# Risoluzione dei problemi relativi allo scambio di certificati tra CVP 12.5 e PCCE 12.0

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Sfondo Risoluzione dei problemi Conclusioni Informazioni correlate

## Introduzione

In questo documento viene descritto come risolvere i problemi relativi allo scambio di certificati tra Cisco Customer Voice Portal (CVP) versione 12.5(X) e Cisco Package Contact Center Enterprise (PCCE) versione 12.0(X).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Package Contact Center Enterprise (PCCE) release 12.0
- CVP release 12.5
- Workstation di amministrazione PCCE (AW)
- PCCE Single Pane of Glass (SPOG)

#### Componenti usati

- Cisco Package Contact Center Enterprise (PCCE) release 12.0
- CVP release 12.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Sfondo

PCCE 12.5 supporta l'aggiornamento in più fasi, ovvero è possibile aggiornare CVP alla versione 12.5 mentre PCCE è ancora nella versione 12.0. In questo scenario CVP è stato aggiornato alla

versione 12.5 mentre PCCE rimane nella versione 12.0. Dopo l'aggiornamento quando si accede a SPOG e si tenta di configurare il server di report CVP, viene segnalato un errore che impedisce la comunicazione con il server.

## Risoluzione dei problemi

Passaggio 1. Verificare lo stato del server di report CVP. Passare a Portico diagnostico CVP e verificare che lo stato del sistema di report sia In servizio.

Screenshots G	en	eral	-						
MDS-PCCE-awh	ds0	1a SH-PCCE-c	vpr	pt 🖪 MDS-PCCE-cvp01a	S	H-PO	CE	-cvp01b	
🗲 🕘 🏉 http://lo	calh	ost:8000/cvp/diag		ג-¢ (@ cv	P Di	iagnost	tic F	Frame View 🛛 🗶	
		Serv Mgr. ALL_SS	-	~			~	Refresh	Th
		Level: DEBUG		✓			I.	RPT state: In Service	Ca
STANDARD		INFRA		LEGACY MSG			IJ	System Port Usage: NA	Q Up
ALL:		LOAD_SUBSYSTEM:		MSGLAYER_MESSAGE:		GED			byt Pr
CALL:		THREAD:		MSGLAYER_METHOD:		MSC	Ш	Dump IVR Subsystem   Dump IVR Servicts   Dump RPT   Dump Threads   Reset Stats	
METHOD:		MSG:		MSGLAYER_HANDLED_EXCEPTION:		ICM.		Call Server Version: CVP 12.5(1) Build=325	_
PARAM:		MSG_DETAIL:		MSGLAYER_PARAM:				SIP Stack Version: Caffeine 3.2.1.1 Uptime: 189.47:11	
LOW_LEVEL:		MESSAGE_HANDLING:		GLOBAL_EVENT:				Memory - In use:2070808528 bytes, free:1798070912 bytes Processed at: Fri Mar 20 09:04:56 PDT 2020	
CLASSDUMP:		TIMER:		EXTERNAL_EVENT:					
HEARTBEAT:		STATE:		STATIC_FIELD:					
HANDLED_EXCEPTION:		SECURITY:		EXTERNAL_STATE:			U		
OOOQUEUE:		LICENSING:		INTERNAL_STATE:		]			
GARBAGE_COLLECTOR		STARTUP:		CODE_BRANCH:					
MESSAGE:		SHUTDOWN:		CODE_MARKER:					
RPT_JDBC:		STATS:		CLASS_DUMP:					
RPT_CALL_REG:		SNMP:		LOCAL_DUMP:		]			

Passaggio 2. Controllare lo stato del server CVP sul lato A e sul lato B. Passare al Portico diagnostico CVP e verificare che lo stato dei sottosistemi sia In servizio.

MDS-PCCE-awho	ds0	1a 🖪 SH-PCCE-cv	prp	ot 🖪 MDS-PCCE-cvp01a 🖪	SH	I-PC	CE-cvp01b	
🗧 🔿 🏉 http://sł	n-pc	ce-cvp01b:8000/cvp/dis	ag	, D - C 🥵 CV	P Di	agnost	tic Frame View 😕	
		Serv Mgr: SIP	_	~			Refresh	
		Level: DEBUG		✓			SIP state: In Service Dump SIP State Machine	
STANDARD		INFRA		LEGACY MSG			ICM state: In Service	
L:		LOAD_SUBSYSTEM:		MSGLAYER_MESSAGE:		GED	System Port Usage: TOTAL (3000) AVAIL (3000) IN USE (0)	
L:		THREAD:		MSGLAYER METHOD:	П	MSC	Licensing Migrated to CSSM	
THOD:	П	MSG:	Π	MSGLAYER HANDLED EXCEPTION:	П	ICM	Dump SIP Cells   Dump ICM Cells   Dump ICM Properties   Dump IVR Cells (verbose)	
RAM-		MSG DETAIL	Ē	MSGLAVER PARAM		-	Dump IVR Subsystem   Dump IVR Serviets   Dump RPT   Dump Threads   Reset Stats	
	믐					-	SNAPSHOT	
W_LEVEL:		MESSAGE_HANDLING:		GLOBAL_EVENT:			INBOUND CALLS 0	
ASSDUMP:		TIMER:		EXTERNAL_EVENT:			OUTBOUND CALLS 0	
ARTBEAT:		STATE:		STATIC_FIELD:			RINGTONE CALLS 0	
NOLED EVCERTION		SECURITY-		EVTERNAL CTATE			VIDEO OFFERED 0	
GADLED_EXCEPTION.		SECORTT.		EXTERMAL_STATE.			VIDEO ANSWERED 0	
DOQUEUE:		LICENSING:		INTERNAL_STATE:			GREETING CALLS 0	
ARBAGE_COLLECTOR:		STARTUP:		CODE_BRANCH:			TOTAL CALLS	
ESSAGE:		SHITDOWN		CODE MARKER			SURVEY API DONE 0	
		GHOTDOWN.	-	CODE_INVER.	-	-	SURVEY API FAILED 0	
PT_JDBC:		STATS:		CLASS_DUMP:			TRANSCRIPT API DONE 0	
PT_CALL_REG:		SNMP:		LOCAL_DUMP:			TRANSCRIPT API FAILED 0	
T BATCH		SAF-			_		INBOUND CALLS PER SECOND 0.0	
ukituti		204.				-	Snapshot SIP Stack Dialogs 0	
to:							TOTAL - SINCE STARTUP	
361							New Calls 2	
EBUGIO - DEBUGI41 - DEBUGI40						Connect msgs reved from ICM 4		
						Completed Calls 2		
IAME				LEVEL MASK			Abnormal Disconnects 0	

Passaggio 3. Controllare lo stato del certificato da SPOG.

Elencare il certificato da AW e verificare che il server di report CVP sia stato importato nell'archivio certificati AW.

C:\Program Files (x86)\Java\jre1.8.0\_221\bin>keytool -list -v -keystore ..\lib\security\cacerts Quando viene richiesta la password, digitare changeit.

**Nota:** Se il certificato WSM (Web Service Manager) del server di report CVP non è stato importato nell'archivio certificati AW, seguire le procedure di esportazione e importazione descritte nelle sezioni **Esporta certificati server CVP** e **Importa certificato WSM server CVP** in server ADS in questo documento: <u>PCCE Self-signed Certificate Exchange.</u>

Passaggio 4. Verificare lo stato del certificato dal server di report CVP.

ы ≝ /

Elencare il certificato dal server di report CVP e assicurarsi che il certificato AW sia stato importato nell'archivio certificati del server di report CVP.

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore list -storepass

Quando viene richiesta la password, digitarla in C:\cisco\cvp\conf\Security.properties.

Nota: Se il certificato AW non è stato importato nell'archivio certificati del server di report CVP, seguire le procedure di esportazione e importazione descritte nelle sezioni Esporta certificati server ADS e Importazione dei server ADS nei server CVP e nel server di report nel presente documento: <u>PCCE Self-signed Certificate Exchange.</u>

Passaggio 5. Accertarsi di aver importato i certificati di CVP Reporting Web Service Manager (WSM) in tutti i modelli AW PCCE. Verificare inoltre di aver importato tutti i certificati dei server AW nel server di report CVP.

Passaggio 6. Controllare gli avvisi in SPOG e assicurarsi che i server CVP siano sincronizzati. Passare a Panoramica > Magazzino.



Passaggio 7. Accedere al server di report CVP per verificare che non siano stati segnalati errori. Passare a Panoramica > Configurazione dispositivo > Server di report CVP.

😻 Getting Started 🚥 United Contact Cente 🔟 Cisco United Intellige													
cisco	Unified Contact Cente	r Enterprise Man	agement				Alerta	peceadmin Administrator					
	Device Configuration												
	CVP Server	Device Name	sh-pcce-cvprpt.goctii.con		Call Server Association	0							
Overview	CVP Reporting Server												
	Virtualized Voice Browser	Properties	Database Configuration	Infrastructu	re								
	Finesse												
Infrastructu	Identity Service	Trunk Utilization A Change In value requires a Reporting Server restart Change Enable Reporting Define the maximum size of the file used to record the data feed measages during a DB fall over. Note that this is limited by the amount of free disk space.											
Organization		Maximum File S	iize	(	100	MB Iz							

Passaggio 8. Modificare la configurazione e salvarla. Passare a Panoramica > Configurazione dispositivo > Server di report CVP e fare clic su Salva.

alialia cisco	Unified Contact Center	r Enterprise Management	Alerts	pcceadmin Administrator							
	Device Configu	ration									
Overview	CVP Server CVP Reporting Server	Device Name sh-pcce-cvprpt.goctil.com Call Server Association									
	Virtualized Voice Browser Finesse	Successfully saved									
Infrastructu	Identity Service	ty Service Properties Database Configuration Infrastructure									
Organization		Define the limits for number of threads to be used by the server. Maximum Threads * 523									
Users		Advanced									
Ø		Statistics Aggregation Interval * 20 minutes									

## Conclusioni

- PCCE ES\_37 è richiesto per il funzionamento di PCCE 12.0 con componenti CVP 12.5.
- I certificati dei server di report CVP devono essere scambiati tra CVP Reporting Server e AW.
- Per PCCE 12.0 e CVP 12.5, non è necessario scambiare certificati tra i server CVP (Call Server, VXML Server) e i server AW. Tuttavia, per il trasferimento di applicazioni VXML da SPOG e Smart Licensing, è necessario lo scambio di certificati tra questi server.

#### Informazioni correlate

PCCE Self-signed Certificate Exchange

Guida alla configurazione e all'amministrazione di PCCE

Documentazione e supporto tecnico – Cisco Systems