SSL 证书 - Covalent

证书安装指南

webnic
accelerate your business

请选择您的版本

Covalent Apache ERS v2.4（或以下）SSL 安装指南

Covalent Apache ERS v3.0 （或以上）SSL 安装指南

Covalent Apache ERS v2.4（或以下）SSL 安装指南

步骤 1：下载最新 Intermediate CA 证书

1. 通过此链接下载 Intermediate CA 证书。

   选择和你的 SSL 证书适合的 Intermediate CA 证书。

2. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.crt。

3. 此文件可以和 SSL 证书储存于相同的目录。如：/usr/local/ssl/crt

步骤 2：获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。

2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

   证书正文的例子：

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

   [加密数据]

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

3. 根据 Apache 的命名规定，把证书以.crt 格式储存。例：public.crt。

4. 在收到已签名的 SSL 证书，把证书储存至临时的目录。

5. 从 Covalent SSL Certificate and Key Management Tool 选择 Install CA Signed Certificate。你将被提示储存着证书的临时目录路径。Covalent SSL 将安装该证书。

   - 签名证书将会储存在目录 /path/to/ssl1.5/certs。证书的名称与临时证书一致，yourserver.domain.cert （例：www.covalent.net.cert）。

注：为证书签名的程序并不会对私钥造成任何影响。

此程序是必要的。

- 私钥将储存在目录 /path/to/ssl15/keys。名称是 yourserver.domain.key（例：www.covalent.net.key）。

6. 在你的网站的 Virtual Host 设定，在 **httpd.conf** 文件里，你需要加入以下 SSL 指令：

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

注：此指令说明了 Intermediate CA 证书的储存路径，如果你使用其他的储存路径或文件名称，你需要更改指令里的路径或文件名称。

7. 如果你的主机在运行中，执行以下指令终止主机：**/path/to/apache1.3/bin/covalent-faststart-ctl stop**
8. 然后执行以下指令重启主机：**/path/to/apache1.3/bin/covalent-faststart-ctl startssl**
9. 在重启主机时，系统将会提示输入证书的密码。
10. 把已签名的证书和其私钥进行备份。
11. 要检验您的证书是否已正确安装，请使用 Symantec 的证书检查工具。

Covalent Apache ERS v3.0 （或以上）SSL 安装指南

观看线上演示

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

步骤 1：下载 Intermediate CA 证书

4. 通过此链接下载 Intermediate CA 证书。

   选择和你的 SSL 证书适合的 Intermediate CA 证书。

5. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.crt。

6. 此文件可以和 SSL 证书储存于相同的目录。如：/usr/local/ssl/crt

步骤 2：安装 SSL 证书

12. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。

13. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

    证书正文的例子：

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

    [加密数据]

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

14. 根据 Apache 的命名规定，把证书以.crt 格式储存。例：public.crt。

15. 把证书储存至持有证书的目录。例：/usr/local/ssl/crt/.

步骤 3：设置主机

注：在一些情况，Apache 会同时包含 httpd.conf 和 ssl.conf 文件。请根据以下指令输入或修改 httpd.conf 或 ssl.conf。不要同时输入 httpd.conf 和 ssl.conf 文件，这会造成系统冲突进而令 Apache 无法启动。

1. httpd.conf 或 ssl.conf 必须更新以便使用对称密钥。
2. 在 httpd.conf 或 ssl.conf 的虚拟主机部分，确认在虚拟主机里包含以下指令。

   如果没有请加入以下指令：

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

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

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

   注意：一些 Apache 的版本可能不接受 SSLCertificateChainFile 的指令，请使用 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
```

注意：第一个指令命令 Apache 如何找到证书文件，第二个指令命令 Apache 如何找到密钥，第三个指令则是中间证书颁发机构的位置。如果你使用和上述例子中不同的目录和文件名称，你需要更改指令中的路径和文件名。

3. 保存您的 httpd.conf 或 ssl.conf 文件并重新启动 Apache。你可以通过以下 apachectl 脚本进行：

   apachectl stop

   apachectl startssl

4. 您现在应该可以在您的 Apache-SSL 主机使用 SSL 证书。

5. 要检验您的证书是否已正确安装，请使用 Symantec 的证书检查工具。