Gestisci certificato componenti PCCE per SPOG

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Nuova interfaccia utente - SPOG Esportazione certificato SSL AW (Administration Workstation) **Finesse** Cisco ECE CUIC Cisco idS LiveData **VVB** Importazione certificato SSL in keystore CVP Call Server e server di report **Admin Workstation** Finesse, CUIC, Cisco idS e VB Scambio di certificati tra Finesse e CUIC/LiveData

Introduzione

In questo documento viene descritto come scambiare i certificati SSL autofirmati di Admin Workstation (AW) con Customer Voice Portal (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtualized Voice Browser (VB) per Package Contact Center Enterprise (PCCE) Single Pane of Glass (SPOG).

Contributo di Nagarajan Paramasivam e Robert Rogier, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Packaged/Unified Contact Center Enterprise (PCCE/UCCE)
- Piattaforma VOS
- Gestione certificati
- Archivio chiavi dei certificati

Componenti usati

Le informazioni di questo documento si basano sui seguenti componenti:

- Admin Workstation (CEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- Cisco ECE

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.

Premesse

Si consiglia di aver letto e compreso la Guida di amministrazione e configurazione PCCE, in particolare l'appendice di riferimento alla fine che descrive l'impostazione e la configurazione dei certificati. <u>Guida alla configurazione e all'amministrazione di PCCE</u>

Nuova interfaccia utente - SPOG

Packaged CCE 12.0 ha una nuova interfaccia utente conforme ad altre applicazioni per contact center. L'interfaccia utente consente di configurare la soluzione tramite un'unica applicazione. Accedere alla nuova amministrazione di Unified CCE all'indirizzo https://<IP Address>/cceadmin. <Indirizzo IP> è l'indirizzo dell'AW CCE unificato del lato A o B o dell'HDS esterno opzionale.

In questa release, l'interfaccia di amministrazione di Unified CCE consente di configurare quanto segue:

- Campagne
- Cortesia Callback
- Gruppi di server SIP
- Trasferimento file: Il trasferimento di file è possibile solo tramite AW Principal (AW Lato A nell'implementazione di agenti nel 2000 e AW configurato in distribuzioni di agenti 4000 e 12000).
- Modelli di instradamento: Il modello di numero composto in Unified CVP Operations Console è ora denominato modello di routing in Unified CCE Administration.
- Percorsi: In Amministrazione CCE unificata, il codice di routing è ora il prefisso della posizione anziché l'ID del sito.
- Configurazione dispositivo: L'amministrazione CCE unificata consente di configurare i seguenti dispositivi: CVP Server, CVP Reporting Server, VB, Finesse, Identity Service (installazione Single Sign-On).
- Risorse del team: L'amministrazione CCE unificata consente di definire e associare le seguenti risorse per i team di agenti: Variabili Chiamata Layout, Layout Desktop, Rubriche Telefoniche, Flussi Di Lavoro, Motivi (Non Pronto, Disconnetti, Completamento Chiamate).
- E-mail e chat

Prima di gestire il sistema tramite SPOG, è necessario scambiare i certificati SSL tra CVP (Customer Voice Portal), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtual Voice Browser (VB) e Admin Workstation (AW) per stabilire una comunicazione di trust.

Esportazione certificato SSL

AW (Administration Workstation)

Passaggio 1. Accedere all'<u>URL https://localhost</u> nel server AW e scaricare i certificati SSL del server.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

| 4 | Talue | - |
|---|---|------|
| fersken Seriel nunder Signature algorithm | 12 00 e8 45 3x 33 58 & 39 80 #425875A | |
| Sgrature hash algorithm | sha256 | - 14 |
| fald from | 13 April 2018 15-41-20 | |
| unid to: | 10 April 2009 18:40:20 | |
| Ligert | andi-riag-com | 1.0 |
| | Difference Corver | ie |

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

| 1.0 | TerfC + Level (Hard) + Del | | | - 61 | Stands Card |
|-----|--|-----------------|----------------------------|--------|-------------|
| | Sea | Internation | 1 per | line . | |
| | - artist | 294.891.910 | International Constitution | | 344 |
| | and the second s | 10168-3019 1226 | every Cethula | | 189 |

Finesse

Passaggio 1. Accedere alla pagina <u>https://Finesseserver:8443/cmplatform</u> e scaricare il certificato tomcat.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

| 1.00 | | | | and the second |
|------|--|-------------------|------------------------|----------------|
| | here | the extract | Type . | ite . |
| | and the second s | 12-09-2019 (16:09 | Internetly Continuity | 199 |
| ÷ | G 446.cm | 12-04-2010 (0.08 | Security Continues - | 240 |
| No. | C2 PRALIE | 2004-000 Num | Decisity Dettilization | 110 |
| | C2/Md.co. | 0.08.200 0.08 | Include California | 3490 |

Cisco ECE

Passaggio 1. Accedere alla pagina https://ECEWebServer e scaricare il certificato SSL del server.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

| 100 C | | | |
|--------------|---------------------|--------------------|-------|
| Salar | Can well Ad | 7.ett | 104 |
| 12 and on | 2110-0219-0219-0216 | Investigation | 178 |
| The week our | 5-74-201 (128) | Incompliant failes | 110 |
| ig and an | 10.00.0000.0000 | Innaki Carringe | 1198. |
| 121000 | 11-00-0110 75.54 | Sample Lattern | 1.44 |

CUIC

Passaggio 1. Accedere alla pagina <u>https://CUICServer:8443/cmplatform</u> e scaricare il certificato tomcat.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

| | Maria | Interested | ther | 10.0 | |
|--------|--------------|----------------------|------------------------|------|------|
| | C ANALM | 10-06-009 TU/H | Initially Carttly also | | 100 |
| en . | Ca AND or | 10-49-2014 TB/W | Savory Cardinale | | 1148 |
| hini i | CHOK.me | 10 de - primite a 11 | (music Destinate) | | 118 |
| | C# CHURAN | 15-26-2019-06/10 | Incode Cartheren | | 144 |
| | Top Hold and | 10-04-009 Tale: | Security Centilization | | 218 |
| | C2 Webland | 10.46-2019 (1.10) | Samaly Catholies | | 248 |

Cisco idS

Passaggio 1. Accedere alla pagina <u>https://IDSServer:8553/idsadmin/</u> e scaricare il certificato tomcat.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

| 1. de jaris figies 1. de jaris figies 1. de jaris (e. r. | Incomp Earth-an- | 3.48 |
|--|---|---|
| 1.00.00110.00 | Security Calificate Security Cardinate | 3.00 |
| 1.4.2010 | Income Cambooks | 1.00 |
| | | |
| 14-06-2019-00-01 | Secold Labburg | 1.438 |
| 1-6.251 (10.9 | Second Gentlow | 248 |
| Distance includes | Include Cathlands | 0.000 |
| 11-00-00-00-07 | - South Cardione | 248 |
| 19-08-0214-08-07 | Investo Cardinant | 1.08 |
| | 11-00-09-00-07 19-08-00-68-07 | 15.00 (PhD0017) Bacally Cardinals 16.00 (2014)(2017) Bacally Cardinals |

LiveData

Passaggio 1. Accedere alla pagina <u>https://LiveDataServer:8444/cuic/gadget/LiveData/</u> e scaricare il certificato tomcat.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

| | NePC + Gorden für + Get | | 5.04 | (A) [Sectoria |
|------|-------------------------|--------------------|----------------------|------------------------------------|
| | tere * | Des worthan | 1.04 | in |
| | C Arthour | 104-011-028 | Security Entries | 140 |
| h | Contract of the second | 101-061-0018-01-02 | betung Detrives | 3.448 |
| de l | CE CECKINF | 0.44-000.002 | Balany Carthole | 140 |
| | G CHOILine | 15.06.0074.00M | Annually (unifying) | 110 |
| | CI Photos | 10-09-0275-02.04 | Interly Delificate | 198 |
| | C2768.cm | 10.05.275.019 | Security Carthone | 199 |
| | C Chinese | 10-00.011110.01 | Investo Lintellinea | 1.014 |
| | (1) 000uw | 114.249-017 | Industry Continues | 140 |
| | (Linebalan) | 10-05-0233-00107 | Security Certificate | 100 |
| | T21 Conductationary | 43-06-2244-00X2 | Interio Colificate | 140 |

VVB

Passaggio 1. Accedere alla pagina <u>https://VVBServer/appadmin/main</u> e scaricare il certificato tomcat.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

| | the PC + lose the ICs + Cel - | | + | 20 |
|---|-------------------------------|--|----------------------|------|
| | tere | The worked | 144 | he . |
| | THE ADDAMA | 0.04.001110.0 | Terrori, Cardona | 248 |
| ÷ | THE AME OF | 12-08-20-9-12-08 | Incusty-Carebulter | 2.68 |
| | T2-CHCR.ver | 5.0.000.017 | Incode Carolinate | 1.68 |
| | 12 CHOLM | 100 ph-200 million | Investige Carthology | 2.68 |
| | 12 Healing | 10.06-001879-08 | Density Cardions | 148 |
| | California.com | 10-04-000 -0.00 | Density Cariforni | 1.08 |
| | C2 IOSecure | 10.00.00000000 | Taluth Cathline | 1.48 |
| | 12 think | 20-08-0070786-07 | Design Carolinger | 148 |
| | 1210-shrah.or | 10.00-2019 (0.07 | Initial Cardinson | 1487 |
| | To londard on | 100 584 586 987 97 | terring Carefulate | 1.48 |
| | 12 Weiger | 10 D-20191544 | Describe Carthle per | 1481 |
| | C2 Without | (0.00.00000000000000000000000000000000 | Carriedo A produceso | 1.68 |

Importazione certificato SSL in keystore

CVP Call Server e server di report

Passaggio 1. Accedere al server CVP e copiare i certificati AW CCE Admin nella cartella C:\cisco\cvp\conf\security.

| | Tea PC & Local Date (1) & Chair & Cal | a used a secondar | | + 41 | I have been seen |
|-------|---------------------------------------|-------------------|---------------------|------|------------------|
| | fore 1 | December | iter. | 24 | |
| | 13 Heytere | 16-06-009-0-0 | 101103-001 | | 110 |
| 18 | 10 P.M. | 10-28-229-529 | incode Calification | | 2.49 |
| id on | Carlos . | 100000 | Second General | | 1.48 |

Passaggio 2. Passare alla pagina **%CVP_HOME%\conf** e aprire security.properties per copiare la password del keystore.

| | term . | Sale incident | Sec. | 14 | |
|---|----------------------------|---------------|------------------------------|------|--------------------|
| | 2 marts | - | International Vision | | 148 |
| - | Market and a second second | | | | and a start of the |
| | The Lat Average Time Help | | and the second second second | 1000 | |

Passaggio 3. Aprire il prompt dei comandi come amministratore ed eseguire il comando **cd %CVP_HOME%\jre\bin**.



Passaggio 4. Utilizzare questo comando per importare i certificati AW nel server CVP.

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS - alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

Ching of the database in the second design of the second second

Passaggio 5. Quando viene richiesta la password, incollare la password copiata dal file security.properties.

Passaggio 6. Digitare sì per considerare attendibile il certificato e assicurarsi di ottenere il risultato Certificato aggiunto al keystore.



Passaggio 7. Viene visualizzato un messaggio di avvertenza insieme all'importazione completata. Ciò è dovuto al formato proprietario Keystore, è possibile ignorarlo.

Avviso:

II keystore JCEKS utilizza un formato proprietario. È consigliabile eseguire la migrazione a PKCS12, un formato standard del settore che utilizza "keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore - deststoretype pkcs12".

| Are instantion to the second of the second | 10000 |
|--|--------------|
| The JCESS beautions used a prophytic productor, 12 is recommended to sha | with the PR |
| Bill abids in an industry intellers, foreign union, "heaters), "important the | a personal |
| Contrast Conditional Additional Processory High Despitation in the other the period of the Conditional Addition | and constant |

Admin Workstation

Passaggio 1. Accedere al server AW e aprire il prompt dei comandi come amministratore.

Passaggio 2. Passare a C:\Program Files(x86)\Java\jre1.8.0_181\lib\security e verificare che il file cacerts esista.

| | Same - | Ten modial | 1,94 | int. |
|---|---------------------|------------------|--------------|-------|
| | a entry | 10.04.2010.1010 | Rog Automo- | |
| ÷ | - maritie | to be directure. | | 110 |
| - | mainteniture | Think Jone 1978 | 100710-004 | 110 |
| | Ciere 5 | 10.04.004.014 | No. | 114/9 |
| | predday. | 10-04-2010 10-10 | AUGUSTIN . | 140 |
| | and an entropy | 10.04.079.10.16 | DOM: NO | 0.01 |
| | (an every define) | 2148-0111-011 | RILCOM | 0.00 |
| | In stand its arrest | Trial data take | CONTRACTORY. | 1.000 |

Passaggio 3. Digitare il comando cd %JAVA_HOME% e immettere il comando.

| C:>>cd xJAVA_HOM | Đc | |
|------------------|---------------------|-------|
| C:\Program Files | (x86)\Java\jre1.8.8 | 181)_ |

Passaggio 4. Utilizzare questo comando per importare i certificati Finesse nel server AW.

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias <u>fina.nag.com</u>-keystore .\lib\security\cacerts

Conference Films (and class, Sec) 5.8 (in Annual - Ingent Arts ConferenceScience and Anti-Barbana and Second Stations (align film any second prime of the second states)

Passaggio 5. La prima volta che si utilizza questo strumento chiave, **modificare** la password per modificare la password di un archivio certificati.

Passaggio 6. Immettere una nuova password per il keystore e immetterla nuovamente per confermare la password.



Passaggio 7. Digitare **yes** per considerare attendibile il certificato e assicurarsi di ottenere il risultato **Certificato aggiunto al keystore.**

| Irust this | cert | ificate | ? | [no]: | yes |
|-------------|------|---------|----|--------|-----|
| Certificate | was | added | to | keysto | 1.0 |

Nota: Ripetere i passi da 1 a 7 con tutti gli altri nodi Finesse e con tutti i nodi CUIC

Passaggio 8. Se la password del keystore è stata immessa in modo errato o ha eseguito i passaggi senza essere reimpostata, si prevede che venga generata questa eccezione.

Considerare attendibile il certificato? [no]: sì

Il certificato è stato aggiunto al keystore

errore keytool: java.io.FileNotFoundException: .\lib\security\cacerts (impossibile trovare il percorso specificato)

Immettere la password del keystore: errore keytool: java.io.IOException II keystore è stato alterato o la password non è corretta

Passaggio 9. Per modificare la password del keystore, utilizzare questo comando e riavviare la procedura dal passaggio 4 con la nuova password.

keytool -storepasswd -keystore .\lib\security\cacerts

Collegence Files Calli-Liner, juri. 8, 8, 98 (Neyton) - secondported - Asperant - Albi-on perior (second second) by a factor parameter by factor parameter (second)

Passaggio 10. Dopo l'importazione, utilizzare questo comando per visualizzare il certificato dal keystore.

keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com



Finesse, CUIC, Cisco idS e VB

Passaggio 1. Accedere alla pagina di amministrazione del sistema operativo del server Finesse e caricare i certificati SSL AW nel trust Tomcat.

Passaggio 2. Passare a Amministrazione sistema operativo > Protezione > Gestione certificati.

| or the other lands | Provide State | | A. Science and a |
|--------------------|---------------------|--|---------------------------|
| and a state | Alexandra a | | |
| | | | 1.000 |
| The second states | · the later sealers | and a support of the | and a little state of the |
| | 161 110 | and a second sec | 10 100 |
| | 16 I III | 1000 | The little part - |

Passaggio 3. Fare clic su Carica certificato\Catena certificati e selezionare l'opzione Tomcat-trust dall'elenco a discesa.

Passaggio 4. Esplorare l'archivio certificati nell'archivio locale e fare clic su Pulsante Carica.



Passaggio 5. Ripetere i passaggi per caricare tutti i certificati del server AW nel cluster Finesse.

Nota: Non è necessario caricare il certificato tomcat-trust nel nodo secondario, poiché viene replicato automaticamente.

Passaggio 6. Riavviare il servizio Tomcat per rendere effettive le modifiche apportate al certificato.

Passaggio 7. In CUIC, IDS e VVB, seguire i passaggi da 2 a 4 e caricare il certificato AW.

Scambio di certificati tra Finesse e CUIC/LiveData

Passaggio 1. Conservare i certificati Finesse, CUIC e LiveData in una cartella separata.

| | | | | - | |
|----|-------------------|-------------------|---------------------|--------|-------|
| | Tarra . | Determedited | 140 | tine." | |
| | C RACKING | 11-18-27-91-02-51 | Second Contrativ | | 1.00 |
| m | DOM: ++ | 14-10-1279-1217 | Internet Contractor | | 3,488 |
| ** | al Philical | 12-04-22-01-048 | Service Lateras | | 148 |
| | 110.0 | 10.000-0010-0144 | Reading Coldinate | | 1981 |
| | Tal Exceloser-car | 11-08-229-0031 | Security Calificate | | 1.00 |
| | Contradice. | 10.00.000.0001 | Desity Configure | | 1100 |

Passaggio 2. Accedere alla pagina Amministrazione del sistema operativo Finesse, CUIC e LiveData.

Passaggio 3. Passare a Amministrazione sistema operativo > Protezione > Gestione certificati.

Passaggio 4. Fare clic su Carica certificato\Catena certificati e selezionare l'opzione Tomcat-trust dall'elenco a discesa.

Passaggio 5. Esplorare l'archivio certificati nell'archivio locale e selezionare Certificato server come di seguito, quindi fare clic su Pulsante Carica.

In Finesse server - CUIC e LiveData come attendibilità Tomcat

In CUIC Server - Finesse e LiveData come trust tomcat

In LiveData Server - CUIC e Finesse come trust Tomcat

Nota: Non è necessario caricare il certificato tomcat-trust nel nodo secondario, poiché viene replicato automaticamente.

Passaggio 6. Riavviare il servizio Tomcat su ogni nodo per rendere effettive le modifiche al certificato.