Set Traces and Collect Logs in CCE

Contents

Introduction

Prerequisites

Requirements

Components Used

Set Traces and Collect Finesse Logs

Finesse Client

Option 1: Collect Client Logs Through the Send Error Report Option 2: Set Persistent Logging

Option 3: Web Browser Console

Finesse Server

Option 1: Via the User Interface (UI) - Web Services (Required) and Additional Logs Option 2: Via SSH and Secure File Transfer Protocol (SFTP) - Recommended Option

Set Traces and Collect CVP and CVVB Logs

CVP Call Server

CVP Voice XML (VXML) Application

CVP Operations and Administration Management Portal (OAMP)

Cisco Virtualized Voice Browser (CVVB)

Option 1: Via Administration Account

Option 2: Via SSH and SFTP - Recommended Option

Set Trace and Collect Logs for CUBE and CUSP

CUBE (SIP)

<u>CUSP</u>

Collect the Logs

Set Trace and Collect UCCE Logs

SetTrace Level

Log Collection

Set Trace and Collect PCCE Logs

Set Trace and Collect CUIC/Live Data/IDS Logs

Download logs with SSH

Download Logs with RTMT

Packet Capture on VoS (Finesse, CUIC, VVB)

Introduction

This document describes how to set and collect traces in Cisco Unified Contact Center Enterprise (CCE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Contact Center Enterprise (UCCE)
- Package Contact Center Enterprise (PCCE)
- Cisco Finesse
- Cisco Customer Voice Portal (CVP)
- Cisco Virtualized Voice Browser (VVB)
- Cisco Unified Border Element (CUBE)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Session Initiation Protocol (SIP) Proxy (CUSP)

Components Used

The information in this document is based on these software versions:

- Cisco Finesse Release 12.5
- CVP Server Release 12.5
- UCCE/PCCE Release 12.5
- Cisco VVB Release 12.5
- CUIC Release 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. If your network is live, ensure that you understand the potential impact of any command.

Set Traces and Collect Finesse Logs

Finesse Client

There are several options to collect Finesse client logs.

Option 1: Collect Client Logs Through the Send Error Report

- 1. Log an agent in.
- 2. If an agent experiences any problem during a call or media event, instruct the agent to click the **Send Error Report** link on the top right-hand corner of the finesse desktop.



- 3. The agent sees the **Logs Successfully Sent!** message.
- 4. The client logs are sent to the Finesse server. Navigate to <u>https://x.x.x.x/finesse/logs</u> and log in with an administration account.
- 5. Collect the logs under the **clientlogs**/ directory.

Directory Listing For /logs/ - Up To /

Filename	Size	Last Modifi
<u>3rdpartygadget/</u>		Mon, 22 Feb 2021 23:06:32
admin/		Tue, 12 Jul 2022 18:52:53
<u>cli.log</u>	0.0 kb	Mon, 22 Feb 2021 22:59:10
clientlogs/		Wed, 17 Aug 2022 15:35:52

Option 2: Set Persistent Logging

- 1. Navigate to <u>https://x.x.x.x8445/desktop/locallog</u>.
- 2. Click Sign In With Persistent Logging.



3. The Cisco Finesse agent desktop login page opens. Log the agent in.

Cisco Finesse	
sumohanr	
600003	
Sign in as a Mobile Agent	
Sign In	

4. All the agent desktop interaction is registered and sent to the local storage logs. To collect the logs, navigate to <u>https://x.x.x.8445/desktop/locallog</u> and copy the content into a text file. **Save** the file for further analysis.

Option 3: Web Browser Console

- 1. After an agent logs in, press F12 to open the browser console.
- 2. Select the **Console** tab.
- 3. Check the browser console for the errors. Copy the content into a text file and Save it.

altalta cisco	Cisco Finesse	Not Ready 00:02:57			(C) (C)
*	Team Performance				
Home	Billing	✓ Q Search	Include Logged Out Ag	gents	
	Agent Name	 State 	Time in State	Extension	Actions
	John Cena	Ready	256:57:32	6000002	
Team Data					
ັ ເຈັກີ L Elem	ents Console Sources Network	Performance Memory Application	Security Lighthouse Recorder	Performance insights & AdBlock	08 🛱 🗄 2
▶ ⊘ top ▼	Filter				Default levels • No Issues 4
2022-08-1711	L:16:45.885 -05:00: : 12-FINA.chase	e.com:	: Container :		finesse.js:3742
2022-08-1711	1:16:45.886 -05:00: : 12-FINA.chase	e.com:	: Container : Finesse logger in	nitialized	finesse.js:3742
2022-08-17T1:	L:16:45.886 -05:00: : 12-FINA.chase	e.com:	: Container : Started on: Wed /	Aug 17 2022 11:16:45 GMT-0500 (Centra)	l Daylight <u>finesse.js:3742</u>

4. Select the Network tab, and check the Preserve log option.

5. Right-click any of the network name events and select save as HAR with content.

cisco	Cisco Finesse	Ready ~ ~	Î	 □ Elements ● ◎ ▼ ♀ 	Console Sources I	Network > 08 \$
	Team Performance			≜ Filter	Invert Hide	data URLs
Home	Billing ~	Q Search	Includ	All Fetch/XHR JS C	SS Img Media Font Doc Blocked Requests	WS Wasm Manifest Other Ird-party requests
A	Agent Name	State	Time in State	200000 ms 400000 m	a 600000 ma 800000 ma	1000000 ma 1200000 ma 1400000 ma 16000
Ŭ	John Cena	Ready	257:21:23			
Team Data				Name SystemInfo?getTime 434626014 SystemInfo?getTi 434626014 icon-voice-ready SystemInfo?getTi SystemInfo?getTi SystemIn	Open in new tab Open in new tab Clear browser cache Clear browser cache Clear browser cookies Copy Block request URL Block request domain Replay X0HR Sort By Header Options	<pre>raycaad review Response x s://12-fina.chase.com:8445/fin forgetTimeStamp&nocache=16607 ET 0.201.224.59:8445 rict-origin-whem-cross-origin pse-headers: Access-Control-All control-Allow-Credentials,Acce Methods,Access-Control-Mux-Age llow-Meaders</pre>

Finesse Server

Option 1: Via the User Interface (UI) - Web Services (Required) and Additional Logs

- 1. Navigate to https://x.x.x./finesse/logs and log in with the administration account.
- 2. Expand the directory **webservices**/.

openfire/	Tue, 02 Aug 2022 00:45:59 G
openfireservice/	Thu, 07 May 2020 01:38:30 G
realm/	Wed, 17 Aug 2022 01:55:51 G
tomcat/	Sat, 13 Aug 2022 03:01:01 G
webservices/	Sun, 14 Aug 2022 07:41:43 G

- Apache Tomcat/7.0.94
- 3. Collect the last web service logs. Select the last unzip file. For Instance, **Desktop-Webservices.201X**-..log.zip. Click the file link and you see the option to **Save** the file.

Directory Listing For /logs/webservices/ - Up To /logs						
Filename	Size	Last Modified				
Desktop-webservices.2022-08-10T04-43-22.953.log.zip	4732.1 kb	Sun, 14 Aug 2022 07:40:54 GMT				
Desktop-webservices.2022-08-14T00-40-54.953.log	90079.1 kb	Wed, 17 Aug 2022 16:26:44 GMT				

4. Collect the other required logs (depends on the scenario). For instance, openfire for notification service issues, realm logs for authentication issue, and tomcatlogs for APIs issues.

Note: The recommended method to collect the Cisco Finesse server logs is via Secure Shell (SSH) and Secure File Transfer Protocol (SFTP). This method does not only allow you to collect the webservices logs but all additional logs like, Fippa, openfire, Realm, and Clientlogs.

Option 2: Via SSH and Secure File Transfer Protocol (SFTP) - Recommended Option

- 1. Log in to the Finesse server with the SSH.
- 2. Enter this command in order to collect the logs you need. The command collects the logs for 2 hours. You are prompted to identify SFTP server where the logs are uploaded.



- 3. These logs are stored on the SFTP server path: $\langle IP address \rangle \langle date time stamp \rangle \langle active_nnn.tgz , where nnn is timestamp in long format.$
- 4. To collect additional logs like tomcat, Context service, Servm and install logs, look at the Log Collection section of the <u>Cisco Finesse Administration Guide Release 12.5(1)</u>.

Set Traces and Collect CVP and CVVB Logs

CVP Call Server

- 1. The CVP CallServer default level of traces is enough to troubleshoot most of the cases. However, when you need to get more detail on the Session Initiation Protocol (SIP) messages, you need to set the SIP strack traces to the DEBUG level.
- 2. Navigate to the CVP CallServer Diag webpage URL http://localhost:8000/cvp/diag.

Note: This page provides good information about the CVP CallServer and it is very useful to troubleshoot certain scenarios.

3. Select **com.dynamicsoft.DsLibs.DsUALibs** from the **Serv. Mgr** dropdown menu at the top left-hand corner.

Serv Mgr:	org.springframework
Level:	org.springframework SIP
INFRA	org.apache RPT
SUBSYSTEN	SIP.INOUT
.D:	<u>com.dynamicsoft.DsLibs.DsUALibs</u> Infrastructure IVR
)ETAIL:	mmca ICM
\GE_HANDLII	VMS
	MSGBUS

4. Click the **Set** button.



These are your debug settings.

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

6. When you reproduce the problem, collect the logs from C:\Cisco\CVP\logs and select the CVP log file based on the time the problem occurred.

	> Loc	al Disk (C:) > Cisco > CVP > logs >	~ 0	Search logs	م
		Name	Date modified	Туре	Size
55		CVP.2022-08-17.00.log	8/17/2022 9:46 AM	Text Document	2,137 KB
de la	4	CVP.2022-08-16.00.log	8/17/2022 12:00 AM	Text Document	5,231 KB

7. After you reproduce the problem, ensure to restore the traces to the default level. Select **com.dynamicsoft.DsLibs.DsUALibs** from the **Serv. Mgr** dropdown menu at the top left-hand corner and set it to error.

Serv Mgr: com.dynamicsoft.DsLibs.DsUALibs 🗸							
Level: DEBUG 🗸							
STANDARD		INFRA		LEGACY MSG	5	ICM CUSTOM	
ALL:		LOAD_SUBSYSTEM:		MSGLAYER_MESSAGE:		GED125_LOW_LEVEL:	
CALL:		THREAD:		MSGLAYER_METHOD:		MSGBUS_LOW_LEVEL:	
METHOD:		MSG:		MSGLAYER_HANDLED_EXCEPTION:		ICM_SUBSYSTEM_ADMIN:	
PARAM:		MSG_DETAIL:		MSGLAYER_PARAM:			
LOW_LEVEL:		MESSAGE_HANDLING:		GLOBAL_EVENT:			
CLASSDUMP:		TIMER:		EXTERNAL_EVENT:			
HEARTBEAT:		STATE:		STATIC_FIELD:			
HANDLED_EXCEPTION:		SECURITY:		EXTERNAL_STATE:			
DOOQUEUE:		LICENSING:		INTERNAL_STATE:			
GARBAGE_COLLECTOR:		STARTUP:		CODE_BRANCH:			
MESSAGE:		SHUTDOWN:		CODE_MARKER:			
RPT_JDBC:		STATS:		CLASS_DUMP:			
RPT_CALL_REG:		SNMP:		LOCAL_DUMP:			
RPT_BATCH:		SAF:					
Cat				•			
Set							
EBUG/0 - DEBUG/41 - DEBUG/40							
IAME				L	EVEL	MASK	
ro sprinoframework					VARN	41	
rg.apache					RROR	0	
RPT					NFO	0	
SIP.INOUT				N	VARN	0	

SENOUT	TYANA	0
com.dynamicsoft.DsLibs.DsUALibs	ERROR	0
Infrastructure	NFO	0
NR	DEBUG	41
mmca	NFO	0
ICM	DEBUG	41
ALL_SS	INFO	0
MSGBUS	NFO	0

CVP Voice XML (VXML) Application

In very rare circumstances you need to increase the level of traces of the VXML server applications. On the other hand, it is not recommended to increase it unless a Cisco Engineer requests it.

To collect the VXML server application logs, navigate to the specific application directory under the VXML server, for example: C:\Cisco\CVP\VXMLServer\applications\{name of application}\logs\ActivityLog\ and collect the activity logs.

- «	app	lications > BillingQueue > logs > ActivityLog	ٽ ~	Search ActivityLo	g ,
		Name	Date modified	Туре	Size
is	*	activity_log2021-07-29-16-29-46.bt	7/29/2021 4:29 PM	Text Document	7 KB

CVP Operations and Administration Management Portal (OAMP)

In most of the cases the default level of traces of OAMP and ORM are enough to determine the root cause of the problem. However, if the level of traces is required to be increased, here are the steps to execute this action:

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

2. Edit %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. Restart OPSConsoleServer after the modification as shown.

Trace Level Information

Trace Level	ace vel Description		Trace Mask
0	Product install default. No or minimal performance impact expected.	INFO	None
1	Less detailed trace messages with a small performance impact.	DEBUG	DEVICE_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x01011000
2	Detailed trace messages with a medium performance impact.	DEBUG	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + DATABASE_MODIFY + MANAGEMENT=0x05011000
3	Detailed trace message with a high performance impact.	DEBUG	DEVICE_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + DATABASE_MODIFY + MANAGEMENT=0x05111000

Trace Level	Description	Log Level	Trace Mask
4	Detailed trace message with a very high performance impact.	DEBUG	MISC + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + MANAGEMENT + TRACE_METHOD + TRACE_PARAM=0x17371000
5	Highest detailed trace message.	DEBUG	MISC + DEVICE_CONFIGURATION + ST_CONFIGURATION + SYSLVL_CONFIGURATION + BULK_OPERATIONS + BULK_EXCEPTION_STACKTRACE + DATABASE_MODIFY + DATABASE_SELECT + DATABASE_PO_INFO + MANAGEMENT + TRACE_METHOD + TRACE_PARAM=0x17371006

Cisco Virtualized Voice Browser (CVVB)

In CVVB, a trace file is a log file that records activity from the Cisco VVB component subsystems and steps.

Cisco VVB has two main components:

- Cisco VVB Administration traces termed as MADM logs
- Cisco VVB Engine traces termed as MIVR logs

You can specify the components for which you want to collect information and the level of information that you want to collect.

Log Levels extend from:

- Debugging Basic flow details to
- XDebugging 5 Detailed level with Stack Trace

CISCO For Cisco Virtualized Voice Browser	owser Serviceability				Tuny	Administrator
Trace Tools Help						Partiting and
e Configuration - Cisco Virtualized Voic	e Browser Engine					
Save 🔊 Restore Defaults III Check All	H UnCheck All					
	H					
Ready						
lect Service						
ect Service * Engine V Go						
dmum No. of Files * 300 dmum File Size (KB) * 10485						
imum No. of Files * 300 imum File Size (KB) * 10485	Debuoging	XDebussion1	XDebuoning2	XDebuosing3	XDebuoring4	XDebuncino5
imum No. of Files * 300 imum File Size (KB) * 10495 ace Filter Setting IDRARIES	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Site (KB) * 10495 co Filter Setting totacilly JIBRARIES LIB_CFG	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Site (KB) * 10485 co Filter Setting tifsally JBRARIES LIB_CFG LIB_EVENT	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Site (KB) * 10485 sce Filter Setting tiftacily JIBRARIES LIB_CFG LIB_EVENT LIB_DDBC	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Size (KB) * 10485 cce Filter Setting Macilly IBRARIES LIB_CFG LIB_DEC LIB_JINI	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Size (KB) * 10485 centre Setting Idea Size (KB) * 10485 Idea Siz	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Size (KB) * 10495 bfacility BFARRES LIB_CFG LIB_JOBC LIB_JOBC LIB_JOBC LIB_LICENSE LIB_LICENSE LIB_MEDIA	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Size (KB) * 10495 acce Filter Setting Id4a510 Id4a510 Id5a107 Id5a07 Id5_ID5C Id5_ID	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
imum No. of Files * 300 imum File Site (KB) * 10485 10485 1056011/ JIBRARIES LIB_VENT LIB_UDBC LIB_VIN LIB_LICENSE LIB_MIN LIB_MEDIA LIB_KENLET	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5
amum No. of Files * 300 imum File Size (KB) * 10485 ace Filter Setting ubfacility JBRARIES LIB_CFG LIB_UCENSE LIB_UDBC LIB_UCENSE LIB_UDA LIB_EDIA LIB_RMI LIB_SERVLET LIB_TC	Debugging	XDebugging1	XDebugging2	XDebugging3	XDebugging4	XDebugging5

Warning: Xdebugging5 must not be enabled on production loaded system.

The most common logs that you need to collect are the Engine. The default level of traces for the CVVB Engine traces is enough to troubleshoot most issues. However, if you need to change the level of traces for a specific scenario, Cisco recommends that you use the pre-defined System Log Profiles.

System Log Profiles

Name	Scenario in which this Profile must be Activated			
DefaultVVB	Generic logs are enabled.			
AppAdminVVB	For issues with web administration through AppAdmin, Cisco VVB Serviceability, and other web pages.			
MediaVVB	For issues with media setup or media transmission.			
VoiceBrowserVVB	For issues with calls handle.			
MRCPVVB	For issues with ASR/TTS with Cisco VVB interaction.			
CallControlVVB	For issues with SIP signal related are published in the log.			

Option 1: Via Administration Account

1. Open the CVVB main page (https://X.X.X.X/uccxservice/main.htm), and navigate to the Cisco VVB

Serviceability page. Log in with the administration account

cisco	Cisco Virtualized Voice Browser Serviceability For Cisco Virtualized Voice Browser	Navigation Cisco WB Serviceability V Go Administrator About Logout
Alarm Trac	ce Tools Help	

2. Select **Trace > Profile**.



3. Check the profile that you want to enable for the specific scenario and click the **Enable** button. For example enable the profile CallControlVVB for SIP related issues or MRCPVVB for issues related to Automatic Speech Recognition and Text to Speech (ASR/TTS) interaction.

	cisco	Cisco Virtualized Voice Browser Serviceability For Cisco Virtualized Voice Browser
Alar	m Trace	e Tools Help
Log	Profile	es Management
2	Enable	3
_ St	atus ——	
	i) Rea	ady
P	rofiles —	
	D <u>MediaVV</u>	<u>/B</u>
0	DefaultV	<u>//B</u>
0	D <u>AppAdm</u>	<u>iinVVB</u>
(O <u>VoiceBro</u>	<u>owser/VB</u>
(CallCont	ITOIVVB
	D <u>mrcpv</u>	<u>VB</u>
E	nable	

4. You see the successful message after you click the **enable** button.

cisco	For Cisco	Virtualized Voice Browser Serviceability Virtualized Voice Browser
Alarm Tr	race Tools	Help
Log Prof	iles Mana	gement

Status CallControlVVB log profile configurations have been enabled successfully.

- 5. After the problem is reproduced, collect the logs. Use the Real Time Monitor Tool (RTMT) that comes with the CVVB to collect the logs.
- 6. Click the **Cisco Unified Real-Time Monitoring Tool** icon on your Desktop (if needed, download this tool from the CVVB).



7. Provide the IP address of the VVB and click **OK**.

Real-Time Monitoring Tool Login	×
Host IP Address: 10.10.10.30	
Ok Cancel Certificates	

8. Accept the Certificate information if displayed



9. Provide the credential and click **OK**.

Authentication Required	×
A username and password are	being requested by https://cvvb.cc.lab:8443
User Name:	admin
Password:	
Ok	Cancel

10. If you received the TimeZone error, RTMT can close after you click the **Yes** button. Relaunch the RTMT tool.

Timezon	e data version mismatch !!! 🛛 🔀
S	There is a mismatch between timezone version on this RTMT and the server you are trying to connect. Do you want to update the timezone tables on this RTMT to match to that of the server now ? This will need a restart of RTMT.
	Note: Choosing "No" would let you launch RTMT with current timezone version, but you may face some issues related to mismatch in time.
	Yes No

11. Leave the Default configuration selected and click **OK**.

Select Configuration	×
Configuration List:	
Default	
Description:	
OK Cancel	

12. Select Trace & Log Central and then double click Collect Files.



13. In the new open window, select the **Engine** and click **Next**.

Collect Files					×
Select WB Services/Applica	ations				
ľ		elect all Servi	res on all Serve	are	
	11.0	elect all Delvi	ces on an oeive	,10	
Name			All Servers		cvvb.cc.lab
Administration					
Cluster View Daemon					
DB Perfmon Counter Service					
Database					
Engine					
SNMP Java Adapter					
Voice Subagent					
	- De els				
	< Back	Next >	Finish	Cancel	

14. Click Next again in the next window.

Collect Files		×
Select System Services/Applications		
Colori		
	all Services on all Servers	
Name	All Servers	cvvb.cc.lab
Boot Logs		
Cisco AMC Service		
Cisco AMC Service AlertLog		
Cisco AMC Service CallLog		
Cisco AMC Service DeviceLog		
Cisco AMC Service PPRLog		
Cisco AMC Service ServerLog		
Cisco AMC Service ServiceLog		
Cisco AXL Web Service		
Cisco Abort Transaction Spooling		
Cisco Audit Event Service		
Cisco Audit Logs		
Cisco CAR Web Service		
Cisco CCM DBL Web Library		
Cisco CCM NCS Web Library		
Cisco CCM PD Web Service		
Cisco CCMAdmin Web Service		
Cisco CCMRealm Web Service		
Cisco CCMService Web Service		
Cisco CCMUser Web Service		
Cisco CDP		
Cisco CDP Agent		
Cisco CallManager Cisco IP Phone Services		
Cisco Certificate Change Notification		
Cisco Certificate Change Notification Service		
Cisco Change Credential Application		
Cisco Common User Interface		
< Back Ne	xt > Finish Cance	1

15. Select **Relative Range** and ensure you select time to cover the time of your bad call.

Collect File Options: Collection Time		
Absolute Range		
Select Reference Server Time Zone	Client:(GMT-5:0)Eastern Daylight Time-America/New_York	Ŧ
From Date/Time	5/15/17 - 7:03 AM	-
To Date/Time	5/15/17 - 8:03 AM	-

16. On the Download File Options, click **Browse** and select the directory where you want to save the file, then click **Open**.

a Open	×
Look <u>i</u> n: 🗖	tracefiles 🔻 🖬 🗂 🔡 🚍
EMSLogFil	e
Folder <u>n</u> ame:	C:\Users\jdoe\Downloads\Exercise1_2017-05-15_07-00-42\tracefiles
Files of <u>T</u> ype:	All Files 🗸 🗸
	Open Cancel

17. Once all is selected, click **Finish** button.

Collect File Options: Collection Time			
 Absolute Range 			
Select Reference Server Time Zone	Client:(GMT-5:0)E	Eastern Daylight Time-America/Ne	w_York 🔫
From Date/Time	5/15/17 - 7:03 AM		
To Date/Time	5/15/17 - 8:03 AM		
Relative Range			
Files Generated in the last	60	✓ Minutes	•
Download File Options			
Select Partition	Active Partition	-	
Download File Directory	ads\Exercise1_201	7-05-15_07-00-42\tracefiles	Browse
○ Zip Files			
Do Not Zip Files			
Uncompress Log Files			
Delete Collected Log Files from	Server		
Note: The result file can be found in the user specified directory structur	the directory name e.The File Name is	ed ≺Node Name≻ created under as specified by the user.	
< Bacl	K Next >	Finish Cancel	

18. This collects the log files. Wait until you see the confirmation message on RTMT.

🔲 Trace & Log Central	X
 Trace & Log Central Remote Browse Collect Files Query Wizard Schedule Collection Local Browse Real Time Trace Collect Crash Dump Collect Install Logs Audit Logs 	Collect Files in progress for node cwb.cc.lab Downloading results into C:\Users\jdoe\Downloads\Exercise1_2017-05-15_ Completed downloading results intoC:\Users\jdoe\Downloads\Exercise1_ Downloaded files for node cwb.cc.lab Downloaded stdout.log from the node: cwb.cc.lab Downloaded Cisco001MIVR029.log from the node: cwb.cc.lab Downloaded GC.log from the node: cwb.cc.lab

- 19. Navigate to the folder where the traces are saved.
- 20. The Engine logs are all that you need. To find them navigate to \<time stamp>\uccx\log\MIVR folder.

Option 2: Via SSH and SFTP - Recommended Option

- 1. Log in to the VVB server with the Secure Shell (SSH).
- 2. Enter this command in order to collect the logs you need. The logs are compressed and you are prompted to identify SFTP server where the logs are uploaded. file get activelog/uccx/log/MIVR/*
- 3. These logs are stored on the SFTP server path: <IP address>\<date time stamp>\active_nnn.tgz, where nnn is timestamp in long format.

Set Trace and Collect Logs for CUBE and CUSP

CUBE (SIP)

1. Set the logs timestamp and enable the logging buffer.

```
#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
```

Warning: Any change on a production Cisco IOS® software GW can cause an outage.

2. This is a very robust platform that can handle the suggested debugs at the provided call volume without issue. However, Cisco recommends that you:

• Send all logs to a syslog server instead of to the logging buffer.

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

• Apply the debug commands one at a time, and check the CPU utilization after each one.

show proc cpu hist



3. Enable these debugs:

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

- 4. Reproduce the problem.
- 5. Disable the traces.

#undebug all

6. Collect the logs.

term len 0 show ver show run show log

CUSP

1. Turn on SIP traces on CUSP.

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

- 2. Reproduce the problem.
- 3. Turn logging off once you are done.

Collect the Logs

1. Configure a user on the CUSP (for example, test).

2. Add this configuration at the CUSP prompt.

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

- 3. FTP to the CUSP IP address. Use the username (test) and password as defined in the previous step.
- 4. Change directories to /cusp/log/trace.
- 5. Get the log_<filename>.

٩,

Set Trace and Collect UCCE Logs

Cisco recommends to set trace levels and collect traces via Diagnostis Framework Portico or System CLI tools.

Note: For more information about Diagnostic Framework Portico and System CLI, visit the chapter <u>Diagnostic tools</u> in the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1).

When you troubleshoot most of the UCCE scenarios, if the default level of traces does not provide enough information, set the level of traces to 3 in the required components (with some exceptions).

Note: Visit the <u>Trace Level</u> section on the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1) for more information.

For instance, if you troubleshoot Outbound Dialer issues, the level of traces must be set to level 2 if the Dialer is busy.

For CTISVR (CTISVR), level 2 and level 3 do not set the exact registry level recommended by Cisco. The recommended trace registry for CTISVR is 0XF8.

- 1. On the UCCE Agent PG, open the Registry Editor (Regedit).
- 2. Navigate to HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a and b)\EMS\CurrentVersion\library\Processes\ctisvr.

E Registry Editor			
File Edit View Favorites Help			
rile Edit view ravorites Heip V - Cisco Systems, Inc. V - ICM I - 12.5 > - CertMon Cisco SSL Configuration v - citi I - 12.5 v - CG1A > - CG > - DMP v - EMS v - Library	Name (Default) EMSAIILogFilesMax EMSBreakOnExit EMSBreakOnInit EMSDebugBreak EMSDebugBreak EMSDisplayToScreen EMSEnableGlobalExceptionHa EMSForwardLevel EMSGenerateSmallMemoryDu EMSLogFileCountMax EMSLogFileCountMax	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ	Data (value not set) 0x77359400 (200000000) 0x0000000 (0) 0x0000000 (0) 0x0000000 (0) 0x0000000 (0) 0x0000000 (1) 0x00000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x00000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x0000000 (1) 0x00000000000000000000000000000000000
Processes ctisvr nm	EMSLogFileMax EMSNTEventLogLevel	REG_DWORD REG_DWORD REG_DWORD	0x01c9c380 (30000000) 0x00000002 (2) 0x000000f8 (248)

3. Double click the **EMSTraceMask** and set the value to **f8**.

Edit DWOR	RD (32-bit) Value	2
Value name: EMSTraceMask]
Value data: f8	Base Hexadecimal Decimal OK Cancel	1

4. Click **Ok** and close the Registry Editor. These are the steps to set any of the UCCE component traces (the RTR process is used as an example).

SetTrace Level

1. Open the Diagnostic Framework Portico from the server you need to set the traces, and log in as the Administrator user.



2. On the Commands section, navigate to Trace and select SetTraceLevel.



3. On the **SetTraceLevel** window, select the **component** and the **level**.

C Intro://localhost 7/50/ D • S Certific C Outfied ICM/CCE Diagnosti × · ()· Unified ICM/CCE Diagnostic Framework Portico Hostname: 12UCCE-RA.chase.com Address: ::1		
Commands: Alarm SetAlarms GetAlarms Configuration ListConfigurationCategories GetConfigurationCategory Inventory ListAppServers	SetTraceLevel Component: Router A/rtr Level: TraceSettingCookie: Show URL Submit	

4. Click **Submit**. When finished, you see the Ok message.

Hostname: 12UCCE-RA.chase.com Address: ::1		
Commands: Alarm SetAlarms GetAlarms Configuration ListConfigurationCategories GetConfigurationCategory Inventory ListAppServers	SetTraceLevel Component: Level: TraceSettingCookie: Show URL Submit	Router A/rtr
License GetProductLicense	SetTraceLevelReply (OK)	

Warning: Set the level of traces to level 3 while you attempt to reproduce the problem. After the problem is reproduced, set the trace level to default. Use special caution when you set the JTAPIGW traces, since level 2 and level 3 set the Low level traces and this can cause a performance impact. Set level 2 or level 3 in the JTAPIGW during non-production time or in a lab environment.

Log Collection

1. From the Diagnostic Framework Portico, in the **Commands** section, navigate to **Trace** and select **ListTraceFile**.



2. On the ListTraceFile window, select the Component, FromDate, and ToDate. Check the Show URL box, and then, click Submit.

← → @ https://localhost:7890 ♀ ♥ Certific ♥ @ Unified ICM-CCE-CCH Diag ×	\therefore
Unified ICM-CCE-CCH Diagnostic Framework Portico	
Hostname: Sprawler115.PCCEMEA.cisco.com Address: ::1	
Commands: ListTraceFiles	
Alarm SetAlarms Component: Router A/rtr	
GetAlarms FromDate: MM/DD/YYYY 1 /8 /2018 HH:MM:SS 12 :0 Central Standard Tim Configuration AM V -6:00)	ae (UTC
ListČonfigurationCategories GetConfigurationCategory ToDate: MM/DD/YYYY 1 /8 /2018 HH:MM:SS 1 : 30 : 33 Central Standard Tim -6:00)	ne (UTC
Inventory UseTzadjustoff: NO V	
License GetProductLicense	

3. When the request finishes, you see the OK message with the link of the ZIP log file.

CISCO Unified ICM/C Hostname: 12UCCE-RA.cha	CCE Diagnostic Framework Portico
Commands: Alarm SetAlarms GetAlarms Configuration ListConfigurationCategories GetConfigurationCategory Inventory ListAppServers License	ListTraceFiles Component: Router Aver FromDate: MM/DD/YYYY & 17 2002 HH:MM:SS 12 0 0 AM Central Standard Time (UTC -5:00) ToDate: MM/DD/YYYY & 17 2002 HH:MM:SS 12 23 41 PM Central Standard Time (UTC -5:00) UseTzadjustoff: MO Show URL Submit
GetHoouctLicense Log ListLogComponents ListLogFiles Network GetNetStat	ListTraceFilesReply (OK) RouterAIciti] rtr 20220817124205018 4176769.zip Date: Wed Aug 17 2022 00:00: 00 GMT-0500 (Central Daylight Time)

4. Click the **ZIP file link** and **Save** the file in the location you choose.

Set Trace and Collect PCCE Logs

PCCE has its own tool to setup trace levels. It is not applicable to UCCE environment where Diagnostic Framework Portico or system CLI are the preferred ways to enable and collect logs.

1. From the PCCE AW server, open the Unified CCE Web Administration tool and log in to the Administrator account.

Unified CCE Administration
Enter your password
administrator@pcce.com

Sign In
Sign in as a different user

2. Navigate to **Overview > Infrastructure Settings > Log Collection** in order to open the Log Collection page.



3. On the Log Collection page, click **Trace Levels** which opens the **Trace Levels** dialog box.

alialia cisco	Unified Contact Center Enterpri	ise Management	Alerts	
	Log Collection			
Overview	Select Component(s)*	Log Collection Schedule*	End Time	Duration (m
Infrastructure	CCE Finesse	08/17/2022 12:20	08/17/2022 12:50	30 min
٩	CVP	Collect Logs Trace Level	5	

4. Set the Trace Level to **Detailed** on CCE and leave it as **No Change** for CM and CVP, then click **Update Trace Levels**.

Trace Levels		×
Component	Current Level	Set Level To
CCE	Normal	No Change
СМ	Normal	No Change
CVP	Normal	No Change
		Update Trace Levels Cancel

5. Click Yes to acknowledge the Warning.



- 6. After the problem is reproduced, open **Unified CCE Administration** and navigate back to **System >Log Collection**.
- 7. Select **CCE** and **CVP** in the Components pane.
- 8. Select the appropriate Log Collection Time (the default is the last 30 min).
- 9. Click **Collect Logs** and **Yes** to the dialog warning. The log collection starts. Wait a few minutes before it finishes.

Start Time	End Time	Duration	Components	Size	Status	Actions
08/17/2022 12:25	08/17/2022 12:55	30 min	CCE, CVP	1.8 MB	Q	± 0

10. Once finished, click **Download** button in the **Actions** column to download a zipped file with all logs in it. **Save** the **zip file** in any location you find appropriate.

Set Trace and Collect CUIC/Live Data/IDS Logs

Download logs with SSH

- 1. Log in to the SSH Command Line (CLI) of CUIC, LD, and IDS.
- 2. Run the command in order to collect CUIC related logs.

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. Run the command in order to collect LD related logs.

file get activelog livedata/logs/*.*

4. Run the command in order to collect IdS related logs.

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

5. These logs are stored on the SFTP server path: $\langle IP \ address \rangle \langle date \ time \ stamp \rangle \langle active_nnn.tgz$, where nnn is timestamp in long format.

Download Logs with RTMT

- 1. Download RTMT from OAMP page. Log in to https://<HOST ADDRESS>/oamp where HOST ADDRESS is the IP address of the server.
- 2. Navigate to **Tools > RTMT plugin download**. Download and install the plugin.
- 3. Launch RTMT and log in to the server with admin credentials.
- 4. Double click **Trace and Log Central** and then double click **Collect Files**.
- 5. You can see these tabs for the specific services. You must select all services/servers for CUIC, LD, and IDS.

For CUIC:

Colle	ect Files	
S	elect CUIC Services/Applications	
	☑ Select	all Services on all Servers
•	Name	All Servers
Inte	Iligence Center OAMP Service	
Inte	Iligence Center Perfmon Service	
Inte	Iligence Center Reporting Service	×
Inte	Iligence Center SNMP Java Adapter Service	Ľ
Inte	Iligence Center Serviceability Service	

For LD:

Collect Files	
Select LiveData Services/Applications	
🗹 Sele	ct all Services on all Servers
Name	All Servers
CCE Live Data ActiveMQ Service	Ľ
CCE Live Data Cassandra Service	V
CCE Live Data NGINX Service	V
CCE Live Data Socket.IO Service	×
CCE Live Data Storm Services	
CCE Live Data Web Service	K
CCE Live Data Zookeeper Service	

For IDS:

Collect Files

Select IdS Services/Applications	
	Select all Services on all Servers
Name	All Servers
Cisco Identity Service	

For Platform services, it is generally a good idea to select **Tomcat** and **Event** viewer logs:

Collect Files	
Select System Services/Applications	
Selec	t all Services on all Servers
Name	All Servers
Cisco Seniceability Reporter Calléctivities Report	
Cisco Serviceability Reporter DeviceReport	H
Cisco Serviceability Reporter PPRReport	
Cisco Serviceability Reporter ServerReport	
Cisco Serviceability Reporter ServiceReport	
Cisco Stored Procedure Trace	H
Cisco System Arent	H
Cisco Tomcat	
Cisco Tomcat Security Logs	
Cieco Tomcat State Sanlat	
Cisco Trace Collection Service	H
Cisco Trust Varification Service	H
Cisco LIXI Web Senice	H
Cisco Unified Mobile Voice Access Service	
Cisco Unified OS Admin Web Service	H
Cisco Unified OS Platform API	H
Cisco Unified Reporting Web Service	
Cisco User Data Services	
Cisco WebDialer Web Service	H
Cisco WebDialerRedirector Web Service	H H
Cron Lons	
Event Viewer-Application Log	
Event Viewer-System Log	
FIPS Logs	

6. Select the **Date** and **Time** along with the destination folder in order to **Save** the logs.

Packet Capture on VoS (Finesse, CUIC, VVB)

1. Start the Capture

To start the capture, establish a SSH session to the VOS server authenticate with the Platform Administrator account.



1a. Command Syntax

The command is utils network capture and the syntax is as follows:

<#root>

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 - show hosts as dotted IP numeric 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 - the dest addr destination address of the packet as a host name or IPV4 address port - the port number of the packet (either src or dest) num 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. Capture All Traffics

For a typical capture, one can collect ALL packets of ALL sizes from and to ALL address into a capture file called **packets.cap**. To do this simply execute on the admin CLI utils network capture eth0 file packets count 100000 size all



1c. Capture based on Port number

In order to troubleshoot a communications issue with the Cluster Manager, it can be desireable to use the port option to capture based on a specific port (8500).

For more information about which services require communications on each port, refer to the TCP and UDP Port Usage Guidefor the applicable version of the respective component.



1d. Capture based on host

To Troubleshoot an issue with VOS and a particular host, it can be necessary to use the 'host' option to filter for traffic to and from a particular host.

It can also be necessary to exclude a particular host, in this case use a "!" in front of the IP. An example of this would be utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1



3. Reproduce the problem symptom

While the capture has started to reproduce the problem symptom or condition so that the necessary packets are included in the capture. If the problem is intermittent, it can be necessary to run the capture for an extended period. If the capture ends, it is because the buffer is filled. Restart the capture and the previous capture is automatically renamed so the previous capture is not lost. If a capture is needed for an extended period of time, use a monitor session on a switch to capture at the network level.

4. Stop the capture

To stop the capture, hold the **Control** key and press **C** on the keyboard. This causes the capture process to end and no new packets are added to the capture dump.

5.



Once this is complete, a capture file is stored on the server in the location 'activelog platform/cli/' 6. Collect the capture from the server

The capture files are stored in activelog platform/cli/ location on the server. You can transfer the files through CLI to an SFTP server or to the local PC with the RTMT.

4a. Transfer capture file through the CLI to an SFTP server

Use the command file get activelog platform/cli/packets.cap to collect the packets.cap file to the SFTP server. Alternatively, collect all .cap files stored on the server, use file get activelog platform/cli/*.cap. Finally, fill in the SFTP server IP/FQDN, port, username, password, and directory information:

```
- - X
A 14.48.60.75 - PuTTY
login as: Administrator
Administrator@14.48.60.75's password:
Last login: Wed Jun 9 13:39:29 2010 from 172.18.251.22
Command Line Interface is starting up, please wait ...
   Welcome to the Platform Command Line Interface
admin:utils network capture eth0 file packets count 100000 size all host ip 14.48.27.183
Warning: existing packets.cap was renamed packets_6.cap
Executing command with options:
                        count=100000
 size=ALL
                                                interface=eth0
                        dest=
                                                port=
 ip=14.48.27.183
Control-C pressed
admin:file get activelog platform/cli/*.cap
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 7
Total size in Bytes: 658062
Total size in Kbytes: 642.6387
Would you like to proceed [y/n]? y
SFTP server IP: 14.48.27.201
SFTP server port [22]:
User ID: administrator
Password: *******
Download directory: /
Transfer completed.
admin:
```

The CLI indicates success or failure of the file transfer to the SFTP server.

4b. Use RTMT to transfer a capture file to a local PC.

Launch the RTMT. If it is not installed on the local PC, install the appropriate version from the VOS Administration page and then navigate to the **Applications > Plugins** menu. Click **System**, then **Trace & Log Central**, then double click **Collect Files**. Click **Next** through the first menu.

Trace	& Log Central		
Trace I	Log Central		
ummary R row	Step 3		
	lectroes		
	iry Wizard		
-D str	edule Collector		
- 0.00	al Browse		
00 P R4	al Time Trai Collect Files		
-D co	lect Crash		
ervices Co	lect Install Select CCM Services/Applications		
nce Aut	It Logs Select.	all Services on all Servers	
are Loniformer	Name	All Servers	Ccm8pub
the Log mener	Cisco Bulk Provisioning Service		
	Cisco CAR Scheduler		
rat	Cisco CAR Web Service		
og Central	Cisco CDR Agent		
	Cisco CDR Repository Manager		
•	Cisco CDR files on CM server	8	<u> </u>
lever	Cisco CDH files on Publisher Processed	<u> </u>	<u> </u>
	Cisco CTManager	<u> </u>	<u> </u>
	Cisco CTL Provider	8	8
	Cisco Califanaper Cisco Califanaper Cisco ID Phone Senirae	8	H H
	Cisco Californayer Costo P Priore Services	8	
2 •	Cisco Certificate Authority Provy Function	H	H H
	Cisco Change Credential Application	i	ă de la caracteria de la c
	Cisce DHCP Monitor Service		
	Cisco Dialed Number Analyzer	0	
	Cisco Extended Functions		
	Cisco Extended Functions Report		
	Cisco Extension Mobility		
	Cisco Extension Mobility Application		
	Cisco IP Manager Assistant		
	Cisco IP Voice Media Streaming App		
	Cisco License Manager		
	Cisco Messaging Interface		
	Cisco TAP's Service		
	Cisco Listed Mahile Unice Access Depice	- H	8
	Crisco Unified Mobile Voice Access Service	H	8 0
	THE R. P. CO. WHERE STREET STREET, SAMPLE		

In the second menu, choose the checkbox for **Packet Capture Logs** on the server which the capture was performed, then click **Next**.

Select System Services/Applications		
Select all	Services on all Servers	
Name	All Servers	ccm8pub
Cisco WebDialerRedirector Web Service		
Cron Logs		
Event Viewer-Application Log		
Event Viewer-System Log		
Host Resources Agent		
IPT Platform CLI Created Reports		
IPT Platform CLI Logs		
IPT Platform Cert Monitor Logs		
IPT Platform CertMgr Logs		
IPT Platform Cluster Manager Logs		
IPT Platform GUI Logs		
IPT Platform IPSecMgmt Logs		
IPT Platform RemoteSupport Logs		
Install File Signing		
Install and Upgrade Logs		
MIB2 Agent		
Mail Logs		
Mgetty Logs		
NTP Logs		
Netdump Logs		
Packet Capture Logs		
Prog Logs		
SAR Logs		
SNMP Master Agent		
Security Logs		
Service Manager		
Spooler Logs		
System Application Agent		

On the final screen, choose a time range when the capture was performed, and a download directory on the local PC.

llect Files					×
Collect File Options:					
Collection Time					
Absolute Range					
Select Reference Server Time Zon	e Client:(GMT-5:0))Eastern Day	light Time-Ame	erica/New_York	~
From Date/Time	6/9/10 - 1:56 PM				
To Date/Time	6/9/10 - 1:56 PM		-		
Relative Range					
iles Generated in the last	5	•	Hours		•
Developed File Directory				Deserved	
Download File Directory	D:ltraces			Browse	
O Zip Files					
Do Not Zip Files					
Uncompress Log Files					
Delete Collected Log Files from	n Server				
Note: The result file can be found in the user specified directory structure	n the directory nan re.The File Name	ned <node n<br="">is as specifie</node>	ame> created i d by the user.	under	

RTMT closes this window and proceeds to collect the file and store it on the local PC in the specified location.