SSL 證書 - Covalent

證書安裝指南

webnic
accelerate your business

請選擇您的版本

Covalent Apache ERS v2.4（或以下）SSL 安裝指南

Covalent Apache ERS v3.0 （或以上）SSL 安裝指南

Covalent Apache ERS v2.4（或以下）SSL 安裝指南

步驟 1：下載最新 Intermediate CA 證書

1. 通過此鏈接下載 Intermediate CA 證書。

   選擇和你的 SSL 證書適合的 **Intermediate CA** 證書。

2. 複製 Intermediate CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 intermediate.crt。

3. 此文件可以和 SSL 證書儲存於相同的目錄。如：**/usr/local/ssl/crt**

步驟 2：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。

2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

   證書正文的例子：

   -----BEGIN CERTIFICATE-----

   [加密數據]

   -----END CERTIFICATE-----

3. 根據 Apache 的命名規定，把證書以**.crt** 格式儲存。例：**public.crt**。

4. 在收到已簽名的 SSL 證書，把證書儲存至臨時的目錄。

5. 從 **Covalent SSL Certificate and Key Management Tool** 選擇 **Install CA Signed Certificate**。你將被提示儲存著證書的臨時目錄路徑。 Covalent SSL 將安裝該證書。

   - 簽名證書將會儲存在目錄 **/path/to/ssl1.5/certs**。證書的名稱與臨時證書一致，yourserver.domain.cert （例：www.covalent.net.cert）。

注：為證書簽名的程序並不會對私鑰造成任何影響。

此程序是必要的。

- 私鑰將儲存在目錄 **/path/to/ssl15/keys**。名稱是 yourserver.domain.key（例：www.covalent.net.key）。

6. 在你的網站的 Virtual Host 設定，在 **httpd.conf** 文件裡，你需要加入以下 SSL 指令：

SSLCACertificateFile/path/to/ssl1.5//intermediate.crt

注：此指令說明了 Intermediate CA 證書的儲存路徑，如果你使用其他的儲存路徑或文件名稱，你需要更改指令裡的路徑或文件名稱。

7. 如果你的主機在運行中，執行以下指令終止主機：**/path/to/apache1.3/bin/covalent-faststart-ctl stop**
8. 然後執行以下指令重啟主機：**/path/to/apache1.3/bin/covalent-faststart-ctl startssl**
9. 在重啟主機時，系統將會提示輸入證書的密碼。
10. 把已簽名的證書和其私鑰進行備份。
11. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

Covalent Apache ERS v3.0 （或以上）SSL 安裝指南

觀看線上演示

http://www.symantec.com/tv/products/details.jsp?vid=1452855338001

步驟 1：下載 Intermediate CA 證書

1. 通過此鏈接下載 Intermediate CA 證書。

   選擇和你的 SSL 證書適合的 Intermediate CA 證書。

2. 複製 Intermediate CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 **intermediate.crt**。

3. 此文件可以和 SSL 證書儲存於相同的目錄。如：**/usr/local/ssl/crt**

步驟 2：安裝 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。

2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

   證書正文的例子：

   -----BEGIN CERTIFICATE-----

   [加密數據]

   -----END CERTIFICATE-----

3. 根據 Apache 的命名規定，把證書以.crt 格式儲存。例：public.crt。
4. 把證書儲存至持有證書的目錄。例：/usr/local/ssl/crt/.

步驟 3：設置主機

注：在一些情況，Apache 會同時包含 httpd.conf 和 ssl.conf 文件。請根據以下指令輸入或修改 httpd.conf 或 ssl.conf。不要同時輸入 httpd.conf 和 ssl.conf 文件，這會造成系統衝突進而令 Apache 無法啟動。

1. httpd.conf 或 ssl.conf 必須更新以便使用對稱密鑰。
2. 在 httpd.conf 或 ssl.conf 的虛擬主機部分，確認在虛擬主機裡包含以下指令。

如果沒有請加入以下指令：

SSLCertificateFile /usr/local/ssl/crt/public.crt

SSLCertificateKeyFile /usr/local/ssl/private/private.key

SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt

注：一些 Apache 的版本可能不接受 SSLCertificateChainFile 的指令，請使用 SSLCACertificateChainFile。

例如：

```
#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile /usr/local/ssl/crt/public.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /usr/local/ssl/private/private.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt
```

注：第一個指令命令 Apache 如何找到證書文件，第二個指令命令 Apache 如何找到密鑰，第三個指令則是中間證書頒發機構的位置。如果你使用和上述例子中不同的目錄和文件名稱，你需要更改指令中的路徑和文件名。

3. 保存您的 **httpd.conf** 或 **ssl.conf** 文件並重新啟動 Apache。你可以通過以下 **apachectl** 腳本進行：

   apachectl stop

   apachectl startssl

4. 您現在應該可以在您的 Apache-SSL 主機使用 SSL 證書。

5. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。