

apache + mod_ssl

Carlos Bacelar

Criptografia
DIUM

2008

Software

Distribuições e Documentação disponível nos *web sites*:

- Servidor *http* Apache
www.apache.org
- *OpenSSL* toolkit
www.openssl.org
- Módulo SSL para Apache: *mod_ssl*
www.modssl.org

Configuração do Servidor

Directivas de configuração:

- `SSLEngine on`: activação do módulo SSL;
- `SSLCertificateFile`; `SSLCertificateKeyFile`: localização do certificado e chave do servidor;
- `SSLCertificateChainFile`: cadeia do certificado do servidor;
- `SSLCACertificateFile`: localização da CA para os certificados dos clientes;
- `SSLCipherSuite`: escolha das cifras admitidas para negociação (lista verificável com “`openssl ciphers`”);

```
SSLCipherSuite HIGH:MEDIUM
```

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

Configuração: Directorias

- SSLRequireSSL: obriga acesso por https;
- SSLVerifyClient require: requer certificado do cliente (autenticação mútua...)
- SSLVerifyDepth: tamanho máximo da cadeia de certificado do cliente;

- Exemplo:

```
<Location /cademo>  
SSLRequireSSL  
SSLVerifyClient require  
SSLVerifyDepth 2  
</Location>
```

Controlo de acesso

- SSLRequire: especifica requisitos para acesso...
- Exemplo:

```
<Location /cademo/sec>  
SSLRequireSSL  
SSLVerifyClient require  
SSLVerifyDepth 3  
SSLRequire (  %{SSL_CLIENT_S_DN_CN} eq "User2" \  
              and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20 \  
              ) or %{SSL_CLIENT_S_DN_CN} eq "SuperUser" \  
  
</Location>
```

Certificados

- **Servidor:** deve conter o nome do *site* (*Fully Qualified Domain Name*) no campo DN/CN
 - ① gerar chaves (`openssl genrsa ...`);
 - ② gerar pedido de certificado (`openssl req -new ...`);
 - ③ assinar certificado (`./sign.sh ...`);
- **Cliente:** deve ser inserido no *browser* para este o fornecer no estabelecimento de ligação SSL.
 - Passo que envolve a criação de um ficheiro PKCS12 contendo o certificado do utilizador, a chave, e a cadeia de certificação
 - `openssl pkcs12 ...` (ver guião das TPs)

Ficheiro de configuração

```
<VirtualHost _default_:443>
DocumentRoot "/sw/var/apache2/htdocs"
AddHandler cgi-script .cgi
ServerName localhost:443
SSLEngine on
SSLCipherSuite HIGH:MEDIUM
SSLCertificateFile /sw/etc/apache2/ssl.crt/server.crt
SSLCertificateKeyFile /sw/etc/apache2/ssl.key/server.key
SSLCertificateChainFile /sw/etc/apache2/ssl.crt/ca.crt
SSLCACertificateFile /sw/etc/apache2/ssl.crt/ca.crt

<Location />
Options +ExecCGI
SSLRequireSSL
</Location>
<Location /cademo>
...
</Location>
<Location /cademo/sec>
...
</Location>
</VirtualHost>
```

Demo

- https sem autenticação do cliente:
`https://localhost/printenv.cgi`
- autenticação do cliente
`https://localhost/cademo/printenv.cgi`
- controlo de acesso restrito
`https://localhost/cademo/sec/printenv.cgi`