CAcert svn setup notes

Author: Jan Dittberner <jandd@cacert.org>
Version: 0.2
Date: 2011-04-27

Contents

Initial setup

- install using lxc-setup

```
sudo ./lxc-setup -n svn -l 8G -i 10.0.0.20 -r `pwgen -s 32 -n 1` \
  -a svn-admin@cacert.org
sudo lxc-start -n svn -f /etc/lxc/svn.conf -d
```

- adduser jandd
- adduser jandd sudo
- ssh-copy-id for jandd via forwarded connection from host
- `apt-get install aptitude`
- install additional packages: libapache2-svn, subversion, apache2-mpm-worker, openssl, wget
- edit /etc/ssh/sshd_config to disable non-key and root logins
- invoke-rc.d ssh restart
- echo "10.0.0.20 svn svn.intra.cacert.org" >> /etc/hosts

Configuration of Apache virtual hosts

svn.cacert.org:80

- HTTP
- read only
- no authentication
- no access to restricted areas

- server name: svn.cacert.org
- aliases: nocert.svn.cacert.org, cert.svn.cacert.org
- modified default virtual host

```
<VirtualHost 10.0.0.20:80>
        ServerName svn.cacert.org
        ServerAlias nocert.svn.cacert.org
        ServerAdmin svn-admin@cacert.org

        <Location />
                Dav svn
                SVNPath "/srv/svnrepo"
                Order deny,allow
                Allow from all

             #   AuthType basic
             #   AuthName           "CAcert.org Subversion repository"
             #   AuthUserFile       "/srv/dav_svn.passwd"

                AuthzSVNAccessFile  "/srv/dav_svn.authz"
        </Location>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/nocert-access.log combined
</VirtualHost>
```

svn.cacert.org:443

- HTTPS
- writeable
- client certificate authentication
- server name: svn.cacert.org
- alias: cert.svn.cacert.org
- `/etc/apache2/sites-available/cert.svn.cacert.org`

```
<IfModule mod_ssl.c>
<VirtualHost 10.0.0.20:443>
        ServerName svn.cacert.org
        ServerAlias cert.svn.cacert.org
        ServerAdmin svn-admin@cacert.org

        SSLEngine on
        SSLCertificateFile      /etc/apache2/ssl/svn.cacert.org.crt.pem
        SSLCertificateKeyFile   /etc/apache2/ssl/svn.cacert.org.key.pem
        SSLCertificateChainFile /etc/apache2/ssl/cacert-chain.pem
```

```
        SSLCACertificateFile    /etc/apache2/ssl/cacert-certs.pem
        SSLVerifyDepth          3
        SSLVerifyClient         require
        SSLUserName             SSL_CLIENT_S_DN_Email_0

        <Location />
                Dav svn
                SVNPath "/srv/svnrepo"
                Order deny,allow
                Allow from all

                AuthzSVNAccessFile  "/srv/dav_svn.authz"
        </Location>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/cert-ssl-access.log combined

        BrowserMatch "MSIE [2-6]" \
                nokeepalive ssl-unclean-shutdown \
                downgrade-1.0 force-response-1.0
        # MSIE 7 and newer should be able to use keepalive
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
</IfModule>
```

nocert.svn.cacert.org:443

- HTTPS
- writeable
- username/password authentication
- server name: nocert.svn.cacert.org
- `/etc/apache2/sites-available/nocert.svn.cacert.org`

```
<IfModule mod_ssl.c>
<VirtualHost 10.0.0.20:443>
        ServerName nocert.svn.cacert.org
        ServerAdmin svn-admin@cacert.org

        SSLEngine on
        SSLCertificateFile      /etc/apache2/ssl/svn.cacert.org.crt.pem
        SSLCertificateKeyFile   /etc/apache2/ssl/svn.cacert.org.key.pem
        SSLCertificateChainFile /etc/apache2/ssl/cacert-chain.pem

        <Location />
                Dav svn
```

```
                SVNPath "/srv/svnrepo"
                Order deny,allow
                Allow from all

                AuthType basic
                AuthName            "CAcert.org Subversion repository"
                AuthUserFile        "/srv/dav_svn.passwd"

                AuthzSVNAccessFile  "/srv/dav_svn.authz"
                Satisfy Any
                Require valid-user
        </Location>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/nocert-ssl-access.log combined

        BrowserMatch "MSIE [2-6]" \
                nokeepalive ssl-unclean-shutdown \
                downgrade-1.0 force-response-1.0
        # MSIE 7 and newer should be able to use keepalive
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
</IfModule>
```

other Apache changes

- enable new virtual hosts:

```
a2ensite cert.svn.cacert.org
a2ensite nocert.svn.cacert.org
```

- enable required Apache modules

```
a2enmod ssl
a2enmod dav_svn
```

- create certificate directories and files

```
mkdir /etc/apache2/ssl
wget -O - http://www.cacert.org/certs/root.crt \
  > /etc/apache2/ssl/cacert-chain.pem
wget -O - http://www.cacert.org/certs/root.crt \
  http://www.cacert.org/certs/class3.crt \
  > /etc/apache2/ssl/cacert-certs.pem
```

Backup/Restore SVN repository

- create svn repository

```
svnadmin create /srv/svnrepo
```

- execute backup.sh on old svn host using a long random passphrase

```
#!/bin/sh
umask 077

BACKUPDIR=/var/tmp/backup-$(date +'%Y%m%d-%H%M%S')
mkdir "$BACKUPDIR"
cd "$BACKUPDIR"

svnadmin hotcopy /root/svnrepo svnrepo
svnadmin -q dump svnrepo | \
  gzip > svnrepo-r$(svnlook youngest svnrepo).svndump.gz

svnlook youngest svnrepo > revision.txt

rm -rf svnrepo
cp /etc/apache2/dav_svn.passwd /etc/apache2/dav_svn.authz .
cp /etc/apache2/server.cert /etc/apache2/server.key .
export GNUPGHOME=/tmp/backupgpg
mkdir "$GNUPGHOME"
umask 022
tar c . | gpg --symmetric > "$BACKUPDIR.tar.gpg"
rm -rf "$GNUPGHOME" "$BACKUPDIR"

echo "backup is in $BACKUPDIR.tar.gpg"
```

- copy encrypted backup data to new svn host
- restore backup using restore-backup.sh using the same long random passphrase

```
#!/bin/bash

if [ ! -f "$1" ]; then
  echo "usage: $0 backupfile.tar.gpg"
  exit 1
fi

BACKUPFILE=$(pwd)/$1
RESTOREDIR=${BACKUPFILE%%.tar.gpg}

umask 077
mkdir ${RESTOREDIR}
cd ${RESTOREDIR}

gpg "${BACKUPFILE}" | tar x

# restore revisions
zcat svnrepo-r$(cat revision.txt).svndump.gz | svnadmin load /srv/svnrepo
```

```
install --mode=0640 --owner=root --group=www-data dav_svn.authz /srv/
install --mode=0640 --owner=root --group=www-data dav_svn.passwd /srv/
install --mode=0640 --owner=root --group=www-data server.cert \
  /etc/apache2/ssl/svn.cacert.org.crt.pem
install --mode=0600 --owner=root --group=root server.key \
  /etc/apache2/ssl/svn.cacert.org.key.pem
chown -R www-data.www-data /srv/svnrepo
```

Final touch

- check Apache configuration

```
apache2ctl configtest
```

- restart Apache

```
apache2ctl restart
```

- add special ferm rules on host in /etc/ferm/ferm.d/svn.conf

```
# -*- shell-script -*-
&CONTAINER_NAT("svn", 172.16.2.15, 10.0.0.20);
&CONTAINER_IN("svn", tcp, (http https));
```