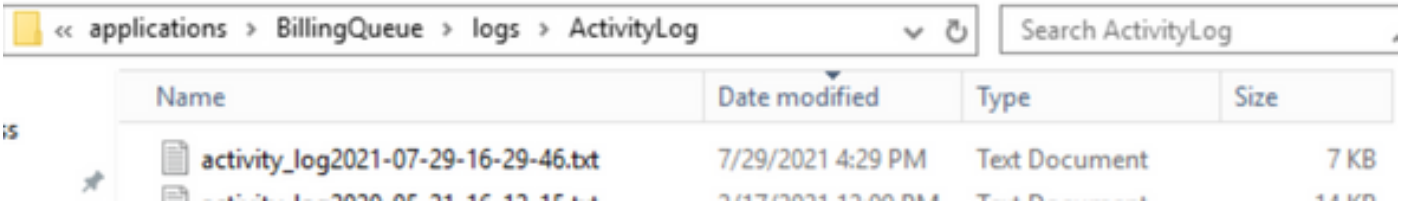
6. 重现问题时，请从C:\Cisco\CVP\logs收集日志，并根据问题发生的时间选择CVP日志文件。



CVP语音XML(VXML)应用

在极少数情况下，您需要增加VXML服务器应用程序的跟踪级别。另一方面，除非思科工程师提出请求，否则不建议增加此数量。

要收集VXML服务器应用程序日志，请导航到VXML服务器下的特定应用程序目录，例如：C:\Cisco\CVP\VXMLServer\applications\{应用程序名称}\logs\ActivityLog\并收集活动日志。



CVP运营和管理管理门户(OAMP)

在大多数情况下，OAMP和ORM的默认跟踪级别足以确定问题的根本原因。但是，如果需要增加跟踪级别，请按照以下步骤执行此操作：

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

2. 编辑 **%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. 修改后，重新启动OPSConsoleServer，如下所示。

跟踪级别信息

跟踪级别	描述	日志级别	跟踪掩码
0	产品安装默认值。预期不会对性能造成影响或影响很小。	信息	无
1	更详细的跟踪消息，对性能的影响较小。	调试	DEVICE_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x0101100
2	详细的跟踪消息对性能的影响不大。	调试	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x0501100
3	对性能有影响的详细跟踪消息。	调试	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + DATABASE_MODIFY + MANAGEMENT=0x0511100
4	详细的跟踪消息，对性能有非常大的影响。	调试	杂项+ DEVICE_CONFIGURATION + ST_CONFIGURATION +

			SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACK TRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + 管理+ TRACE_METHOD + TRACE_PARAM=0x173710 00
5	最高详细跟踪消息。	调试	杂项+ DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACK TRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + 管理+ TRACE_METHOD + TRACE_PARAM=0x173710 06

思科虚拟化语音浏览器(CVVB)

在CVVB中，跟踪文件是记录来自Cisco VVB组件子系统和步骤的活动的日志文件。

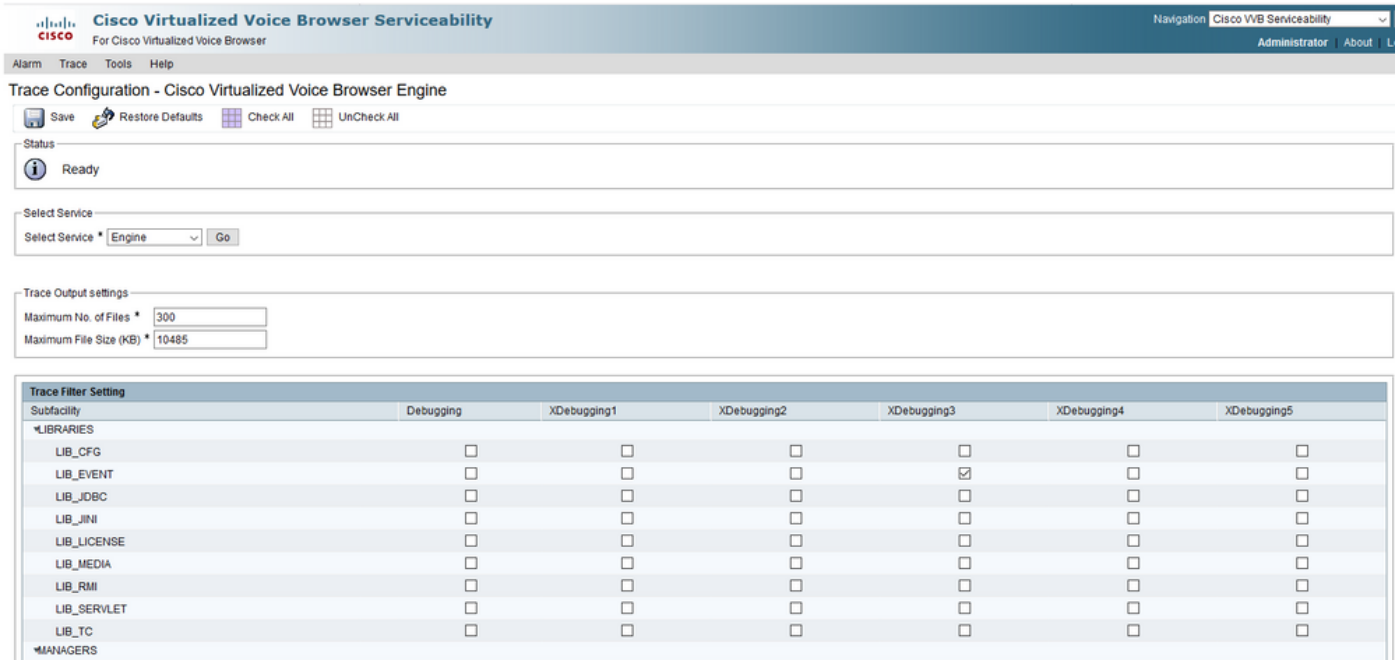
Cisco VVB有两个主要组件：

- Cisco VVB“管理”跟踪称为MADM日志
- 称为MIVR日志的Cisco VVB“引擎”跟踪

您可以指定要为其收集信息的组件以及要收集的信息级别。

日志级别扩展自：

- 调试 — 基本流详细信息到
- XDebugging 5 — 堆栈跟踪的详细级别



警告：不能在生产加载的系统上启用Xdebugging5。

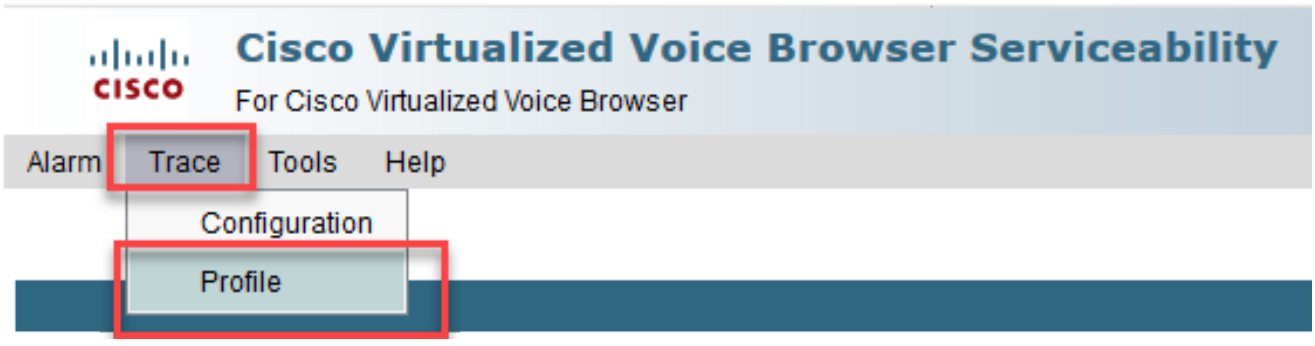
您需要收集的最常见日志是引擎。CVVB引擎跟踪的默认跟踪级别足以解决大多数问题。但是，如果您需要更改特定方案的跟踪级别，Cisco建议您使用预定义系统日志配置文件。

系统日志配置文件

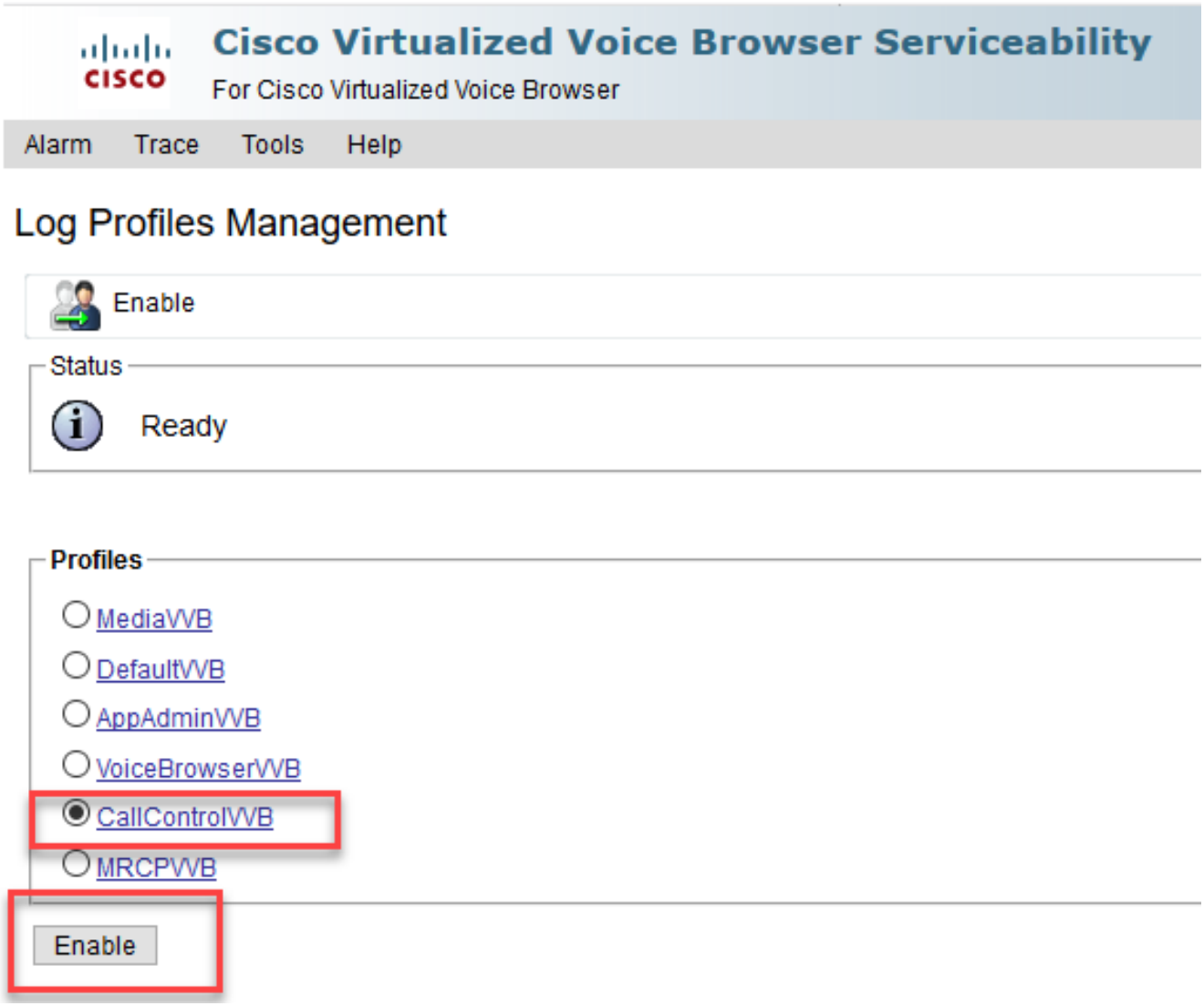
名称	必须激活此配置文件的方案
默认VVB	已启用通用日志。
AppAdminVVB	有关通过AppAdmin、Cisco VVB Serviceability和其他网页进行Web管理题。
MediaVVB	有关介质设置或介质传输的问题。
语音浏览器VVB	有关呼叫处理的问题。
MRCPVVB	有关ASR/TTS与Cisco VVB交互的问题。
CallControlVVB	有关SIP信号的问题，将在日志中发布。

1. 打开CVVB主页(https://X.X.X/uccxservice/main.htm)，然后导航到Cisco VVB Serviceability页面。使用管理帐户登录

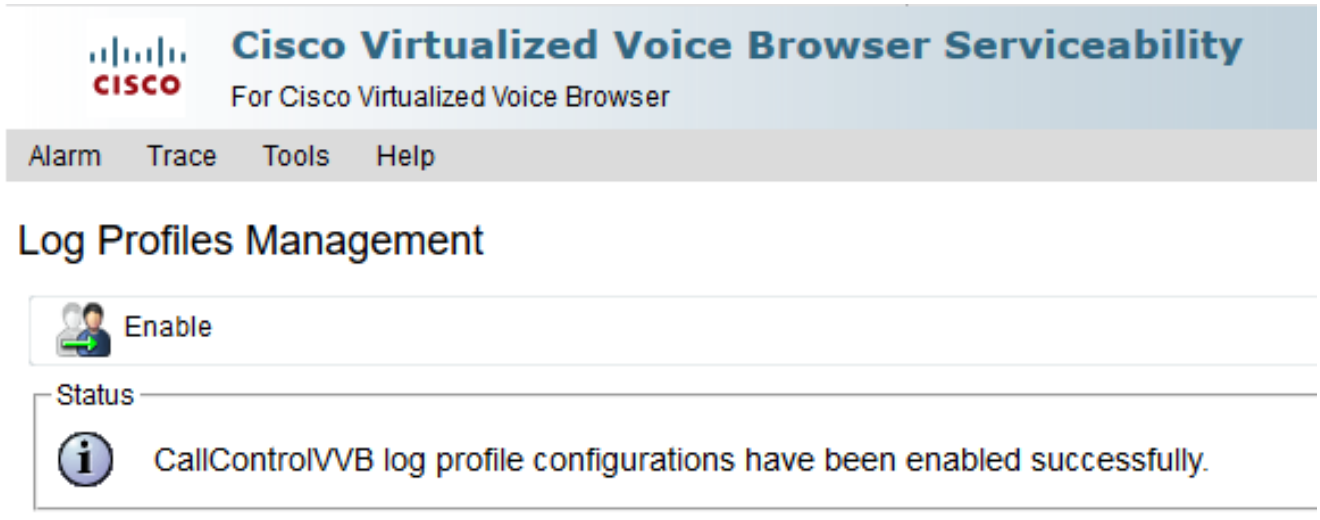
2. 选择 **Trace -> Profile。**



3. 选中要为特定方案启用的配置文件，然后单击**Enable**按钮。例如，启用SIP相关问题的配置文件CallControlVVB，或启用MRCPVVB，以解决与自动语音识别和文本到语音转换(ASR/TTS)交互相关的问题。

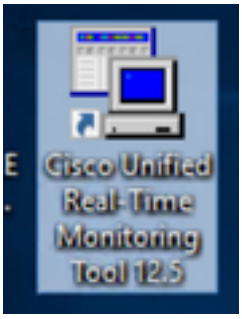


4. 单击enable按钮后，您会看到成功消息。

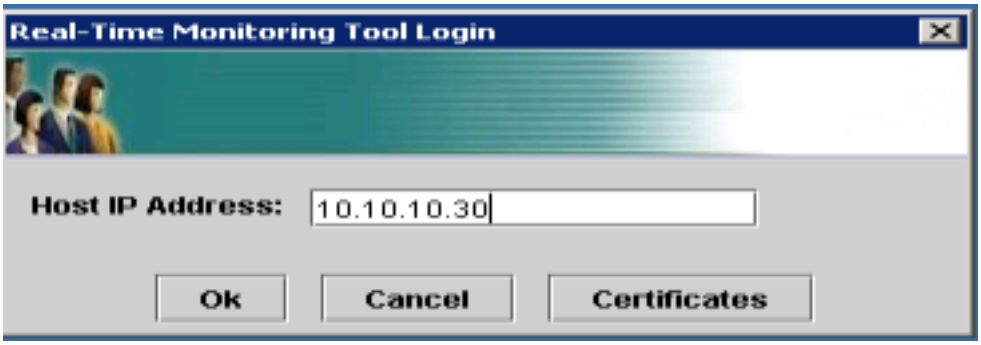


5. 重现问题后，收集日志。使用CVVB附带的实时监控工具(RTMT)收集日志。

6. 点击桌面上的Cisco Unified Real-Time Monitoring Tool图标（如果需要，请从CVVB下载此工具）。

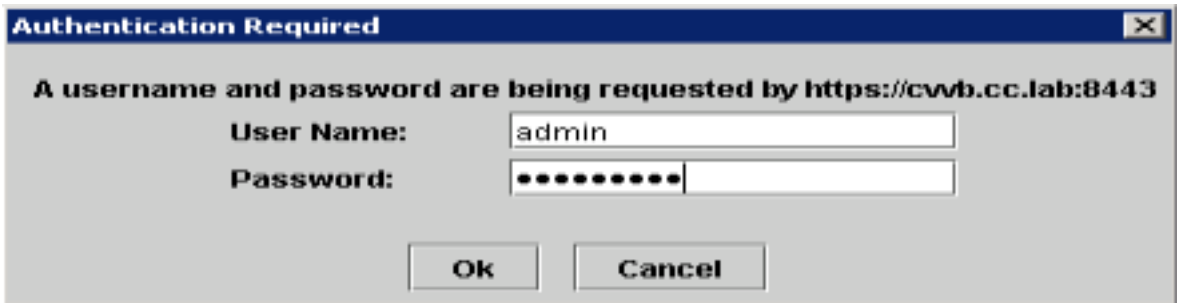


7. 提供VVB的IP地址，然后单击**OK**。



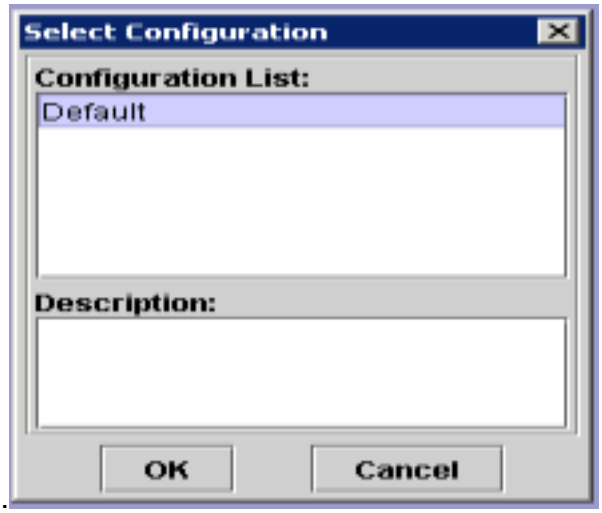
8. 接受证书信息（如果显示）

9. 提供凭证并单击**OK**。

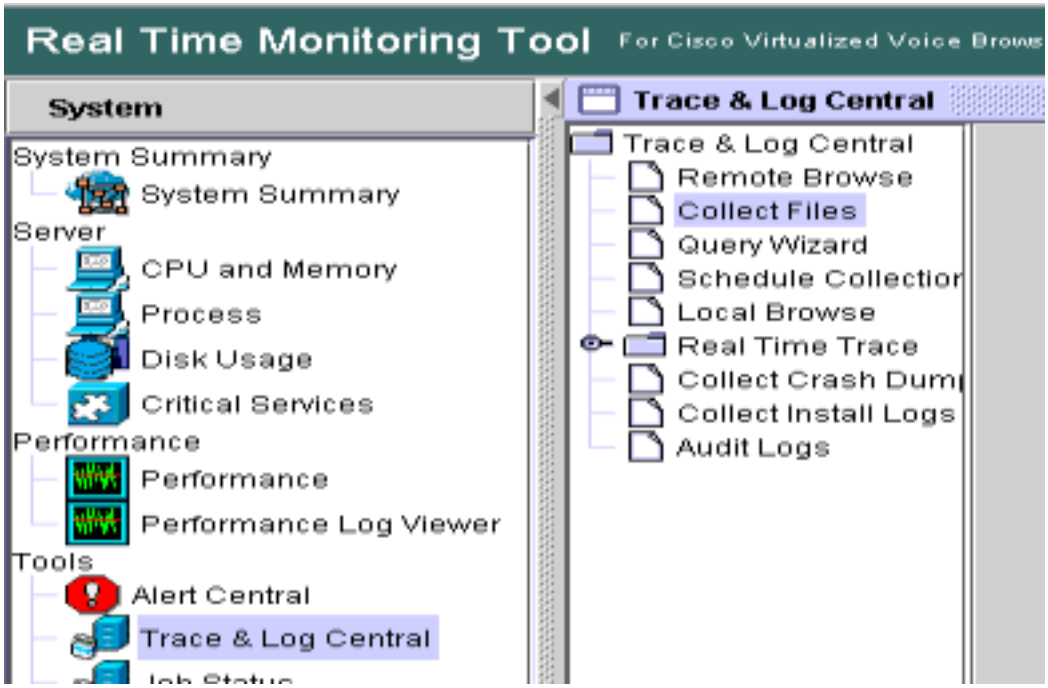


10. 如果收到TimeZone错误，单击**Yes**按钮后，RTMT可以关闭。请重新启动RTMT工具。

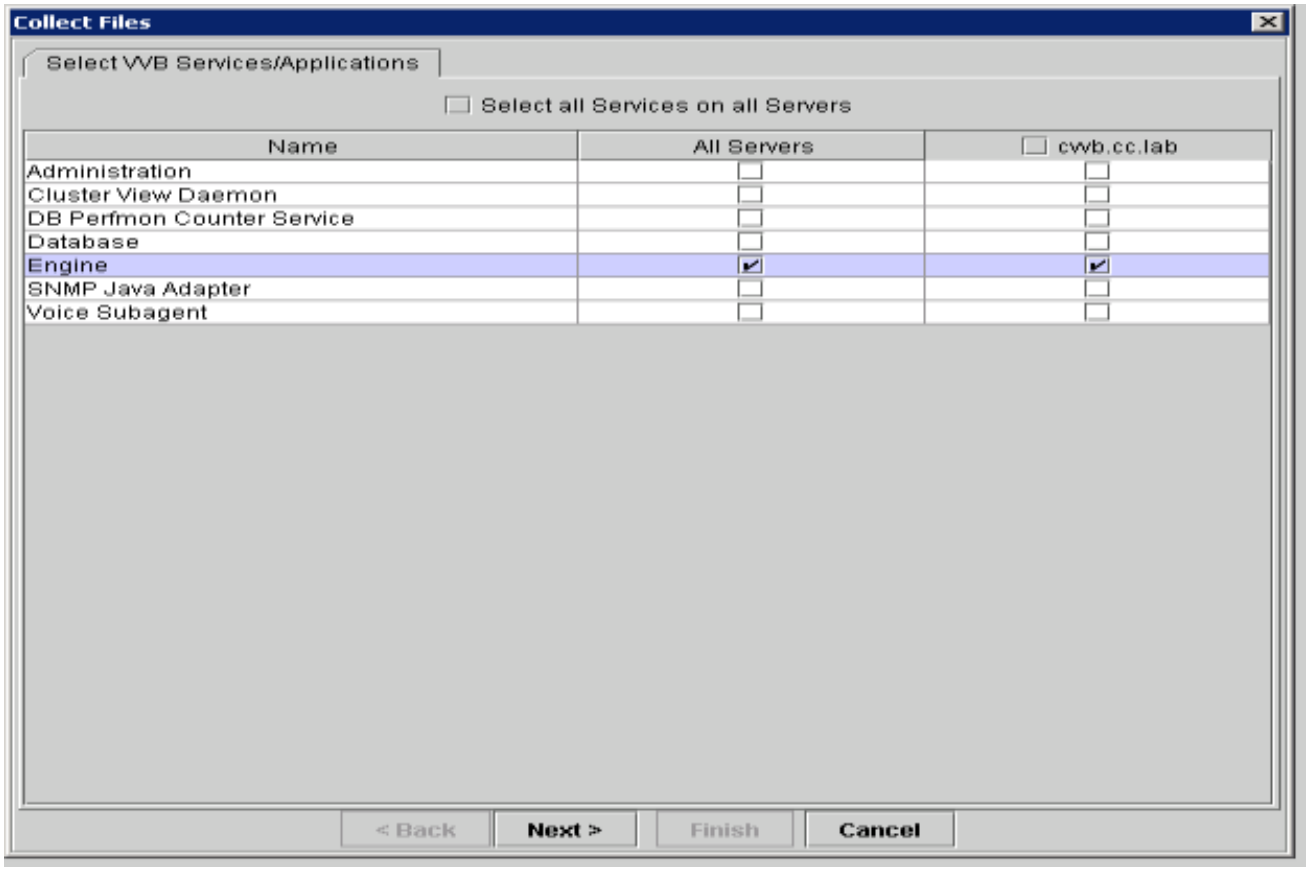
11. 保持选中Default配置，然后单击**OK**。



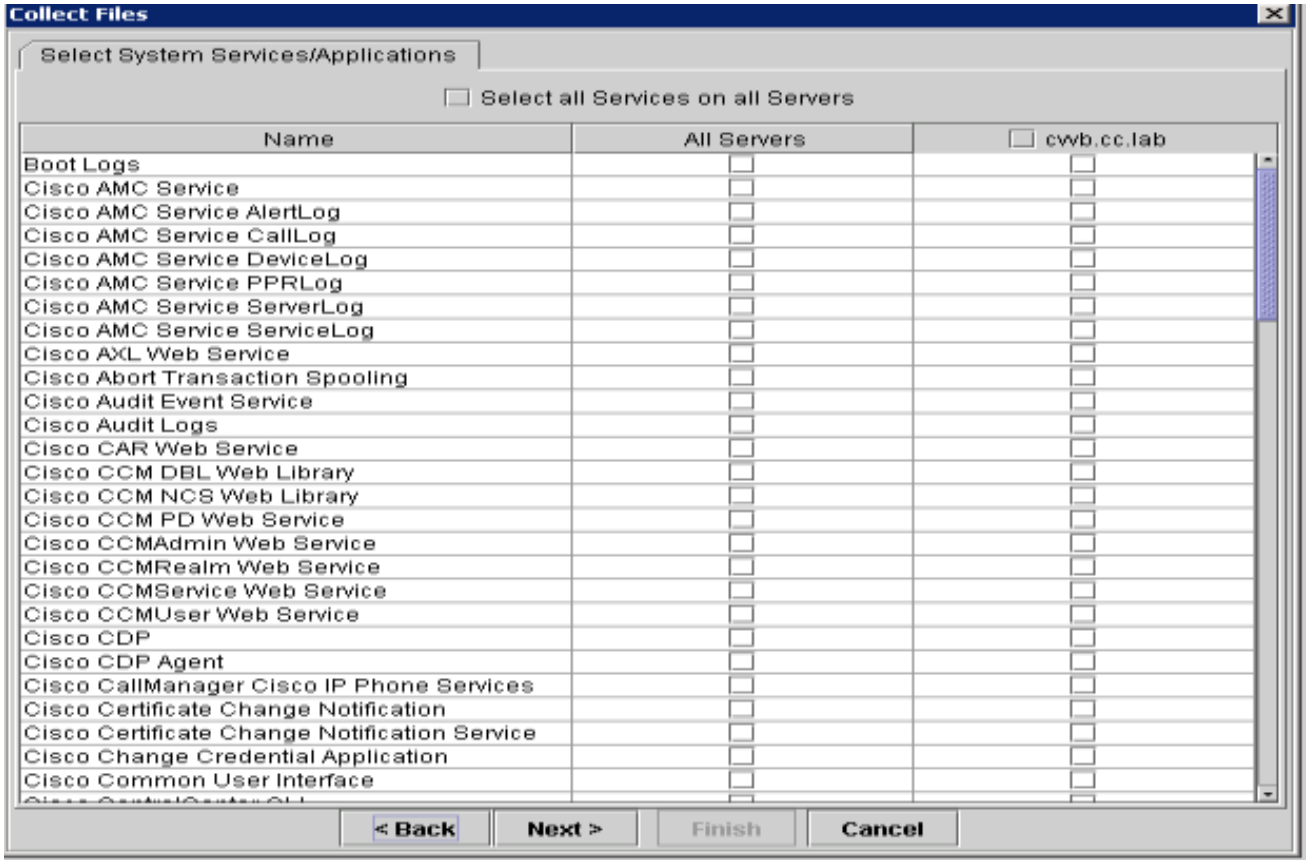
12. 选择**Trace & Log Central**，然后双击**Collect Files**。



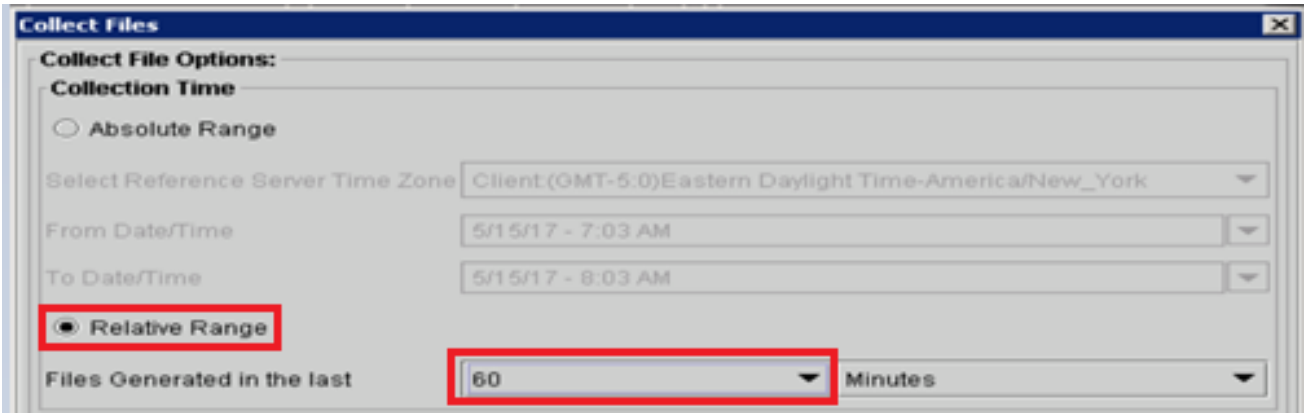
13. 在新打开的窗口中，选择**Engine**并单击“下一步”。



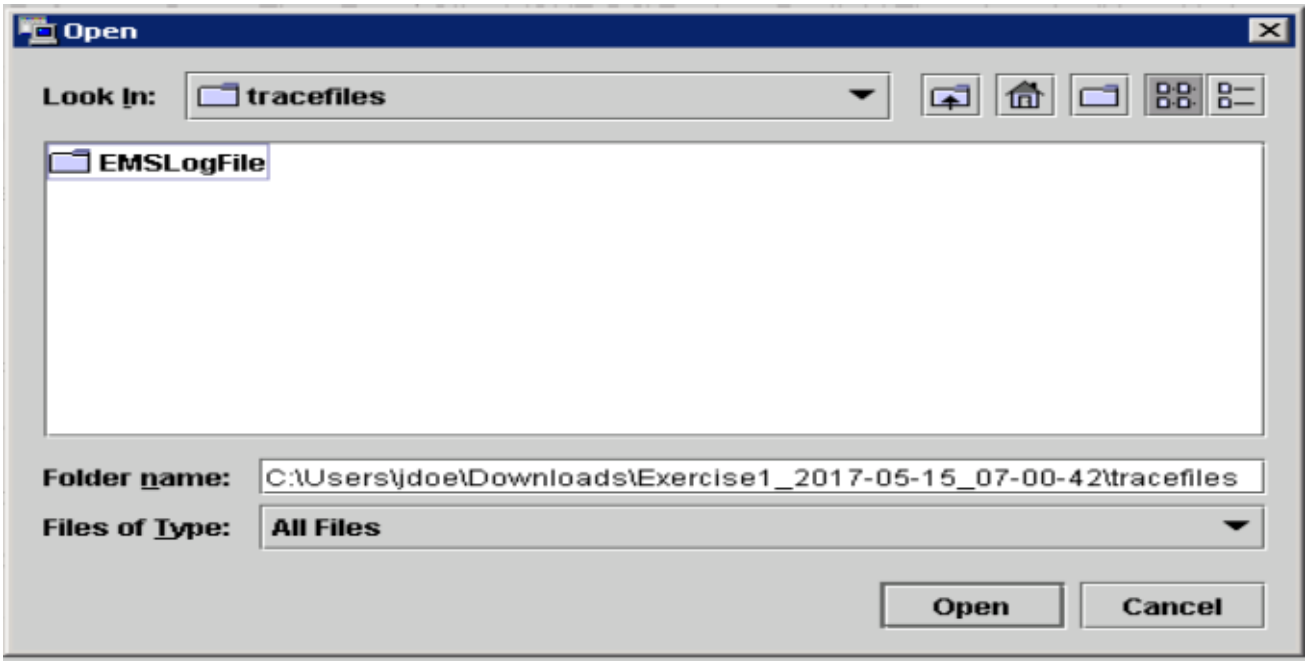
14. 在下一个窗口中再次单击**Next**。



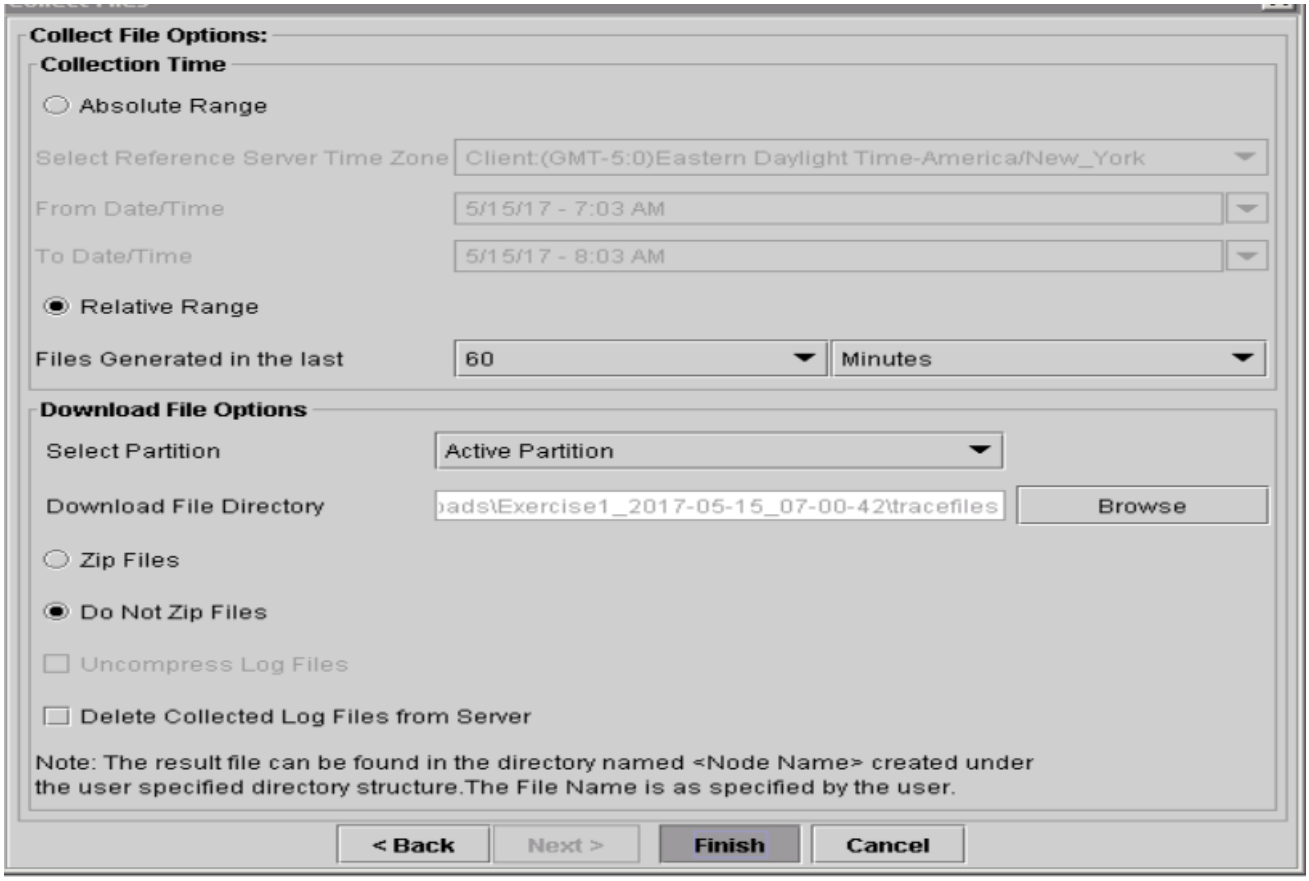
15. 选择**Relative Range**，确保您选择时间以覆盖错误呼叫的时间。



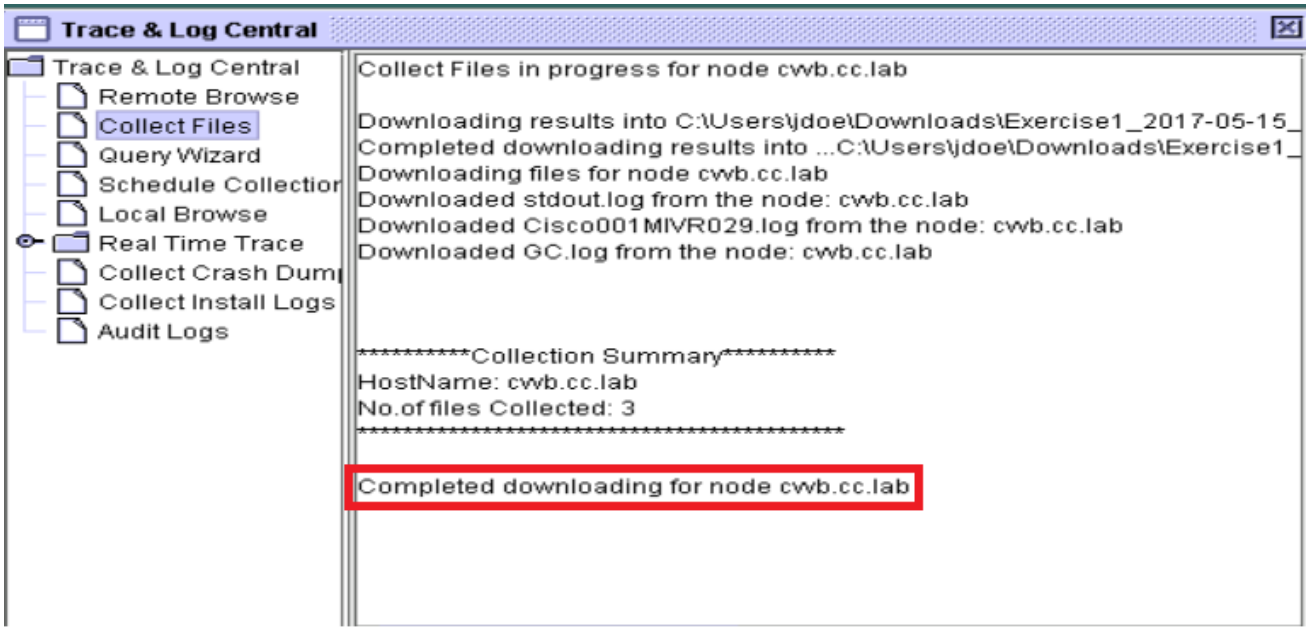
16. 在Download File Options上，单击**Browse**并选择要下载的目录 save 文件，然后单击**打开**。



17. 选择所有选项后，单击**Finish**按钮。



18. 这将收集日志文件。请等待，直到您看到RTMT上的确认消息。

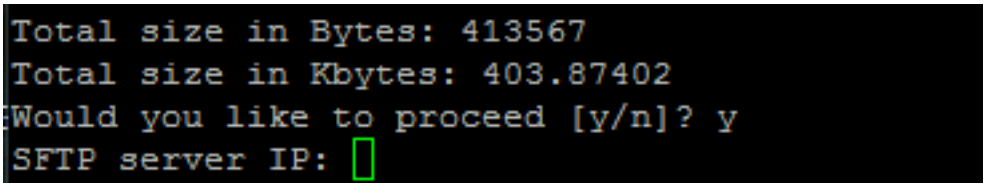


19. 导航到保存跟踪的文件夹。

20. 引擎日志满足您的需求。要找到它们，请导**航到\<time stamp>\uccx\log\MIVR文**件夹。

选项 2：通过SSH和SFTP — 推荐选项

1. 使用安全外壳(SSH)登录VVB服务器。
2. 输入此命令以收集所需的日志。系统会压缩日志，并提示您确定日志上传到的SFTP服务器。
   file get activelog /uccx/log/MIVR/*



3. 这些日志存储在SFTP服务器路径上：*<IP地址>\<日期时间戳>\active_nnn.tgz* ，其中nnn是长格式的时间戳。

为CUBE和CUSP设置跟踪和收集日志

CUBE(SIP)

1. 设置日志时间戳并启用日志记录缓冲区。

```
#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
```

警告：生产Cisco IOS®软件GW上的任何更改都可能导致中断。

2. 这是一个非常强大的平台，可以在提供的呼叫量处理建议的调试，而不会出现问题。但是，思科建议您： 将所有日志发送到系统日志服务器而不是日志记录缓冲区。

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

逐个应用debug命令，并在每条命令之后检查CPU利用率。

```
show proc cpu hist
```

警告： 如果CPU利用率达到70-80%，性能相关服务影响的风险将大大增加。因此，如果GW达到60%，请勿启用其他调试。

3. 启用以下调试：

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

4. 重现问题。
5. 禁用跟踪。

```
#undebug all
```

6. 收集日志。

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

CUSP

1. 在CUSP上启用SIP跟踪。

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

2. 重现问题。
3. 完成后，关闭日志记录。

收集日志

1. 在CUSP上配置用户(例如：测试)。
2. 在CUSP提示符处添加此配置。

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

3. FTP到CUSP IP地址。使用上一步中定义的用户名（测试）和密码。
4. 将目录更改为/cusp/log/trace。
5. 获取log_<filename>。

设置跟踪和收集UCCE日志

思科建议通过Diagnostis Framework Portico或系统CLI工具设置跟踪级别并收集跟踪。

> **注意：** 有关诊断框架门户和系统CLI的详细信息，请访问Cisco Unified ICM/Contact Center Enterprise版本12.5(1)的诊断工具一章。

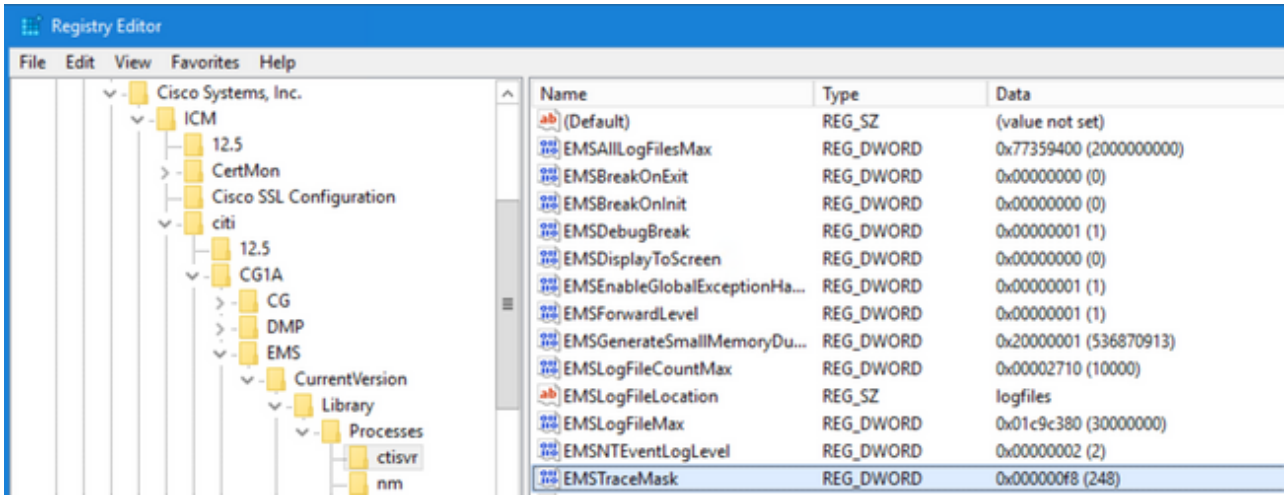
排除大部分UCCE场景故障时，如果跟踪的默认级别没有提供足够的信息，请在所需组件中将跟踪级别设置为3（某些除外）。

> **注意：有关详细信息，请访问Cisco Unified ICM/Contact Center Enterprise版本12.5(1)的适用性指南上的**跟踪级别部分。

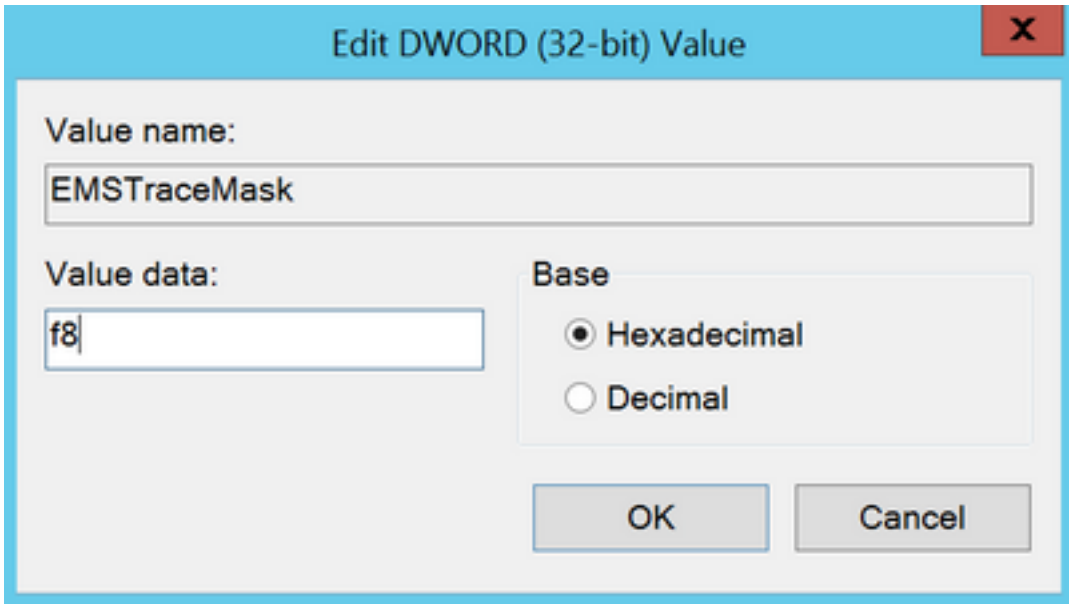
例如，如果您排除出站拨号程序问题，如果拨号程序繁忙，则跟踪级别必须设置为级别2。

对于CTISVR(CTISVR),2级和3级未设置思科建议的确切注册表级别。CTISVR的推荐跟踪注册表为0XF8。

1. 在UCCE代理PG上，打开注册表编辑器(Regedit)。
2. 导航至HKLM\software\Cisco Systems， Inc\icm\<cust_inst>\CG1(a and b)\EMS\CurrentVersion\library\Processes\ctisvr。



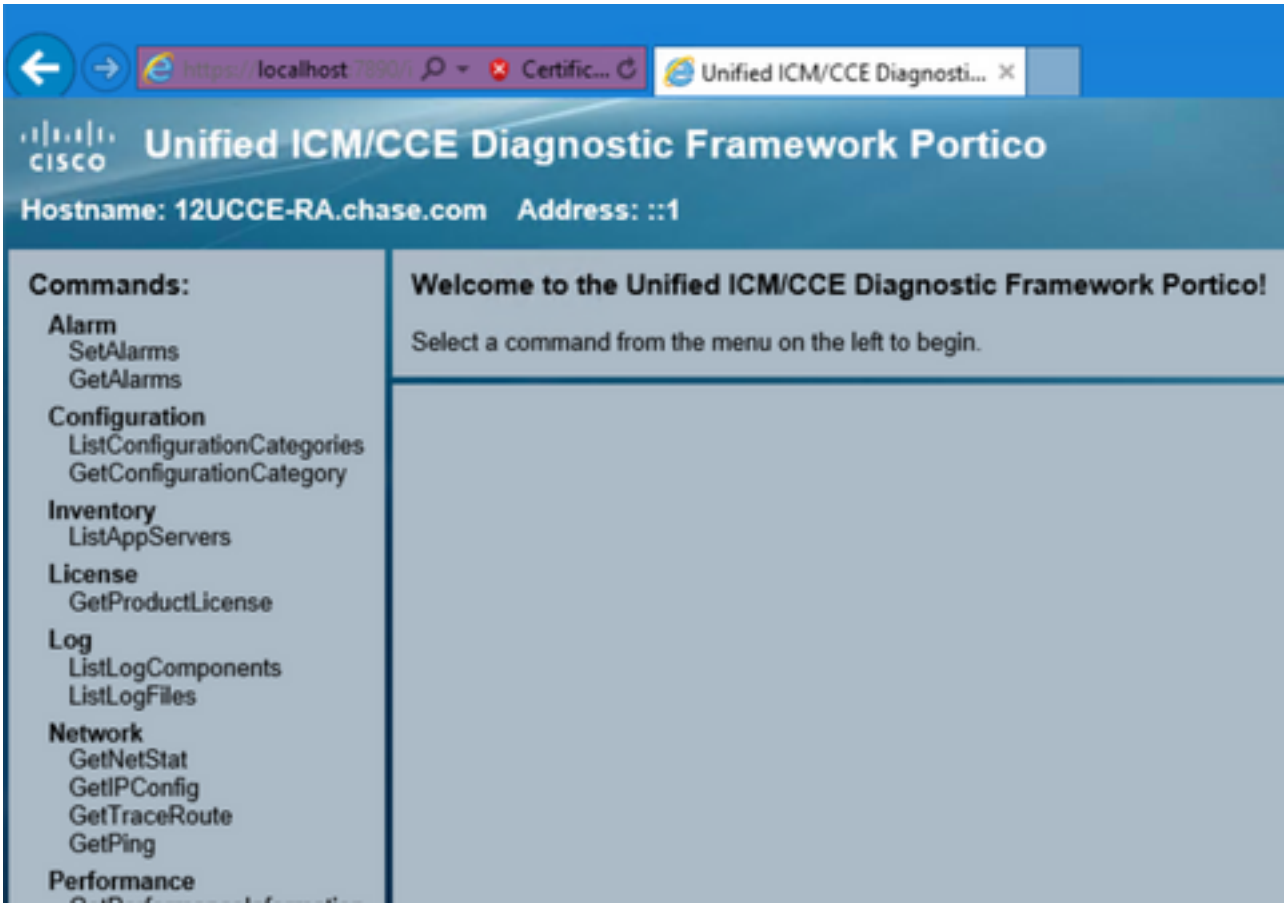
3. 双击**EMSTraceMask**并将值设置为**f8**。



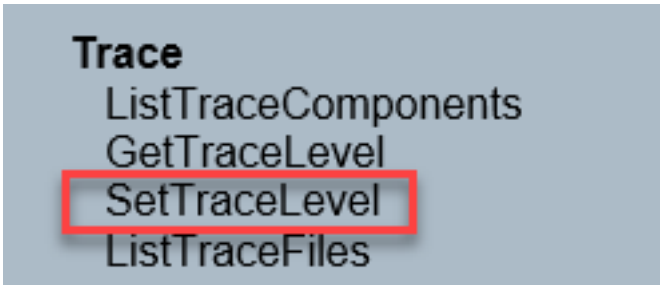
4. 单击**Ok**并关闭注册表编辑器。以下是设置任何UCCE组件跟踪的步骤（以RTR过程为例）。

SetTrace级别

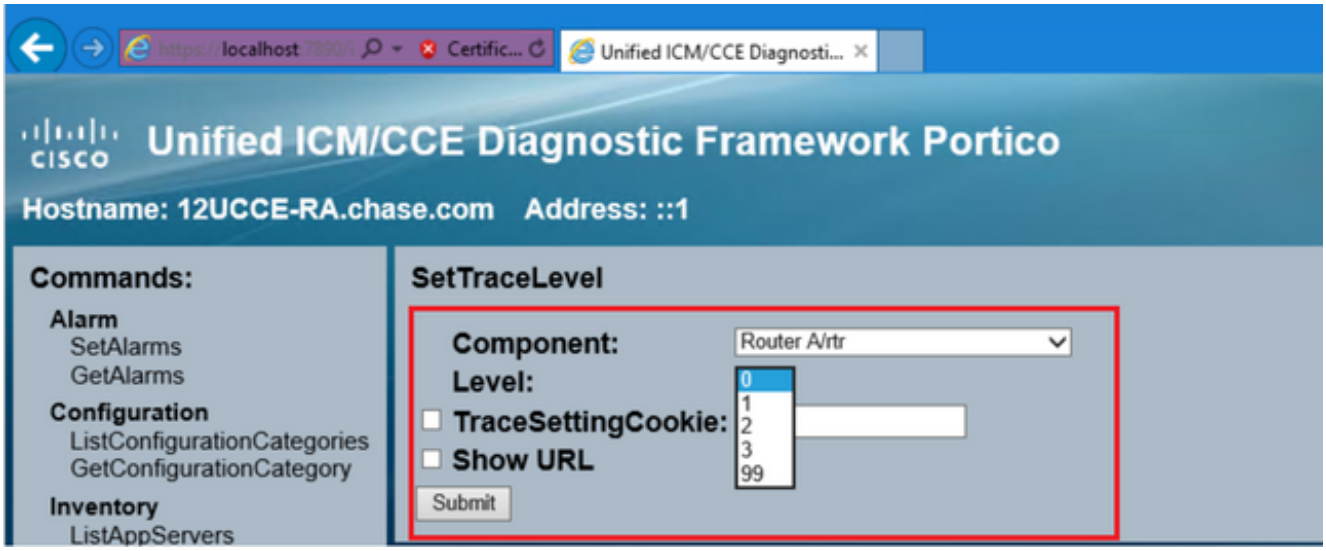
1. 从需要设置跟踪的服务器打开Diagnostic Framework Portico，并以管理员用户身份登录



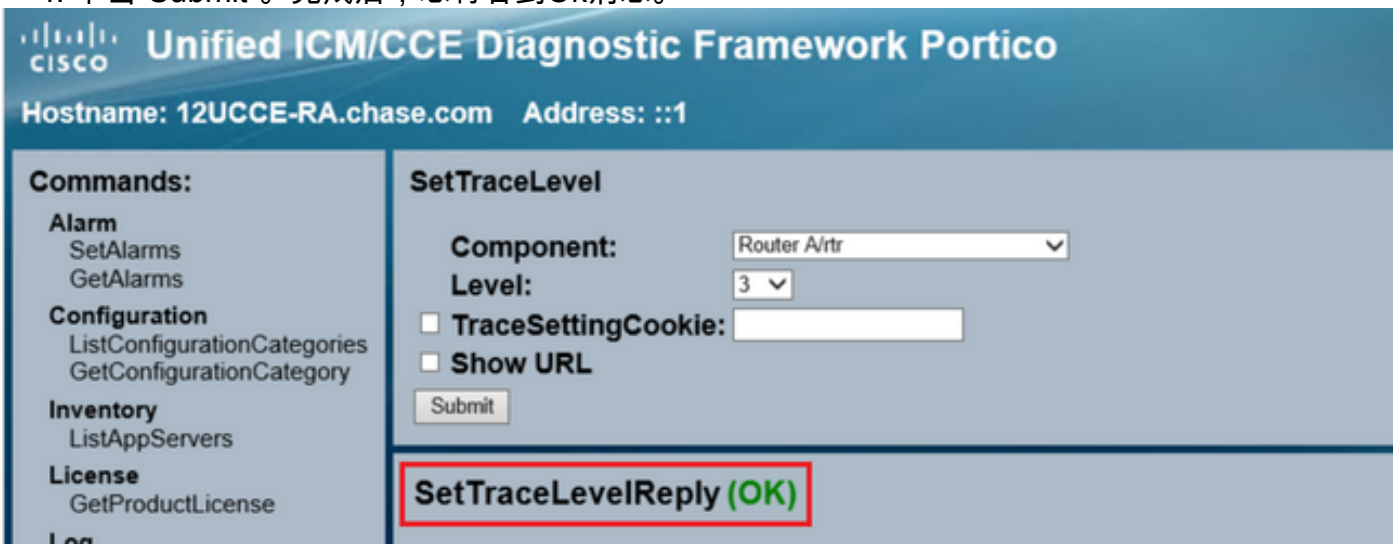
2. 在Commands部分中，导航到**Trace**并选择 **SetTraceLevel**。



3. 在**SetTraceLevel**窗口中，选择组件和级别。



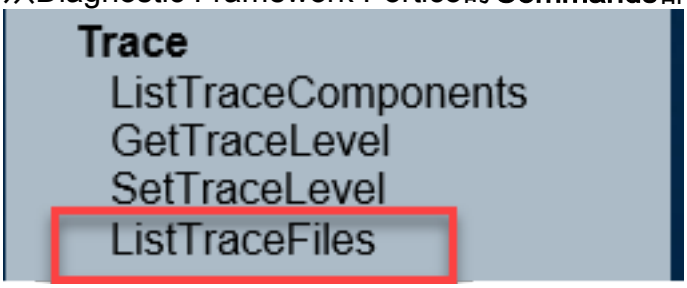
4. 单击“Submit”。完成后，您将看到Ok消息。



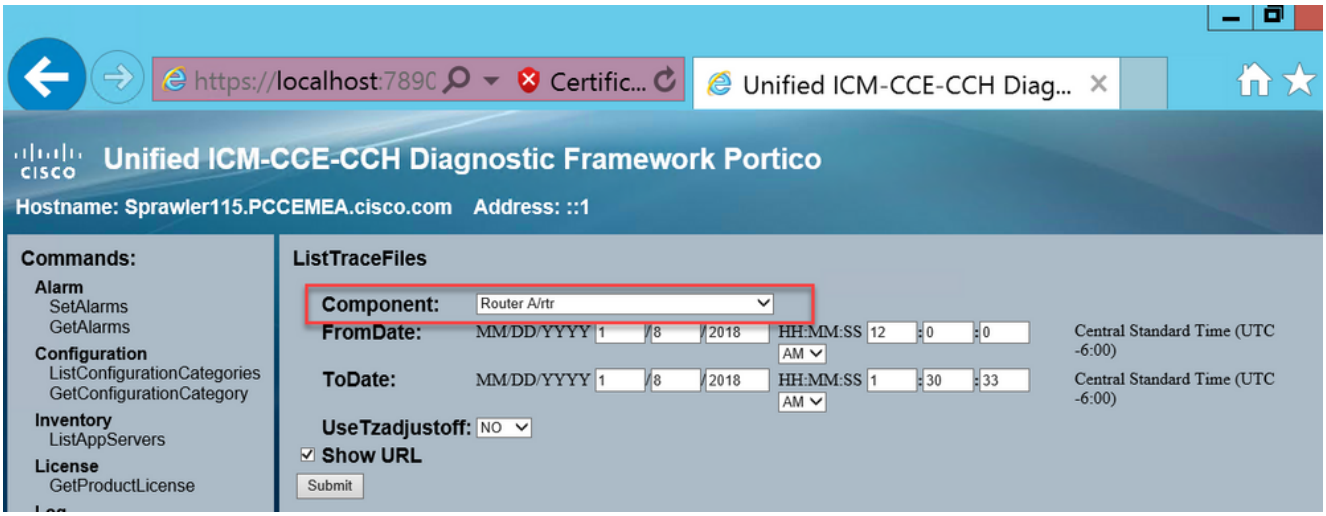
警告：尝试重现问题时将跟踪级别设置为级别3。重现问题后，将跟踪级别设置为默认值。在设置JTAPIGW跟踪时，请特别小心，因为级别2和级别3设置了低级别跟踪，这可能会影响性能。在JTAPIGW的非生产时间或实验室环境中设置2级或3级。

日志收集

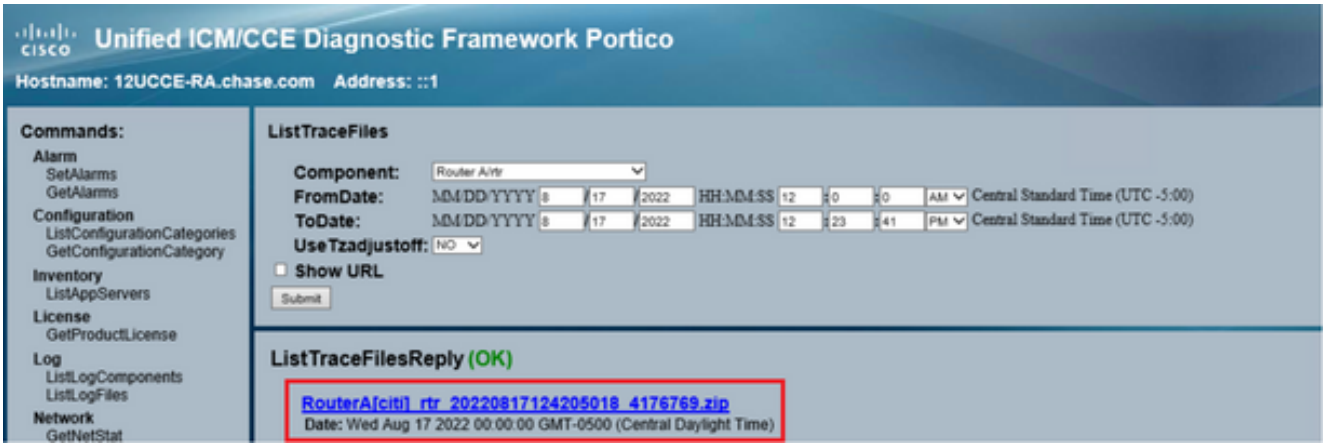
1. 从Diagnostic Framework Portico的**Commands**部分导航到**Trace**，然后选择**ListTraceFile**。



2. 在ListTraceFile窗口中，选择**Component**、**FromDate**和**ToDate**。选中**Show URL**框，然后单击**Submit**。



3. 请求完成后，您会看到OK消息和ZIP日志文件的链接。

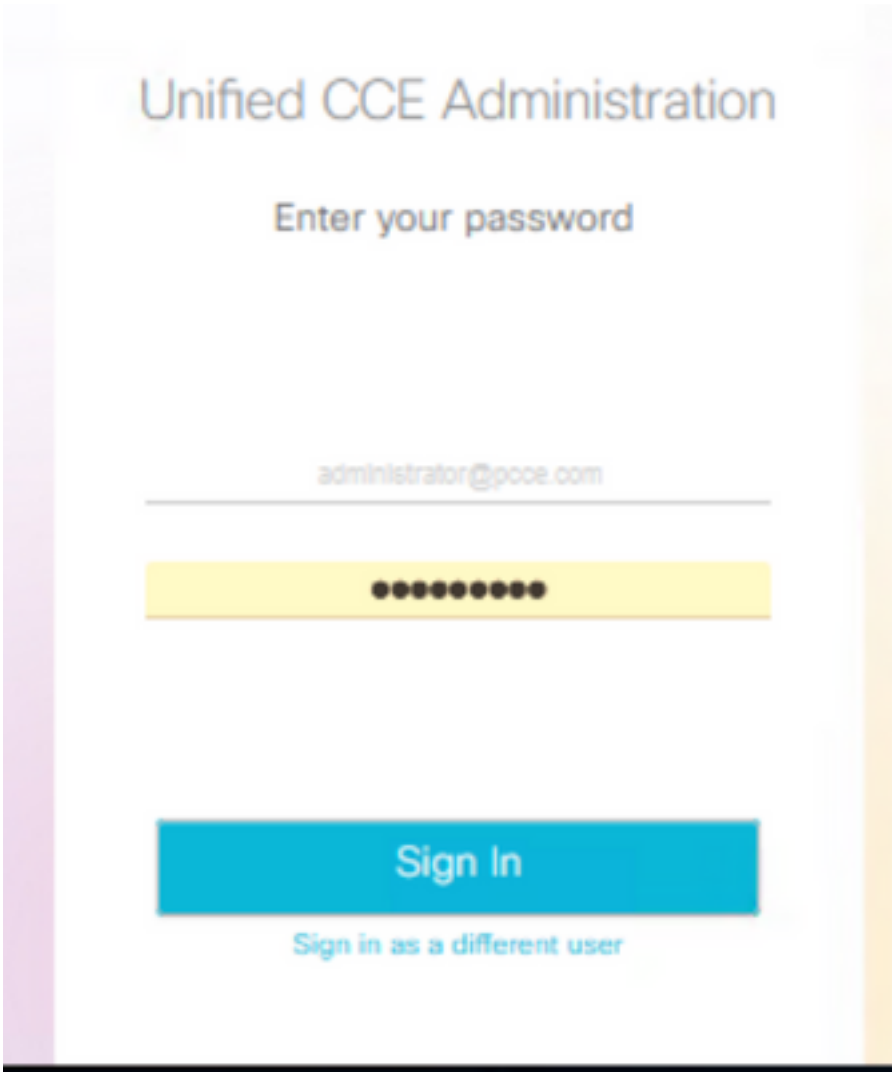


4. 点击ZIP文件链接并 save 您选择的位置中的文件。

设置跟踪和收集PCCE日志

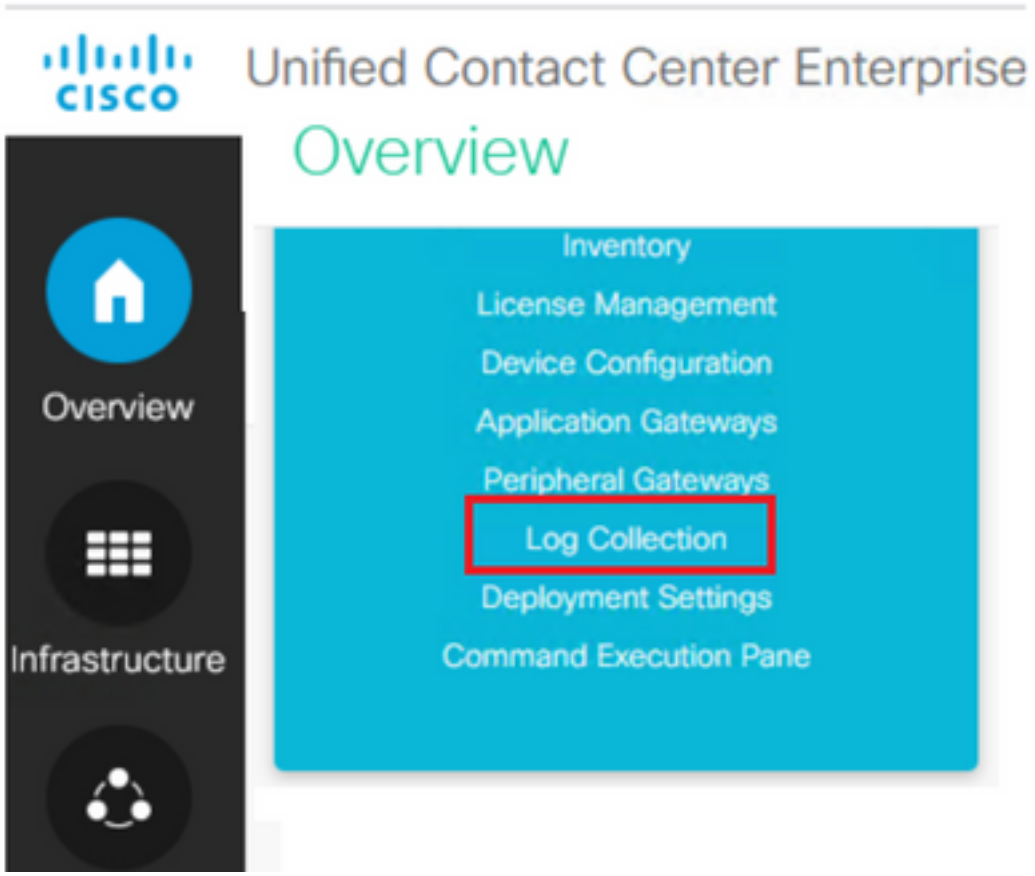
PCCE拥有自己的工具来设置跟踪级别。它不适用于UCCE环境，其中诊断框架Portico或系统CLI是启用和收集日志的首选方法。

1. 从PCCE AW服务器打开Unified CCE Web Administration工具并登录管理员帐户。

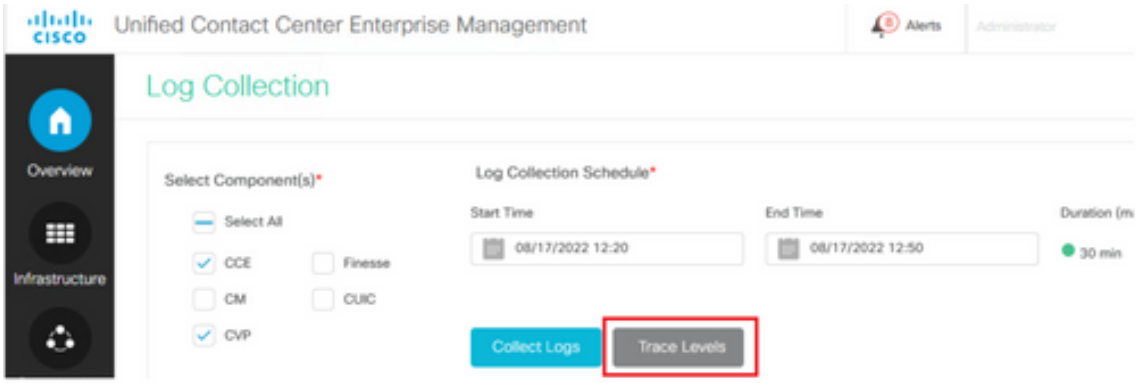


2. 导航到**概述(Overview)->基础设施设置(Infrastructure Settings)->日志收集(Log Collection)**，以

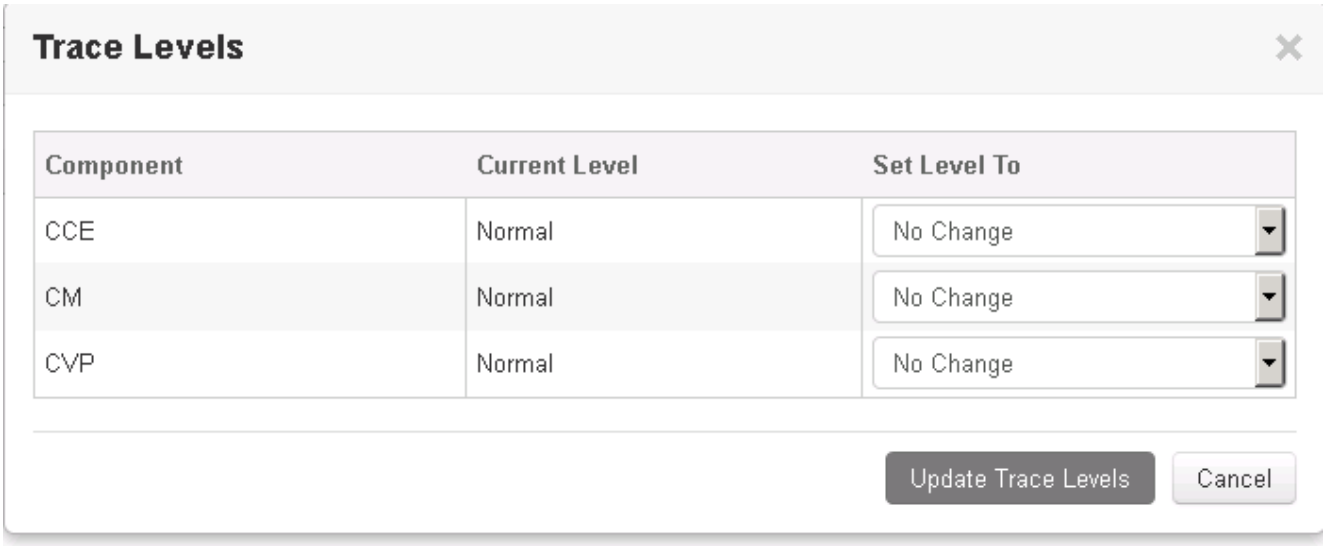
打开“日志收集”(Log Collection)页面。



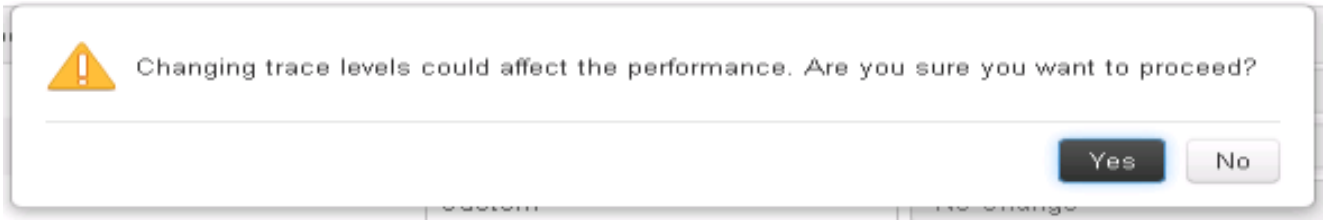
3. 在“日志收集”(Log Collection)页面上，单击**跟踪级别**，打开“跟踪级别”(**Trace Levels)**对话框。



4. 在CCE上将Trace Level设置为**Detailed**，并将CM和CVP保留为**No Change**，然后单击 **更新跟踪级别。**



5. 单击**Yes**确认警告。



6. 重现问题后，打开**Unified CCE Administration**并导航回**System > 日志收集。**
7. 在Components窗格中选择**CCE**和**CVP**。
8. 选择适当的日志收集时间（默认值为30分钟）。
9. 单击**Collect Logs**，然后单击**Yes**打开对话框警告。日志收集开始。等待几分钟，直到它完成。

10. 完成后，点击**操作**列中的**下载**按钮可下载包含所有日志的压缩文件。 Save 您找到适当位置的**zip**文件。

设置跟踪和收集CUIC/实时数据/IDS日志

SSH

1. 登录到CUIC、LD和IDS的SSH命令行(CLI)。
2. 运行命令以收集CUIC相关日志。

```
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. 运行命令以收集LD相关日志。

```
file get activelog livedata/logs/*.*
```

4. 运行命令以收集Ids相关日志。

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

5. 这些日志存储在SFTP服务器路径上：<IP地址>\<日期时间戳>\active_nnn.tgz ，其中nnn是长格式的时间戳。

RTMT

1. 从OAMP页面下载RTMT。登录https://<HOST ADDRESS>/oamp，其中HOST ADDRESS是服务器的IP地址。

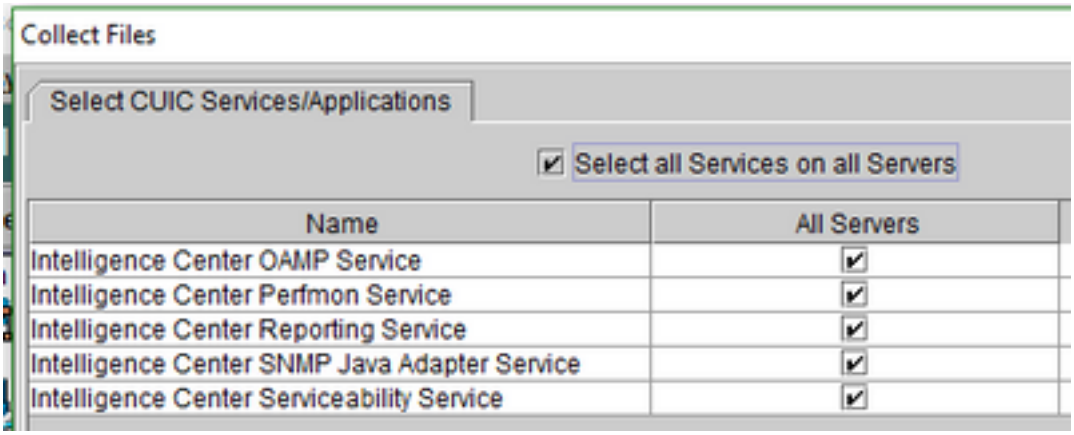
2. 导航到**工具> RTMT插件**下载。下载并安装插件。

3. 启动RTMT并使用管理员凭据登录到服务器。

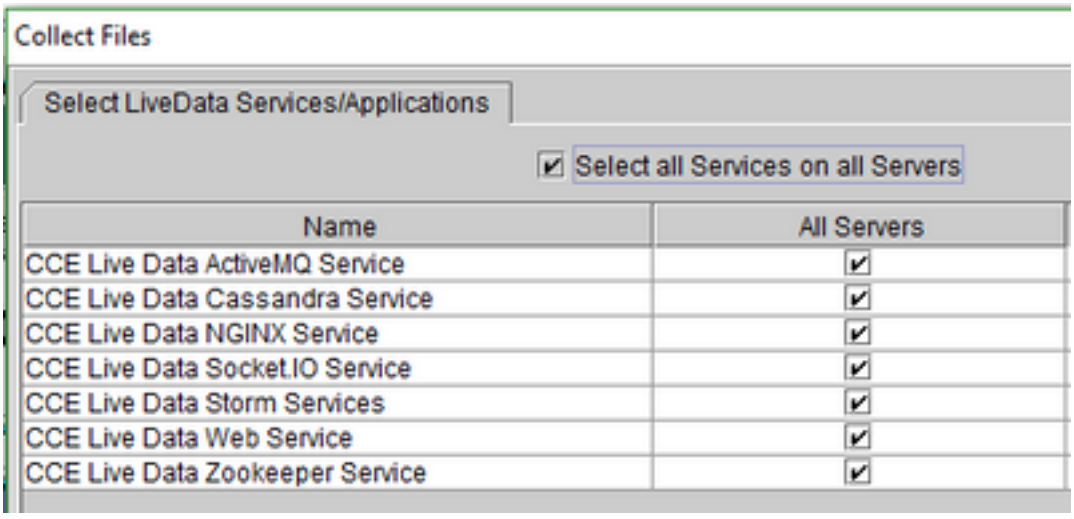
4. 双击**Trace and Log Central**，然后双击**Collect Files**。

5. 您可以看到特定服务的这些选项卡。您必须为CUIC、LD和IDS选择所有服务/服务器。

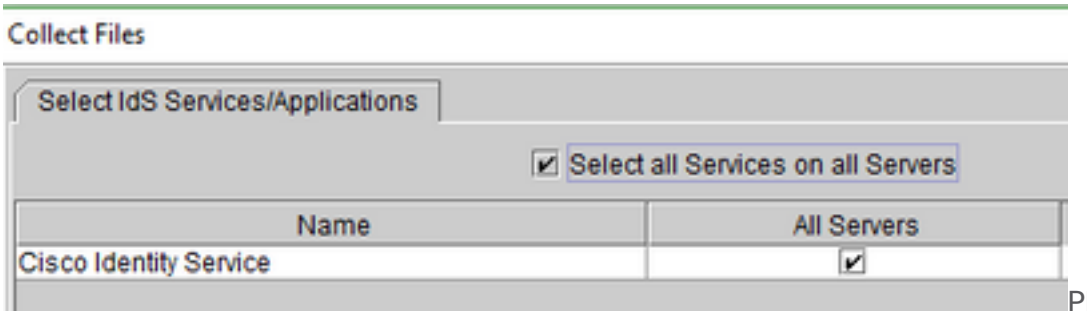
CUIC:



LD:

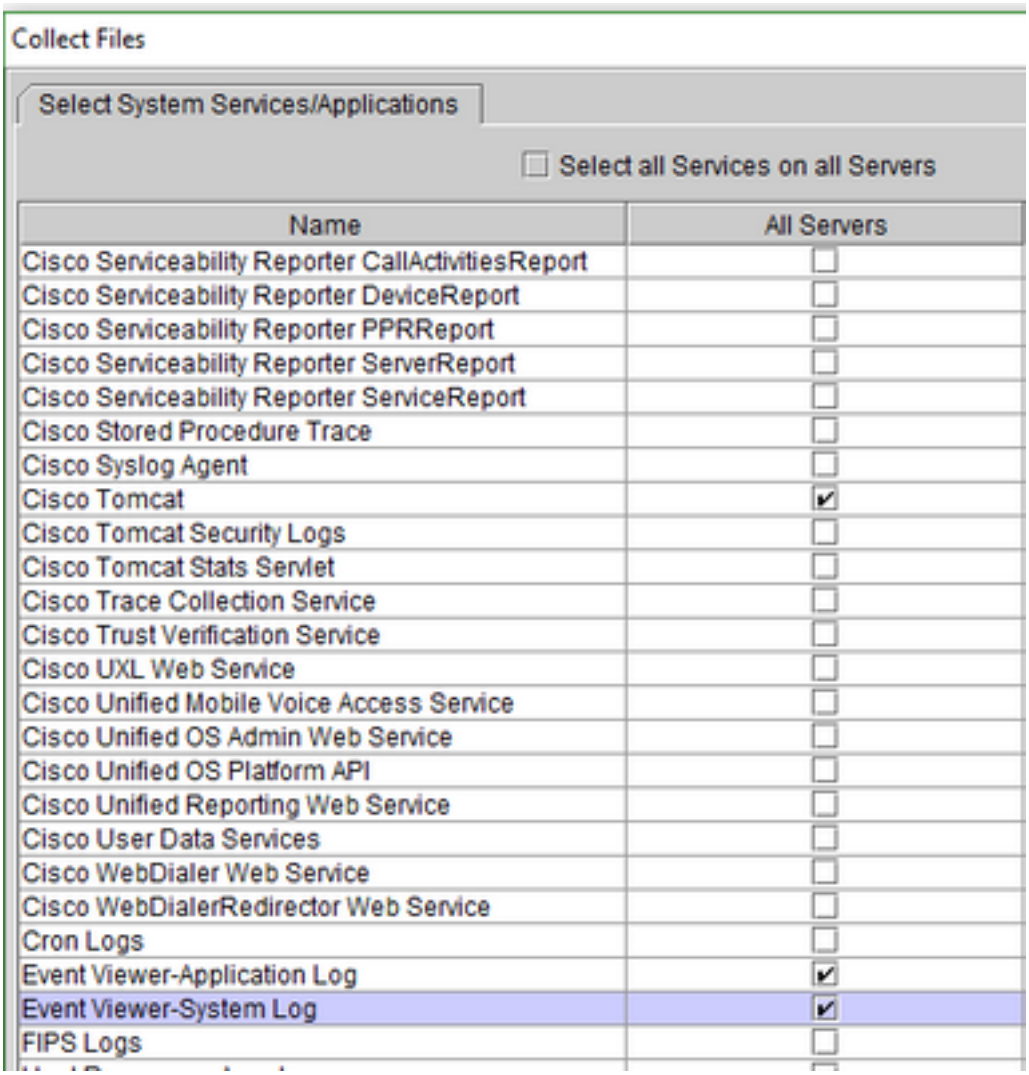


IDS:



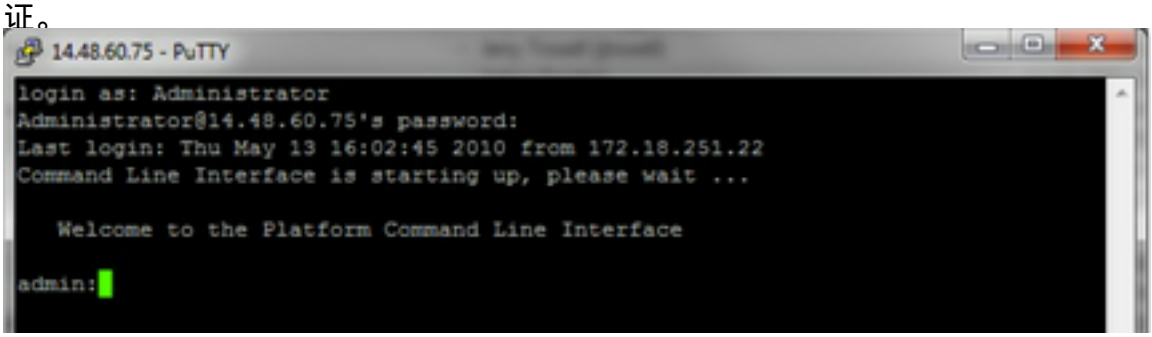
PlatformTomcat

Event Viewer



6. 选择**Date and Time**以及目标文件夹，以便 save 日志。

VoS上的数据包捕获(Finesse、CUIC、VVB)

1. 开始捕获 要开始捕获，请建立到VOS服务器的SSH会话，并使用平台管理员帐户进行身份验证。
2. 

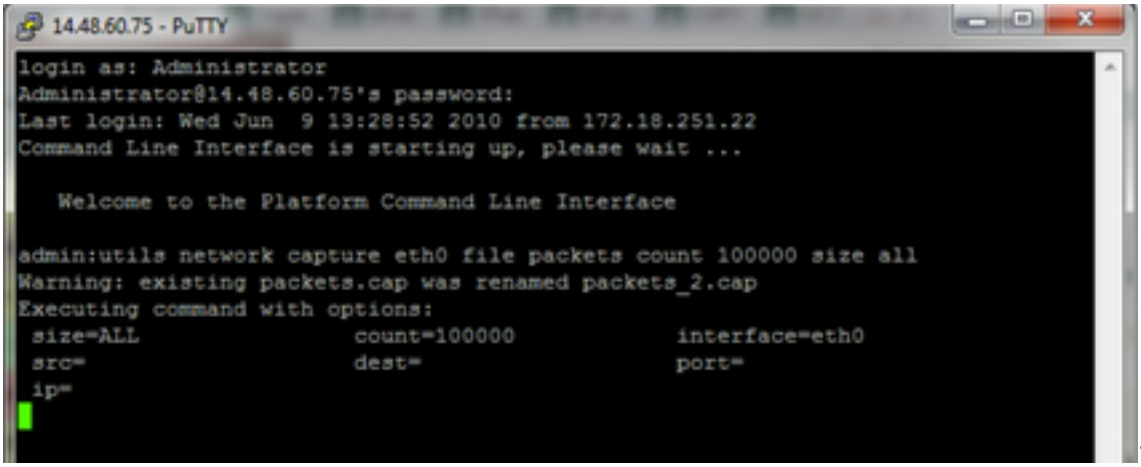
1a。命令语法

命令为 **utils network capture**语法如下：

```
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"
```

1b。捕获所有流量

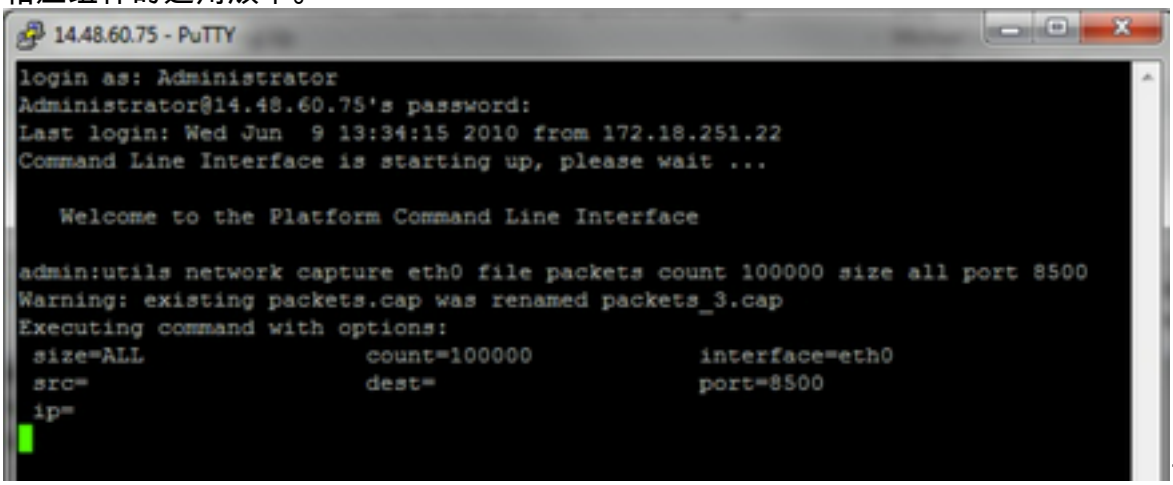
对于典型的捕获，可以将所有大小的ALL地址之间的所有数据包收集到一个名为packets.cap的捕获文件中。 为此，只需在管理CLI上执行 **utils network capture eth0 file packets count 100000 size all**



1c。根据端口号捕获

为了排除与集群管理器的通信问题，需要使用端口选项根据特定端口(8500)进行捕获。

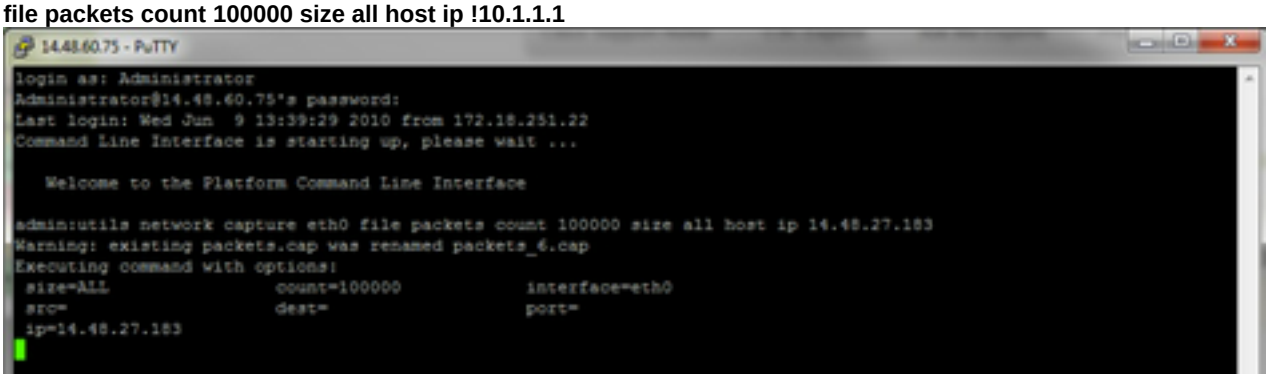
有关哪些服务需要在每个端口上进行通信的详细信息，请参阅TCP和UDP端口使用指南，了解相应组件的适用版本。



1d。根据主机捕获

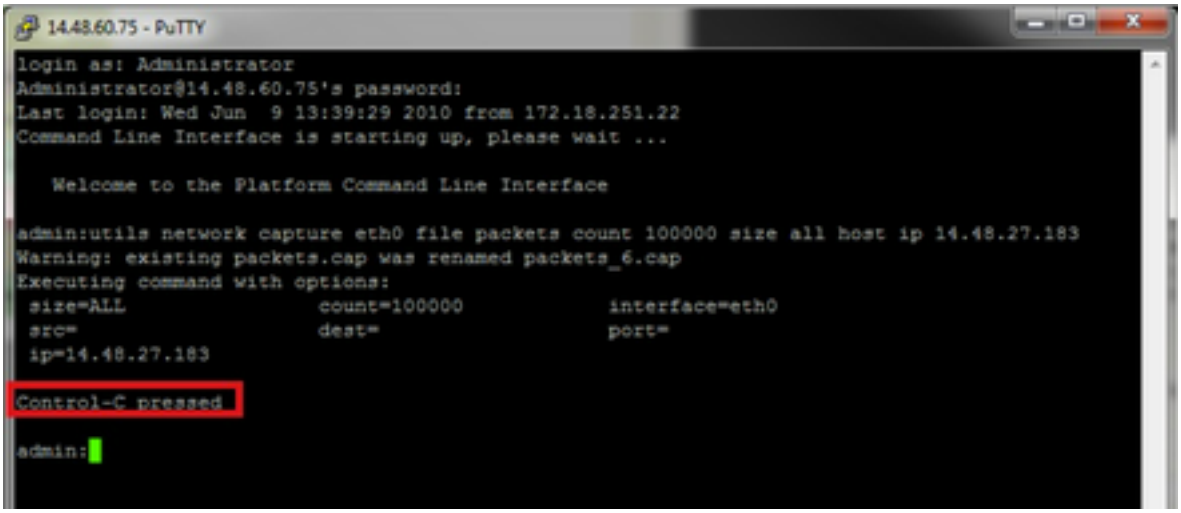
要排除VOS和特定主机的故障，可能需要使用“host”选项过滤进出特定主机的流量。

可能还需要排除特定主机，在本例中应使用“！”在IP地址前面。 例如 **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**



3. 重现问题症状 捕获开始时，会重现问题症状或情况，以便将必要的数据包包含在捕获过程中。如果问题间歇性出现，则可能需要长时间运行捕获。如果捕获结束，这是因为缓冲区已满，请重新启动捕获并自动重命名之前的捕获，这样就不会丢失之前的捕获。如果长时间需要捕获，请使用交换机上的监控会话在网络级别捕获。
4. 停止捕获 要停止捕获，请按住Control键并按键盘上的C。这会导致捕获进程结束，并且不会向捕获转储中添加任何新数据包。

5.



完成后，捕获文件将存储在服务器上“activelog platform/cli/”位置

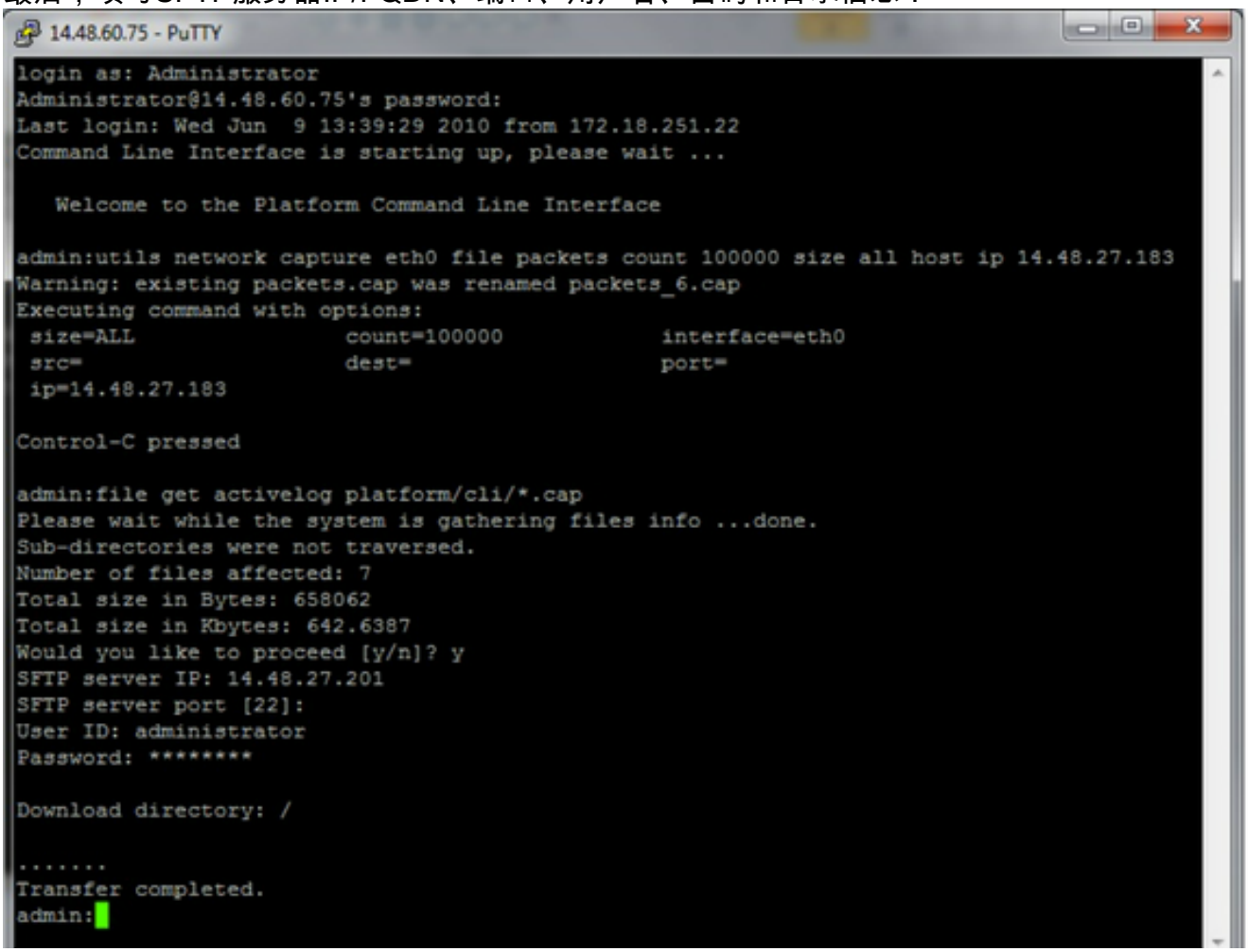
6. 从服务器收集捕获

捕获文件存储在服务器上的“activelog platform/cli/”位置。您可以使用RTMT通过CLI将文件传输到SFTP服务器或本地PC。 4a。通过CLI将捕获文件传输到SFTP服务器

使用命令 **file get activelog platform/cli/packets.cap** 将packets.cap文件收集到SFTP服务器。

或者，要收集服务器上存储的所有.cap文件，请使用'file get activelog platform/cli/*.cap

最后，填写SFTP服务器IP/FQDN、端口、用户名、密码和目录信息：

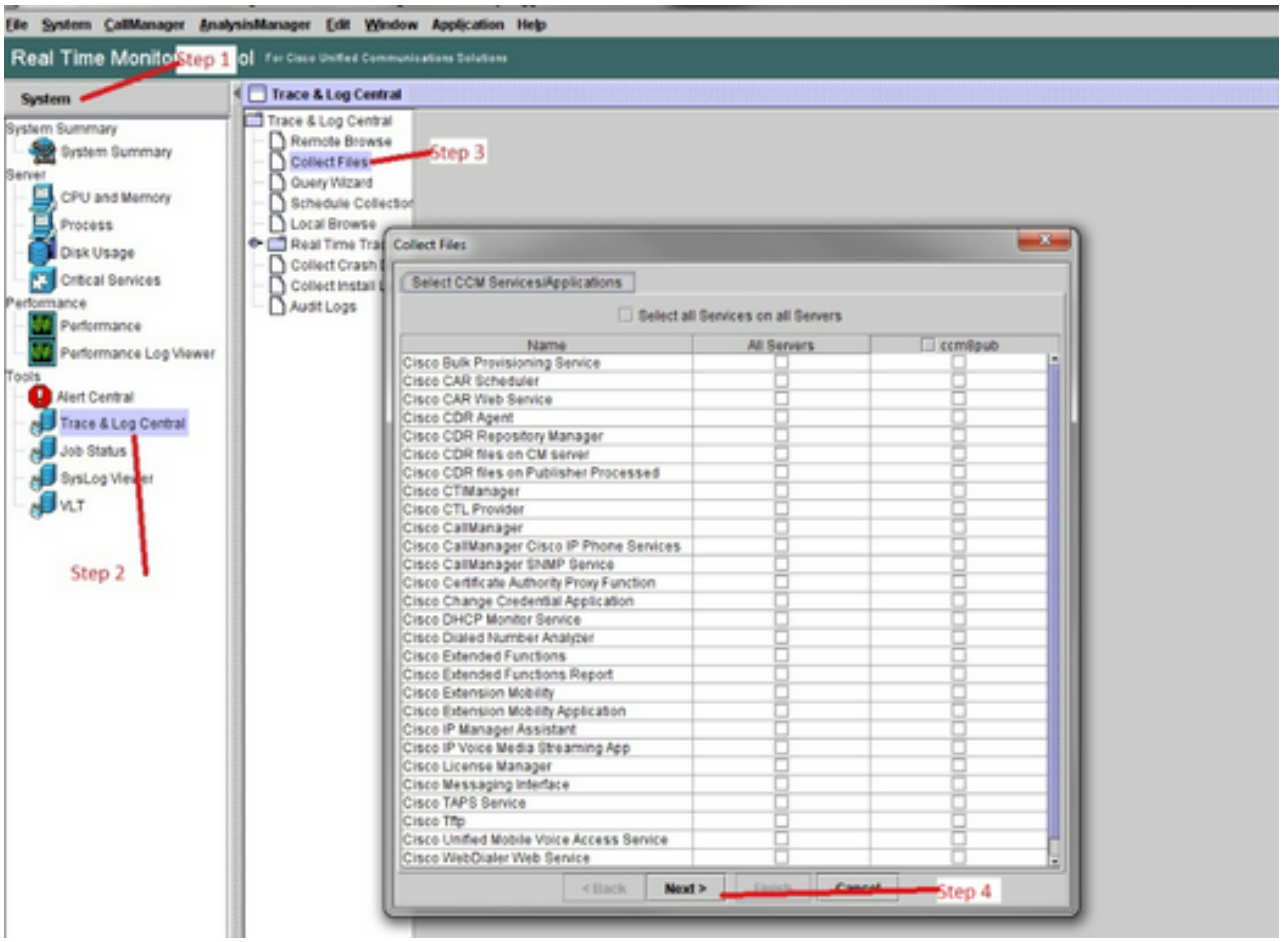


CLI指示文件传输到SFTP服务器成功或失败。

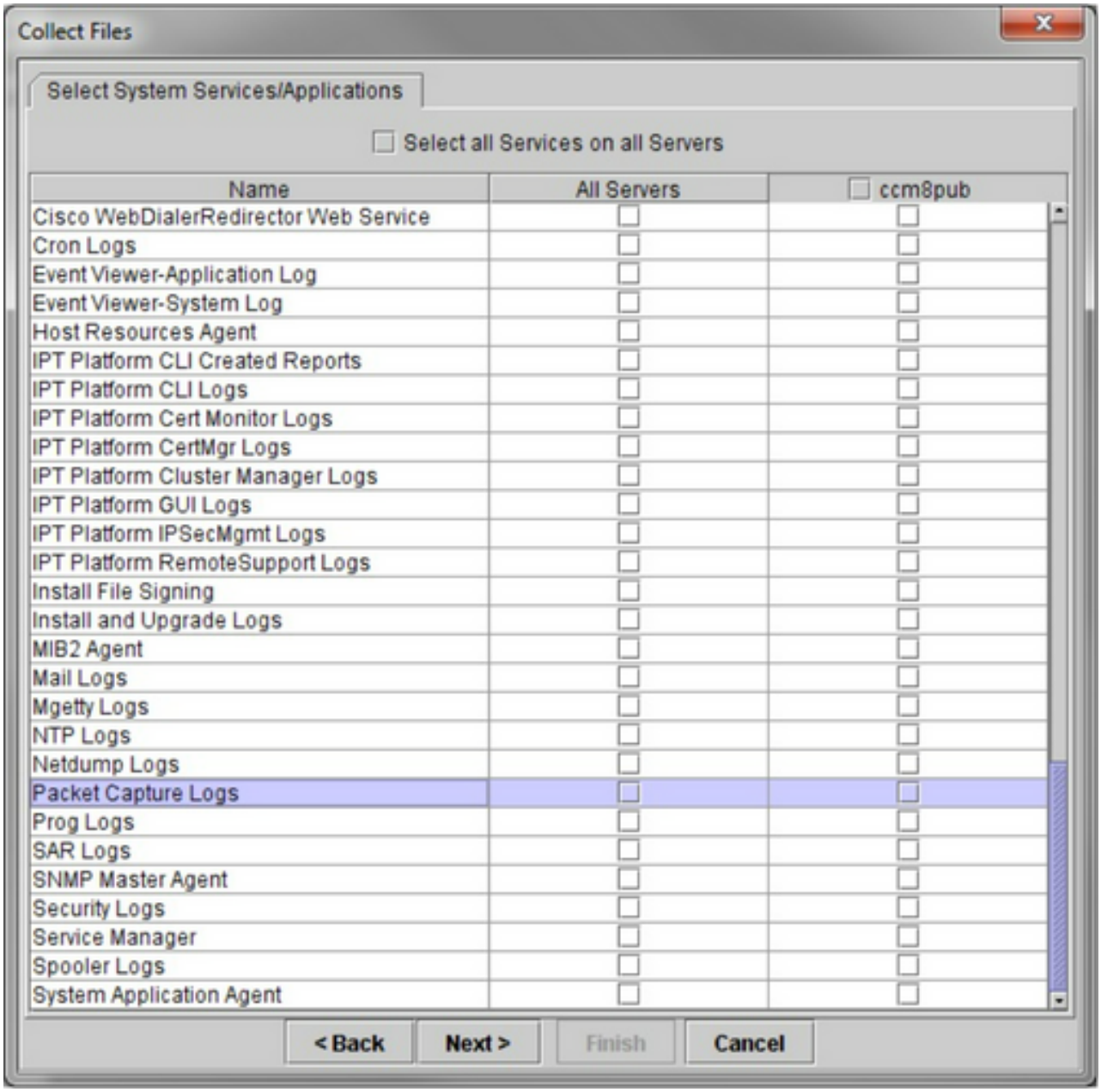
4b。使用RTMT将捕获文件传输到本地PC。

启动 RTMT。 如果未安装在本地PC上，请从VOS Administration页面安装适当的版本，然后

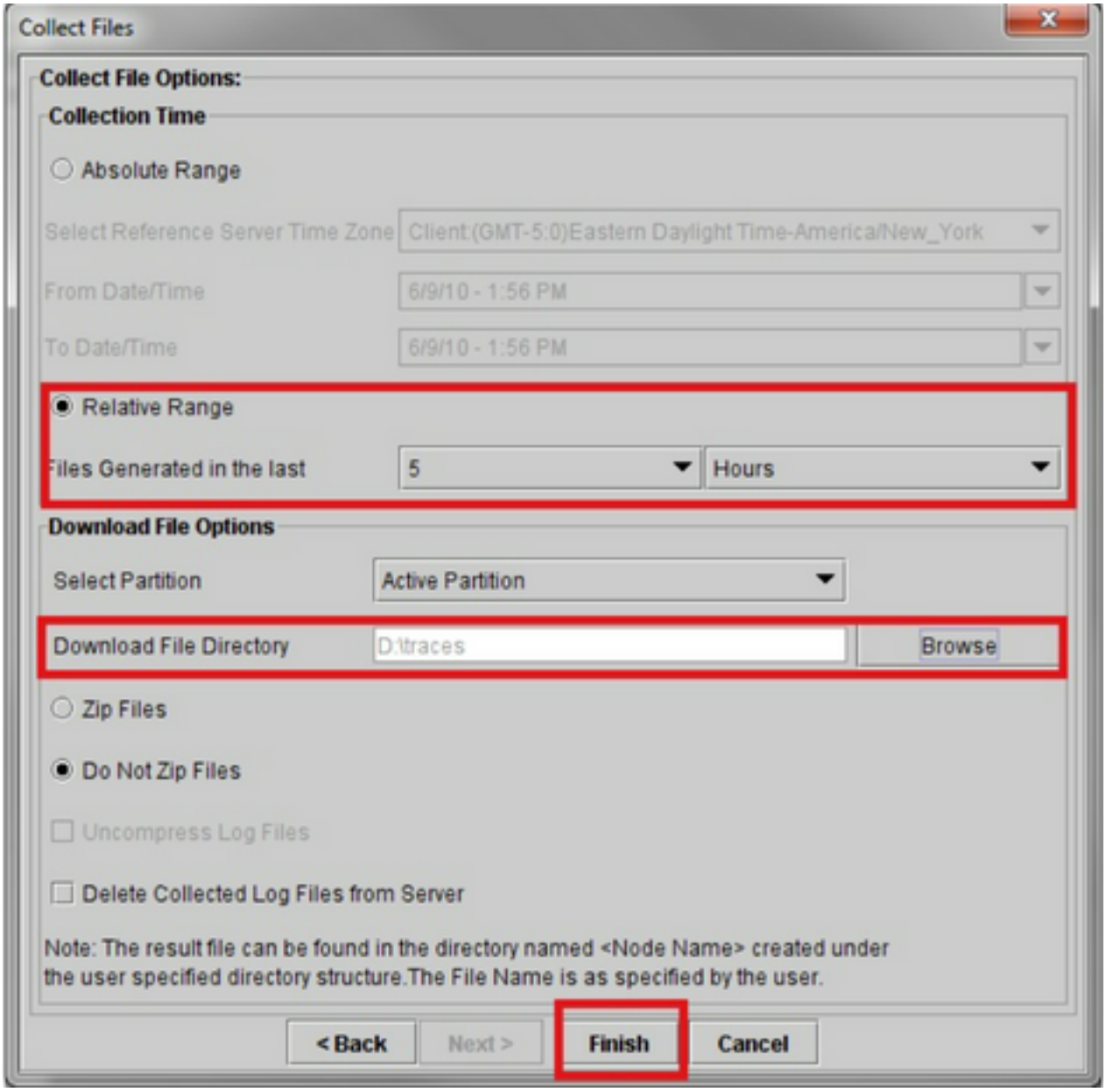
转到Applications -> Plugins菜单。
单击System，然后单击Trace & Log Central，然后双击Collect Files。 单击第一个菜单中的Next。



在第二个菜单中，选中执行捕获的服务器上Packet Capture Logs的复选框，然后单击Next。



在最终屏幕上，选择执行捕获的时间范围以及本地PC上的下载目录。



RTMT关闭此窗口并继续收集文件并将其存储在指定位置的本地PC上。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。