xCAT Web Interface How-To

version 0.1

Min Jun Xi/China/IBM
minjun.xi@cn.ibm.com
10 / 8 / 10, 11:34:31 AM

1 The requirements to xCAT web interface

The xCAT web interface requires the following packages installed on the management node (short as MN):
1) IBM HTTP Server (on AIX)
2) Apache2 HTTP Server (on Linux)
3) xCAT-web-dep (only on AIX)
4) apache2-mod_php5 and php5 (only on SUSE)
5) php (only on Redhat)
6) xCAT
7) xCAT-UI

The information for downloading xCAT and xCAT-UI packages can be accessed from xCAT website: http://xcat.sf.net. If you are using xCAT to manage your cluster, you should know how to get and install the xCAT and xCAT-UI packages.

IBM HTTP Server V6.1 or higher is required, which can be downloaded from the "IBM HTTP Server" web site. IBM HTTP Server is based on the Apache HTTP Server, developed by the Apache Software Foundation. There're many third-party modules written for Apache 2.0 that can be used for IBM HTTP Server. IBM HTTP Server is available for use free of charge but without IBM support. It's not packaged into the *xCAT-web-dep* rpm package because of the underlying legal issues.

The AIX platform lacks of many packages for PHP support, so the package "*xCAT-web-dep*" is created to include all the possible packages for PHP support. Besides, the PHP rpm package is also included into the *xCAT-web-dep* package.

In order to support php, we also have to install several rpm packages on Linux. However, they are different on RHEL and SLES. On RHEL, "*php*" is used to support php; but on SLES, "*apache2-mod_php5*" and "*php5*" are used to support php.

1.1 Install the IBM HTTP Server (only for AIX)

After the "IBM HTTP Server for AIX" (Version 6.1.0.0 is preferred) package is downloaded from the "IBM HTTP Server" web site, you can unzip it and get the directory named "IHS_6.1.0.0". Then, please follow the install guide in the directory "**IHS_6.1.0.0/IHS/docs**".

1.2 Install the xCAT-web-dep rpm package (only for AIX)

From the web page "Browse Files for xCAT on sourceforge.net", you can find the xCAT-web-dep package under "**xcat-dep**" => "**2.x_AIX**". The current build is xcat-web-dep-2.3-200907141002.tar.gz.

You can unzip this tar ball, and get the directory named "*xcat-web-dep*", which contains all the xCAT-UI dependencies. In the directory, you can find the README file, and several rpm packages to be installed.

1.3 Install the php-related rpm package (only on Linux)

The php-related rpm packages have different names on Redhat and SuSE. You have to handle these two distributions separately.

1.3.1 Install "php" on RHELS5.x

Note: The following command should also work on Fedora.

```
yum install php
```

1.3.2 Install "apache2-mod_php5"and "php5" on SLES11

Note: The followding command should also work on SLES 10.x and OpenSuSE.

```
yum install apache2-mod_php5 php5
```

1.4 Install the xCAT-UI rpm package

The *xCAT-UI* rpm package can be found on the website http://xcat.sourceforge.net, you can use the "rpm -ivh" command to install xCAT-UI.

```
rpm -ivh xCAT-UI
```
Note: If the php-related rpm packages are not installed as chapter 1.3 describes, the installation of xCAT-UI will be failed.

1.5 The default account for xCAT web interface

During the installation of xCAT-UI rpm package, the encrypted password of the system "root" user has been put into the xCAT *passwd* database. You can use the following command to have a check:

```
tabdump passwd
```
You should see at least one line, which contains the account information for the web interface. On SLES, you can see that the account information locates in the 4th line, which starts with "*xcat*".

```
#key,username,password,comments,disable
"system","root","cluster",,
"omapi","xcat_key","MXBzOExuQUo0QlFrZWJtbVFWVzl4OEdYT0ExQTF1cFA=",,
"xcat","root","$2a$10$FBaEMr4J5jZ6092.4B6bdutgezyo3lmN1UrYoxrYAIlRSvWl5HJya",,
```

1.6 Enable "https" protocol for xCAT web interface

1.6.1 Redhat

The https protocol is enabled by default on RHEL, Fedora. You don't need to configure it manually.

1.6.2 SuSE

There's one document "Apache Howto SSL" on OpenSuSE's website, the same procedure works for SLES.

1. Make sure that apache starts with mod_ssl loaded.

    ```
    a2enmod ssl
    ```
2. Enable the SSL configuration for apache2

    ```
    a2enflag SSL
    ```

3. Create self signed keys

```
/usr/bin/gensslcert
```

4. Create a virtual host

```
cp /etc/apache2/vhosts.d/vhost-ssl.template  /etc/apache2/vhosts.d/vhost-
ssl.conf
```

5. Restart apache2 service

```
/etc/init.d/apache2 restart
```

1.6.3 AIX

There are two Technotes "Guide to properly setting up SSL within the IBM HTTP Server" and "Using the Key Management Utility"on IBM HTTP Server website.

1. Create the database.

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -create -db <filename>.kdb -pw
 <password>  -type cms -expire  <days> -stash
```

2. Create a self-signed certificate.

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -create -db <dB_name>.kdb -pw
 <password> -size <1024 | 512> -dn<distinguished name> -label <label>
 -default_cert <yes or no>
```

Note: -label: Enter a descriptive comment used to identify the key and certificate in the database.
    -dn: Enter an X.500 distinguished name. This is input as a quoted string of the following format (Only CN, O, and C are required): CN=common_name, O=organization, OU=organization_unit, L=location, ST=state, province, C=country
    Example: "CN=weblinux.raleigh.com,O=temp,OU=temp,L=RTP,ST=NC,C=US"

3. Configure the httpd.conf to create a virtual host.

```
Listen 443
Keyfile "/usr/IBM/HTTPServer/temp/XXX.kdb"
<VirtualHost  *:443>
SSLEnable
SSLClientAuth None
SSLV2Timeout   100
SSLV3Timeout   5000
</VirtualHost>
SSLDisable
```

4. Restart IBM HTTP Server

```
apachectl -k restart
```

1.6.4 Make sure "https://" works for your browser

Point your browser (Firefox, Chrome, or Safari) to *https://<ip>/xcat* , to see whether "https://" works or not.

One more thing, because the SSL certificate is self-signed, you may meet the warning message in your 1st time to isit your HTTP server by "https://" protocol. The warning message shows "**The certificate for this website is invalid**", or "**The site's certificate is not-trusted**", or some other similar warnings, which depends on your web browser.

For such a situation, please feel free to import the certificate into your browser, and the warning message won't show again.

1.7 Preferred Internet Browsers

Due to some compatibility issue, Internet Explorer is not permitted to access the xCAT web interface. Mozilla Firefox, Google Chrome and Apple Safari can be used to access the xCAT web interface.

2 The future

TODO