中華電信通用憑證管理中心 (Public CA)

IBM Websphere Application Server 8.5 伺服器憑證安裝操作 聲明:本說明文件之智慧財產權為中華電信股份有限公司(以下簡稱本公司)所 有,本公司保留所有權利。本說明文件所敘述的程序係將本公司安裝相關軟體的 經驗分享供申請 SSL伺服軟體憑證用戶參考,若因參考 本說明文件所敘述的程序而起的任何損害,本公司不負任何損害賠償責任。

程式使用版本: IBM Websphere Application Server 8.5

- 一、 下載 eCA 根憑證(ePKI Root CA 憑證,也就是中華電信憑證總管理中心 自簽憑證)與 PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)有以 下兩種方式:
 - 1. eCA : <u>http://epki.com.tw/download/ROOTeCA_64.crt</u> PublicCA : <u>http://publicca.hinet.net/CHTM/download/PublicCA_64.crt</u>
 - 您若是本公司之客戶,技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮 檔,解壓縮後包括三個檔案,分別是 eCA 跟憑證(檔名為 b64.cer)、 PublicCA 中繼憑證 pubcab64.cer 與 xxHDxxxxxxx.crt 是簽發給用戶的 SSL 伺服器軟體憑證,其中 xxHDxxxxxxx 是案件流水號。 若是中華電信之所屬單位,於經審驗核准申請之電子表單資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方可以下載憑證串鏈壓縮 檔。解壓縮後可以進行安裝。
- 二、 開啓 Websphere Integrated Solutions Console,登錄後並開啓 SSL 憑證與 金鑰管理介面。

:/logon.jsp	P → A B C × Ø WebSphere Integrated S ×	
說明(日)		
WebSphere. software		
に に に に に に に の の の に の の の の の の の の の の の の の	WebSphere Integrated Solutions Console 使用者 ID: 空碼: 登入 諸als - Property of IBM © Copyright IBM Corp. 1997, 2011 All Rights H * ibm.com 和 WebSphere 是 International Business Machines Corp. 由田樹根 - 其他產品與服務名稱可能是 IBM 或其他公司的樹根 • IBM 現 ght and trademark information 中取得 •	Reserved. 在全球許多遠 行樹標清單可在
- 歡迎使用 55L ● 引導活動) ● ● 伺服器 ● ● 履服務 ● ● 應用程式 ● ● 夏安全 ● ● 安全 ● ● 安全 ● ● 安全 ● ● 安全 ● ● 安全細域 ● ● 雪濱 ● ● SL 憑證和金寶管理 ● ● 安全審核 ● ● 雪墳 ● ● 東鏡和調整 ● ● 疑難排解 ● ● 服務整合 ●	悲記 基礎和金鑰管理 SL 基礎和金鑰管理 SSL 整置 SSL 整置 SSL 配置 Secure Socket Layer (SSL) 通訊協定提供遠端伺服器程序或端點之間的安全通 訊。SSL 安全可用來建立端點的入埠和出埠通訊。如果要建立安全通訊,必須為端 點指定憑避和 SSL 配置。 在本區的舊版中, 您可以為整個應用程式服務環境定義種一配置。運項功能可讓您 集中管理安全通訊。此外,您可以是強預設的 Cell 層次 SSL 配置,以便在多個節 點環境中建立信任區域。 如果您使用了芬輔公用程式將安全環境移轉至本版, 則會還原各個不同端點的書有 Secure Sockets Layer (SSL) 配置。不過,您必須重新配置 SSL, 才能得到集 中管理功能的好感。 配置設定 管理端點安全配置 管理端點安全配置。 管理 EIPS ② 當發生 SSL 配置裝更時, 動能更新執行時期	相關項目 = <u>SSL 配置</u> = <u>勤監</u> 進導講點 SSL <u>設置</u> = 金讀盤存庫和憑證 = 金讀盤 = 金讀盤 = 金讀童理程式 = 這任管理程式 = 憑證管理中心 (CA) 用戶端配置

三、 點選「金鑰儲存庫和憑證」→先前建立的 keystore→點選右邊的「簽章 者憑證」。

SSL 配置

Secure Socket Layer (SSL) 通訊協定提供遠端伺服器程序或端點之間的安全通 訊。SSL 安全可用來建立端點的入埠和出埠通訊。如果要建立安全通訊,必須為端 點指定憑證和 SSL 配置。

在本產品的舊版中,必須手動為 Secure Sockets Layer (SSL) 配置每一個端 點。但在本版中,您可以為整個應用程式服務環境定義單一配置。這項功能可讓您 集中管理安全通訊。此外,您可以置換預設的 Cell 層次 SSL 配置,以便在多個節 點環境中建立信任區域。

如果您使用了移轉公用程式將安全環境移轉至本版,則會還原各個不同端點的舊有 Secure Sockets Layer (SSL) 配置。不過,您必須重新配置 SSL,才能得到集 中管理功能的好處。

配置設定

管理端點安全配置

管理憑證有效期限

管理 FIPS

📝 當發生 SSL 配置變更時, 動態更新執行時期

套用 重設

Ⅲ 直好設定

新建	∎ 刪除 變更密碼	交換簽章者		
	ē 👾 📽			
選取	名稱 🗘	說明 ☆	管理範圍 ♢	路徑 🗘
您可	以管理下列资源:			
	<u>NodeDefaultKeyStore</u>	CHT- HP49R5ZDNode01 的 預設金鑰儲存庫	(cell):CHT- HP49R5ZDNode01Cell: (node):CHT- HP49R5ZDNode01	\${CONFIG_ROOT}/cells/CHT- HP49R5ZDNode01Cell/nodes/CHT- HP49R5ZDNode01/key.p12
	NodeDefaultTrustStore	CHT- HP49R5ZDNode01 的 預設信任儲存庫	(cell):CHT- HP49R5ZDNode01Cell: (node):CHT- HP49R5ZDNode01	\${CONFIG_ROOT}/cells/CHT- HP49R5ZDNode01Cell/nodes/CHT- HP49R5ZDNode01/trust.p12
	ssikeystore	SSL金鑰儲存庫	(cell):CHT- HP49R5ZDNode01Cell: (node):CHT- HP49R5ZDNode01	D:\sslkeystore.p12
	test		(cell):CHT- HP49R5ZDNode01Cell: (node):CHT- HP49R5ZDNode01	D:\test.p12
總計	4			

相關項目

■ SSL 配置

<u>動態出埠端點 SSL</u> 配置

- < 金鑰儲存庫和憑證
- 金鑰集
- 金鑰集群組
- 金鑰管理程式
- 信任管理程式
- <u>憑證管理中心 (CA)</u> 用戶端配置

<u>SSL 憑證和金鑰管理</u> > <u>金鑰儲存庫和憑證</u> > sslkeystore

定義金鑰儲存庫類型,其中包括加密法、RACF(R)、CMS、Java(TM),以及所有信任儲存庫類型。



安裝 eCA 根憑證與 PublicCA 中繼憑證 四、

點選「新增」

5L 憑證	和金鑰管理			2		
<u>SSL 馮證和金鑰管理</u> > <u>金鑰儲存庫和馮證</u> > <u>sslkeystore</u> > 簽章者馮證						
□ 直(:彌爾什中中的 字設定	蚊半有/颈胆 [。]				
新增	割除 攝取	從埠擷取				
	D # #					
選取	別名 🛟	發證對象 ⇔	指紋(SHA 摘要) ≎	期限 ≎		
您可	以管理下列资源	原:				
	<u>root</u>	CN=CHT- HP49R5ZD.cht.com.tw, OU=Root Certificate, OU=CHT- HP49R5ZDNode01Cell, OU=CHT- HP49R5ZDNode01, O=IBM, C=US	92:38:A8:64:6D:6F:88:37:8D:D9:CC:CC:8A:70:FB:46:E4:97:E8:3E	生效時間 2013/1/31 至 2028/1/28。		
總計	1					

別名:eCA 憑證的名稱

檔名: eCA 憑證位置

填寫完成後,按下確定鍵。

SSL 憑證和金鑰管理
SSL 憑證和金續管理 > 金續儲存庫和憑證 > sslkeystore > 簽章者憑證 > 新增簽章者憑證 將簽章者憑證新增到金鑰儲存庫中。 ──般內容
* 別名 eCA * 檔名
D:\ROOTeCA_64.crt 資料類型
Base64 編碼的 ASCII 資料 ▼ 套用 確定 重設 取消

以相同方法安裝 PublicCA 中繼憑證。

SSL 馮諝和金鑰管理 > 金蘊儲4	存庫和瑪濟 > sslkevstore > 簽章者馮濟 > 新增簽章者馮濟
將簽章者憑證新增到金鑰儲存庫中。	0
一般內容	
● 別名	
PublicCA	
∗ 檔名	
D:\PublicCA_64.crt	
资料類型	
Base64 編碼的 ASCII 資料 ▼	
\sim	
套用 確定 重設 取消	

完成後,將可在以下畫面看到 eCA 與 PublicCA 的憑證資訊。

	eca	OU=ePKI Root Certification Authority, O="Chunghwa Telecom Co., Ltd.", C=TW	67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0	生效時間 2004/12/20 至 2034/12/20。
	<u>opensslroot</u>	CN=RootCARSA/2048, OU=CA, O=Root, L=Taipei, ST=Taiwan, C=TW	AF:3C:CD:E2:08:1F:1D:22:D7:C5:4C:ED:F5:F4:7A:FA:70:4D:E3:EC	生效時間 2013/2/1 至 2033/2/1。
	publicca	OU=Public Certification Authority, O="Chunghwa Telecom Co., Ltd.", C=TW	40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F	生效時間 2007/5/16 至 2027/5/16。
	root	CN=CHT- HP49R5ZD.cht.com.tw, OU=Root Certificate, OU=CHT- HP49R5ZDNode01Cell, OU=CHT- HP49R5ZDNode01, O=IBM, C=US	92:38:A8:64:6D:6F:88:37:8D:D9:CC:CC:8A:70:FB:46:E4:97:E8:3E	生效時間 2013/1/31 至 2028/1/28。
總計	4			

五、 回到上一頁後,點選個人憑證。

一般內容	. 其他內容
名稱 ssikeystore	■ 簽章者馮證 - 個人馮巒
說明 SSL金鑰儲存庫	<u>個人憑證</u> <u>個人憑證要求</u> 自訂內容
管理範圍 (cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01	
路徑 D:\sslkeystore.p12	

點選「從憑證管理中心接收・・・」

SSL 憑證和金鑰管理					?
<u>SSL 憑證和金論管理</u> > á	<u> </u>	eystore > 個人憑證			
管理個人憑證。					
■ 喜好設定					
建立 - 刪除 《從	憑證管理中心接收	取代 擷取 匯	〔入 匯出 撒》	肖 更	新
選取	別名	發證對象	發證者	序號	期限
無					
總計 0					

填入個人憑證位置後,按下「確定」鍵。

SSL 憑證和金鑰管理
<u>SSL 憑證和金鑰管理 > 金鑰儲存庫和憑證 > sslkeystore</u> > 個人憑證 > 從 CA 接收憑證
從憑證管理中心 (CA) 接收您的個人憑證,以取代與憑證要求中的公開/私密金鑰相關且儲存在金鑰儲存庫中的暫時憑 證。
一般內容
D:\certreq3.crt
資料類型
Base64 編碼的 ASCII 资料 ▼
[套用 [確定] 重設 取消

若跟憑證、中繼憑證、個人憑證皆有效的情況下,系統會自動將憑證串列建立起來。

(下圖以 OpenSSL 的自簽憑證當 root CA 簽發 SSL 憑證給 www.test.com.tw。)

<u>SSL 憑證和金鑰管理</u> > <u>金鑰儲存庫和憑證</u> > <u>sslkeystore</u> > 個人憑證

管理個人憑證。

Ⅲ 喜好設定	
--------	--

建立 🔹 🔜除	從憑證管理中心接收	取代 擷取 [匯入 匯出 撤消	更新
選取 別名	發證對象	發證者	序號	期限
您可以管理下列资源:				
₽ 93	CN=www.test.com.tw, OU=政府網路處, O=中華 電信股份有限公司數據分 公司, ST=台北市, C=TW	CN=RootCARSA/2048, OU=CA, O=Root, L=Taipei, ST=Taiwan, C=TW	11780414117550831359	生效時間 2013/2/18 至 2033/2/18。
ţ	CN=RootCARSA/2048, OU=CA, O=Root, L=Taipei, ST=Taiwan, C=TW	CN=RootCARSA/2048, OU=CA, O=Root, L=Taipei, ST=Taiwan, C=TW	15285965834589358770	生效時間 2013/2/1 至 2033/2/1。
總計 2				

六、 回到 SSL 憑證和金鑰管理,接著點選「SSL 配置」

CI (1	EE ≥	സ്ച്ന	-A-9	÷ i	ing i	Ħ
SL ;	221	료11니	盂	兩	티니	Ξ

SSL 憑證和金鑰管理

SSL 配置

Secure Socket Layer (SSL) 通訊協定提供遠端伺服器程序或端點之間的安全通 訊。SSL 安全可用來建立端點的入埠和出埠通訊。如果要建立安全通訊,必須為端 點指定憑證和 SSL 配置。 相關項目

SSL 配置

■ <u>金鑰集</u>

金鑰集群組

金鑰管理程式

<u>信任管理程式</u>

用戶端配置

<u>動態出埠端點 SSL</u> 配置

<u> 憑證管理中心 (CA)</u>

金鑰儲存庫和憑證

在本產品的舊版中,必須手動為 Secure Sockets Layer (SSL) 配置每一個端 點。但在本版中,您可以為整個應用程式服務環境定義單一配置。這項功能可讓您 集中管理安全通訊。此外,您可以置換預設的 Cell 層次 SSL 配置,以便在多個節 點環境中建立信任區域。

如果您使用了移轉公用程式將安全環境移轉至本版,則會還原各個不同端點的舊有 Secure Sockets Layer (SSL) 配置。不過,您必須重新配置 SSL,才能得到集 中管理功能的好處。

配置設定

<u>管理端點安全配置</u> 管理憑證有效期限

管理 FIPS

點選「新建」。

新建						
選取	名稱 ◆	管理範圍 ☆				
您可以管理下列資源:						
	<u>NodeDefaultSSLSettings</u>	(cell):CHT-HP49R5ZDNode01Cell:(node):CHT- HP49R5ZDNode01				
	<u>test</u>	(cell):CHT-HP49R5ZDNode01Cell:(node):CHT- HP49R5ZDNode01				
總計	2					

依序填入「名稱」,下拉式選擇之前有建立 SSL 憑證的儲存庫,按下「取得 憑證別名」,確認資訊無誤後,方可按下「確定鍵」鍵。

SSL 憑證和金鑰管理		
<u>SSL 憑證和金<mark>續管理</mark> > <u>SSL 配置</u> > 新建</u> 定義 Secure Socket Layer (SSL) 配置清單。		
<u>一般內容</u>		
名棋 SSL		
信任健友庫名稱 sslkeystore(cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01)	•	
金鑰儲存庫名稱 sslkeystore ()cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01)	-	取得憑證別名
預設伺服器憑證別名 ssl3 ▼		
預設用戶端憑證別名 ssl3 ▼		
管理範圍 (cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01	•	
· 套用 (確定) 重設 取消		
點選「儲存」。		

	∃ 記息	
	⚠ 已對你的大端配置做了變更。您可以:	
	 直接儲存至主要配置中。 	
	● 在儲存或捨棄之前, <mark>檢閱</mark> 變更。	
	🕰 伺服器可能需要重新啟動,這些變更才能生效。	
I		

七、 最後點選「管理端點安全配置」

SSL 憑證和金鑰管理

SSL 配置

Secure Socket Layer (SSL) 通訊協定提供遠端伺服器程序或端點之間的安全通 訊。SSL 安全可用來建立端點的入埠和出埠通訊。如果要建立安全通訊,必須為端 點指定憑證和 SSL 配置。

在本產品的舊版中,必須手動為 Secure Sockets Layer (SSL) 配置每一個端點。但在本版中,您可以為整個應用程式服務環境定義單一配置。這項功能可讓您 集中管理安全通訊。此外,您可以置換預設的 Cell 層次 SSL 配置,以便在多個節 點環境中建立信任區域。

如果您使用了移轉公用程式將安全環境移轉至本版,則會還原各個不同端點的舊有 Secure Sockets Layer (SSL) 配置。不過,您必須重新配置 SSL,才能得到集 中管理功能的好處。

я	issi.	TĒ	F
Ħ	177	거見	Ħ

1

- = <u>SSL 配置</u>
- <u>動態出埠端點 SSL</u>
- 配置
- <u>金鑰儲存庫和憑證</u>
- <u>金鑰集</u>
- <u>金鑰集群組</u>
- 金鑰管理程式
- <u>信任管理程式</u>
- <u> 憑證管理中心 (CA)</u>
 <u> 用戶端配置</u>



管理 FIPS

📝 當發生 SSL 配置變更時, 動態更新執行時期

對需要的入埠與出埠做設定。



以入埠為例,下拉式選單選擇剛剛在 SSL 配置完成的名稱,之後按下「更新憑證別名清單」,最後按下「確定」。

<u>SSL 憑證和金鑰管理</u> > <u>管理端點安全配置</u> > CHT-HP49R5ZDNode01

顯示所選範圍(如 Cell、節點、伺服器或叢集)的 Secure Socket Layer (SSL) 配置。



□ 訊息
▲ 已對你的杰端配置做了變更。您可以:
▲ 直接儲存至主要配置中。
● 在儲存或捨棄之前, <u>檢閱</u> 變更。
⚠ 伺服器可能需要重新啟動,這些變更才能生效。

八、 到此為止,已完成 SSL 憑證之安裝與設定,可以嘗試以「https」的方 式瀏覽網頁,確認 SSL 憑證已經安裝成功。