VCL 2.3 Installation

Install & Configure:

Install & Configure the Database

1. ### Download & Extract the Apache VCL Source
   a. If you have not already done so, download and the Apache VCL source to the database server:

   wget --trust-server-names ''

   b. Extract the files:

   tar -jxvf apache-VCL-2.3.tar.bz2

2. ### Install MySQL Server
   a. Install MySQL Server 5.x:

   yum install mysql-server -y

   b. Configure the MySQL daemon (mysqld) to start automatically:

   /sbin/chkconfig --level 345 mysqld on

   c. Start the MySQL daemon:

   /sbin/service mysqld start

   d. If the iptables firewall is being used and the web server and management nodes will be on different machines, port 3306 should be opend up

   vi /etc/sysconfig/iptables

   ```
   -A RH-Firewall-1-INPUT -m state --state NEW -s <web server IP> -p tcp --dport 3306 -j ACCEPT
   -A RH-Firewall-1-INPUT -m state --state NEW -s <management node IP> -p tcp --dport 3306 -j ACCEPT
   service iptables restart
   ```

3. ### Create the VCL Database
   a. Run the MySQL command-line client:

   mysql

   b. Create a database:

   CREATE DATABASE vcl;

   c. Create a user with SELECT, INSERT, UPDATE, DELETE, and CREATE TEMPORARY TABLES privileges on the database you just created:

   GRANT SELECT,INSERT,UPDATE,DELETE,CREATE TEMPORARY TABLES ON vcl.* TO '**vcluser**'@'localhost' IDENTIFIED BY '**vcluserpassword**';

Replace **vcluser** and **vcluserpassword** with that of the user you want to use to connect to the database

The GRANT command will automatically create the user if it doesn't already exist

d. Exit the MySQL command-line client:

```
exit
```

e. Import the vcl.sql file into the database:

```
mysql vcl < apache-VCL-2.3/mysql/vcl.sql
```

The **vcl.sql** file is included in the **mysql** directory within the Apache VCL source code

---

Next step: VCL 2.3 Web Code Installation

Install & Configure the Web Components

Prerequisites

The following instructions assume these tasks have previously been completed:

- Apache VCL 2.3 has been downloaded
- VCL database has been installed and configured

Web Server:

- Apache HTTP Server v1.3 or v2.x with SSL enabled
- PHP 5.0 or later

The VCL web frontend may run under other web server platforms capable of running PHP code, but has only been tested to work with Apache HTTP Server.

Required Linux Packages:

- **httpd** - Apache HTTP Server
- **mod_ssl** - SSL/TLS module for the Apache HTTP server
- **php** - The PHP HTML-embedded scripting language
- **libmcrypt** - Encryption algorithms library (this requirement can be removed with a patch)

Required PHP Modules:

- **php-gd**
- **php-json** (required if your PHP version is 5.2 or later)
- **php-mysql**
- **php-openssl**
- **php-sysvsem**
- **php-xml**
- **php-xmlrpc**
- **php-ldap** (if you will be using LDAP authentication)
- **php-process** (for RHEL/CentOS 6)

1. ## Install the Required Linux Packages & PHP Modules
   a. If your web server is running a Red Hat-based OS, the required components can be installed with:
   For RHEL / CentOS 5

yum install httpd mod_ssl php php-gd php-mysql php-xml php-xmlrpc php-ldap -y

For RHEL / CentOS 6

yum install httpd mod_ssl php php-gd php-mysql php-xml php-xmlrpc php-ldap php-process -y

You may need the optional server rpm repository for the php-process package to add this run the following command:
rhn-channel --add --channel=rhel-x86_64-server-optional-6

b. Configure the web server daemon (httpd) to start automatically:

/sbin/chkconfig --level 345 httpd on

c. Start the web server daemon:

/sbin/service httpd start

d. If SELinux is enabled, run the following command to allow the web server to connect to the database:

/usr/sbin/setsebool -P httpd_can_network_connect=1

e. If the iptables firewall is being used, port 80 and 443 should be opened up:

vi /etc/sysconfig/iptables

```
-A RH-Firewall-1-INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
```

service iptables restart

2. Install the VCL Frontend Web Code

a. If you have not already done so, download and extract the source files on the web server:

wget --trust-server-names ''
tar -jxvf apache-VCL-2.3.tar.bz2

b. Copy the **web** directory to a location under the web root of your web server and navigate to the destination **.ht-inc** subdirectory:

cp -r apache-VCL-2.3/web/ /var/www/html/vcl
cd /var/www/html/vcl/.ht-inc

c. Copy **secrets-default.php** to **secrets.php**:

cp secrets-default.php secrets.php

d. Edit the **secrets.php** file:

vi secrets.php

- Set the following variables to match your database configuration:
  - **$vclhost**
  - **$vcldb**
  - **$vclusername**

        - **$vclpassword**
    - Create random passwords for the following variables:
        - **$cryptkey**
        - **$pemkey**
    - Save the secrets.php file
e. Run the **genkeys.sh**

```
./genkeys.sh
```

f. Copy **conf-default.php** to **conf.php**:

```
cp conf-default.php conf.php
```

g. Modify **conf.php** to match your site

```
vi conf.php
```

> Modify every entry under **"Things in this section must be modified"**. Descriptions and pointers for each value are included within conf.php.

    - **COOKIEDOMAIN** - set this to the domain name your web server is using or leave it blank if you are only accessing the web server by its IP address

h. Set the owner of the **.ht-inc/maintenance** directory to the web server user (normally 'apache'):

```
chown apache maintenance
```

i. Open the **testsetup.php** page in a web browser:
    - If you set up your site to be https://my.server.org/vcl/ open https://my.server.org/vcl/testsetup.php
    - Debug any issues reported by testsetup.php

3. Log In to the VCL Website

a. Open the index.php page in your browser (https://my.server.org/vcl/index.php)
    - Select **Local Account**
    - Username: **admin**
    - Password: **adminVc1passw0rd**
b. Set the admin user password (optional):
    i. Click **User Preferences**
    ii. Enter the current password: **adminVc1passw0rd**
    iii. Enter a new password
    iv. Click **Submit Changes**

4. Add a Management Node to the Database

a. Click the **Management Nodes** link
    i. Click **Add**
    ii. Fill in these required fields:
        - **Hostname -** The name of the management node server. This value doesn't necessarily need to be a name registered in DNS nor does it need to be the value displayed by the Linux *hostname* command. For example, if you are installing all of the VCL components on the same machine you can set this value to *localhost*.

> Take note of the value you enter for Hostname. In a later step performed during the management node installation, the value enter for Hostname must match the value you enter for FQDN in the /etc/vcl/vcld.conf file on the management node.

        - **IP address** - the public IP address of the management node
        - **SysAdmin Email Address** - error emails will be sent to this address
        - **Install Path** - this is parent directory under which image files will be stored - only required if doing bare metal installs or using VMWare with local disks
        - **End Node SSH Identity Key Files** - enter /etc/vcl/vcl.key unless you know you are using a different SSH identity key file
    iii. Optionally, fill in these fields:
        - **Address for Shadow Emails** - End users are sent various emails about the status of their reservations. If this field is configured, copies of all of those emails will be sent to this address.
        - **Public NIC configuration method** - this defaults to Dynamic DHCP - if DHCP is not available for the public interface of your nodes, you can set this to Static. Then, the IP configuration on the nodes will be manually set using Public Netmask, Public Gateway, Public DNS Server, and the IP address set for the computer under Manage Computers
b. Click **Confirm Management Node**
c. Click **Submit**

d. Click the **Management Nodes** link
    i. Select **Edit Management Node Grouping**
    ii. Click **Submit**
    iii. Select the checkbox for your management node
    iv. Click **Submit Changes**

5. Install & Configure phpMyAdmin (Optional):
   phpMyAdmin is a free and optional tool which allows MySQL to be administered using a web browser. It makes administering the VCL database easier. This tool can be installed on the VCL web server. To install phpMyAdmin, follow the instructions on: VCL 2.3 phpMyAdmin Installation & Configuration

Further steps if using only VMWare

Further steps if using xCAT

Previous Step: VCL 2.3 Database Installation
Next Step: VCL 2.3 Management Node Installation

Install & Configure the Management Node Components

Prerequisites

The following management node installation instructions assume the instructions on the following pages have previously been completed:

- VCL 2.3 Database Installation
- VCL 2.3 Web Code Installation

Supported Operating Systems:

The VCL management node daemon (vcld) has been developed to run on an operating system based on Red Hat Enterprise Linux (RHEL). It has been tested on the following:

- Red Hat Enterprise Linux 4.x
- Red Hat Enterprise Linux 5.x
- Red Hat Enterprise Linux 6.x
- CentOS 5.x
- CentOS 6.x

Required Linux Packages:

The VCL management node daemon (vcld) requires the following Linux packages and Perl modules in order to run (see step 2 below for installation instructions):

- **expat** - A library for parsing XML
- **expat-devel** - Libraries and include files to develop XML applications with expat
- **gcc** - Various compilers (C, C++, Objective-C, Java, ...)
- **krb5-libs** - The shared libraries used by Kerberos 5
- **krb5-devel** - Development files needed to compile Kerberos 5 programs
- **libxml2** - Library providing XML and HTML support
- **libxml2-devel** - Libraries, includes, etc. to develop XML and HTML applications
- **mysql** - MySQL client programs and shared libraries
- **nmap** - Network exploration tool and security scanner
- **openssh** - The OpenSSH implementation of SSH protocol versions 1 and 2
- **openssl** - The OpenSSL toolkit
- **openssl-devel** - Files for development of applications which will use OpenSSL
- **perl** - The Perl programming language
- **perl-DBD-MySQL** - A MySQL interface for perl
- **xmlsec1-openssl** - OpenSSL crypto plugin for XML Security Library

Required Perl Modules:

The VCL management node daemon (vcld) is written in Perl and has been tested on Perl 5.8.x. The following Perl modules available from CPAN are also required (see step 2 below for installation instructions):

- **DBI** - Generic Database Interface
- **Digest::SHA1** - NIST SHA message digest algorithm
- **Mail::Mailer** - Simple mail agent interface
- **Object::InsideOut** - Comprehensive inside-out object support
- **RPC::XML** - A set of classes for core data, message and XML handling
- **YAML** - YAML Ain't Markup Language

1. Install the VCL Management Node Code - Perl Daemon

a. If you have not already done so, download and extract the VCL source files to the management node:

```
wget --trust-server-names 'http://vcl.apache.org/downloads/download.cgi?action=download&filename=%2Fvcl%2Fapache-VCL-2.3.tar.bz2'
tar -jxvf apache-VCL-2.3.tar.bz2
```

b. Copy the **managementnode** directory to the location where you want it to reside (typically **/usr/local**):

```
cp -r apache-VCL-2.3/managementnode /usr/local/vcl
```

2. Install the Required Linux Packages & Perl Modules

Run the install_perl_libs.pl script:

```
perl /usr/local/vcl/bin/install_perl_libs.pl
```

The last line of the install_perl_libs.pl script output should be:

```
COMPLETE: installed all components
```

Note: The script will hang or terminate if it encounters a problem. If this occurs, you will need to troubleshoot the problem by looking at the output.

The install_perl_libs.pl script included in the VCL distribution will attempt to download and install the required Linux packages and Perl modules. It uses the yum utility to install the required Linux packages. The required Perl modules are available from CPAN - The Comprehensive Perl Archive Network. The install_perl_libs.pl script attempts to download and install the required Perl modules by using the CPAN.pm module which is included with most Perl distributions.

The yum utility should exist on any modern Red Hat-based Linux distribution (Red Hat, CentOS, Fedora, etc). If yum isn't available on your management node OS, you will need to download and install the required Linux packages manually or by using another package management utility. After installing the required Linux packages, attempt to run the install_perl_libs.pl script again.

3. Configure vcld.conf

a. Create the **/etc/vcl** directory:

```
mkdir /etc/vcl
```

b. Copy the stock **vcld.conf** file to **/etc/vcl**:

```
cp /usr/local/vcl/etc/vcl/vcld.conf /etc/vcl
```

c. Edit **/etc/vcl/vcld.conf**:

```
vi /etc/vcl/vcld.conf
```

The following lines must be configured in order to start the VCL daemon (vcld) and allow it to check in to the database:

- **FQDN** - the fully qualified name of the management node, this should match the name that was configured for the management node in the database
- **server** - the IP address or FQDN of the database server
- **LockerWrtUser** - database user account with write privileges
- **wrtPass** - database user password
- **xmlrpc_pass** - password for xmlrpc api from vcld to the web interface(can be long). This will be used later to sync the database vclsystem user account
- **xmlrpc_url** - URL for xmlrpc api https://my.server.org/vcl/index.php?mode=xmlrpccall

d. Save the vcld.conf file

4. Configure the SSH Client

The SSH client on the management node should be configured to prevent SSH processes spawned by the root user to the computers it controls from hanging because of missing or different entries in the known_hosts file.

Edit the ssh_config file:

```
vi /etc/ssh/ssh_config
```

Set the following parameters:

```
UserKnownHostsFile /dev/null
StrictHostKeyChecking no
```

Note: If you do not want these settings applied universally on the management node the SSH configuration can also be configured to only apply these settings to certain hosts or only for the root user. Consult the SSH documentation for more information.

5. Install and Start the VCL Daemon (vcld) Service
   a. Copy the vcld service script to /etc/init.d and name it vcld:

      cp /usr/local/vcl/bin/S99vcld.linux /etc/init.d/vcld

   b. Add the vcld service using chkconfig:

      /sbin/chkconfig --add vcld

   c. Configure the vcld service to automatically run at runtime levels 3-5:

      /sbin/chkconfig --level 345 vcld on

   d. Start the vcld service:

      /sbin/service vcld start

      You should see output similar to the following:

      ```
      Starting vcld daemon:
                                                          [  OK  ]
      ```

      The vcld service can also be started by running the service script directly: **/etc/init.d/vcld start**

   e. Check the vcld service by monitoring the vcld.log file:

      tail -f /var/log/vcld.log

      You should see the following being added to the log file every few seconds if the management node is checking in with the database:
      2012-05-15 13:23:45|25494|vcld:main(167)|lastcheckin time updated for management node 1: 2012-05-15 13:23:45

      The vcld -v (verbose) flag is needed in order to see the check-in message.

6. Set the vclsystem account password for xmlrpc api

Using the vcld -setup tool, set the vclsystem account. This is needed to properly use the block allocation features.

/usr/local/vcl/bin/vcld -setup

Select 1. VCL Base Module
Select 2. Set Local VCL User Account Password
Select 2. vclsystem
From the vcld.conf file, paste or type the password from xmlrpc_pass variable and hit enter.

7. Install & Configure the DHCP Service
   a. Install **dhcp** if it is not already installed:

      yum install dhcp -y

   b. Configure the dhcpd service to automatically start at runlevels 3-5:

/sbin/chkconfig --level 345 dhcpd on

c. Configure the dhcpd.conf file.

vi /etc/dhcpd.conf

Configure your dhcpd.conf file according to your network configuration. The contents of the dhcpd.conf file will vary based on how your network is configured. Below is an example of a basic dhcpd.conf file:

```
ddns-update-style none;
shared-network eth0 {
        subnet 10.100.0.0 netmask 255.255.255.0 {
                ignore unknown-clients;
        }
}
```

You will add host definitions to the dhcpd.conf file after you add computers to VCL using the website. The website will display the dhcpd.conf host definitions after the computers have been added to VCL, which can be copied and pasted into the dhcpd.conf file.

d. Start the dhcpd service:

/sbin/service dhcpd start

8. ## Configure Windows Product Keys and/or KMS Server Addresses (Optional)

If you will be deploying Windows environments your institution's Windows product key and/or KMS server addresses must be entered into the VCL database. This can be done by running the following command:

/usr/local/vcl/bin/vcld -setup

Select "**Windows OS Module**" and follow the prompts.

9. ## Download Windows Sysprep Utility (Optional)

If you will be using VCL to deploy bare-metal Windows XP or Windows Server 2003 environments via xCAT, the appropriate versions of the Microsoft Sysprep utility must be downloaded to the management node. The following steps do not need to be completed if you only intend to deploy VMware virtual machines.

The Sysprep utility is included in the Deployment Tools available for free from Microsoft. You do not need to download Sysprep for Windows 7 or Windows Server 2008 because it is included in the operating system.

The Sysprep files need to be downloaded, extracted, and then copied to the management node. The format of the file available for download is Microsoft's .cab format. It is easiest to extract the files on a Windows computer. Windows Explorer is able to open the .cab file and then the files contained within can be copied elsewhere.

a. Windows XP
   i. Download Sysprep for Windows XP: Windows XP Service Pack 3 Deployment Tools
   ii. Extract the Windows XP Sysprep Files
   iii. Copy the extracted Windows XP Sysprep files to the following directory the management node:

```
/usr/local/vcl/tools/Windows_XP/Utilities/Sysprep
```

b. Windows Server 2003
   i. Download Sysprep for Windows Server 2003: System Preparation tool for Windows Server 2003 Service Pack 2 Deployment
   ii. Extract the Windows Server 2003 Sysprep Files
   iii. Copy the extracted Windows Server 2003 Sysprep files to the following directory the management node:

```
/usr/local/vcl/tools/Windows_Server_2003/Utilities/Sysprep
```

10. ## Download Windows Drivers (Optional)

Drivers which aren't included with Windows must be downloaded and saved to the management node. The drivers required will vary greatly depending on the hardware. The only way to know what additional drivers you need is to install Windows on a computer and check for missing drivers.

The drivers must be copied to the appropriate directory on the management node. The VCL image capture process copies the driver directories to the computer before an image is captured. Drivers from multiple directories will be copied based on the version of Windows being captured. There

are driver directories under **tools** for each version of Windows (Windows XP, Windows 7) and for each version group of Windows (version 5, 6). This allows drivers which are common to multiple versions of Windows to be shared in the management node tools directory structure. Examples:

If a chipset driver works for all versions of Windows it should be saved in:
/var/lib/vcl/tools/Windows/Drivers/Chipset

If Windows XP and Windows Server 2003 both use the same network driver it can be saved in:
/var/lib/vcl/tools/Windows_Version_5/Drivers/Network

If a storage driver only works for Windows XP it should be saved in:
/var/lib/vcl/tools/Windows_XP/Drivers/Storage

During the image capture process, each Windows version directory is copied to the computer under C:\Cygwin\home\root\VCL. The order in which the Windows version directories are copied goes from most general to most specific. In the example above, the order would be:
/var/lib/vcl/tools/Windows/*
/var/lib/vcl/tools/Windows_Version_5/*
/var/lib/vcl/tools/Windows_XP/*

The following list shows which driver files should be saved in the driver directories:
/var/lib/vcl/tools/Windows/Drivers - drivers common to all versions of Windows
/var/lib/vcl/tools/Windows_Version_5/Drivers - drivers used by Windows XP and Server 2003
/var/lib/vcl/tools/Windows_XP/Drivers - drivers only used by Windows XP
/var/lib/vcl/tools/Windows_Server_2003/Drivers - drivers only used by Windows Server 2003
/var/lib/vcl/tools/Windows_Version_6/Drivers - drivers used by Windows Vista and Server 2008
/var/lib/vcl/tools/Windows_7/Drivers - drivers only used by Windows 7
/var/lib/vcl/tools/Windows_Server_2008/Drivers - drivers only used by Windows Server 2008
The directory structure under each Drivers directory does not matter. It is helpful to organize each directory by driver class, and each directory should be organized using the same theme. For example:
/var/lib/vcl/tools/Windows_Version_XP/Drivers/Chipset
/var/lib/vcl/tools/Windows_Version_XP/Drivers/Network
/var/lib/vcl/tools/Windows_Version_XP/Drivers/Storage
/var/lib/vcl/tools/Windows_Version_XP/Drivers/Video

11. ## Install & Configure Provisioning Engines and Hypervisors

VCL supports the following, please see the related websites for installation and configuration instructions:

a. xCAT - Extreme Cluster Administration Toolkit
   - Versions Supported:
     - 1.3
     - 2.x
   - See the xCAT website for installation & configuration information: http://xcat.sourceforge.net

b. VMware
   i. See the VMware website for installation & configuration information: http://www.vmware.com
   ii. See the following pages for additional VCL VMware configuration information:
      1. VMware Configuration
      2. VCL 2.3 - Further steps if using only VMware (you probably already did things from this page when installing the web code)

Previous Step: VCL 2.3 Web Code Installation
Next Step: VCL 2.3 Configure Frontend Authentication

Configure Frontend Authentication

Adding Local VCL Accounts

Local VCL accounts are contained within the VCL database. The **admin** account is a local VCL account. Additional local accounts can be added via the backend management node code. After you have finished the backend management node installation, run:

```
vcld -setup
```

1. Select **VCL Base Module**
2. Select **Add Local VCL User Account**
3. Enter the requested information

Adding LDAP Authenciation

Prerequisites for your LDAP server:

- SSL should be enabled on your LDAP server
- An LDAP account that can look up a user's first and last names, user id, and email address (email address is optional) - this will be referred to as 'vcllookup' on this page. You can skip this step if anonymous binds are enabled on your LDAP server and an anonymous bind will be able to look up userids, names, and email addresses.
- If your LDAP server is behind a firewall, you will need to allow your VCL web server to access tcp port 636 on your LDAP server

Prerequisites for your VCL web server:

- **php-ldap** needs to be installed
- If your LDAP server's SSL certificate is self-signed, your VCL web server needs to have the root CA certificate that was used to sign the LDAP server certificate installed. The PEM formatted certificate needs to be added to the ca-bundle.crt file. On CentOS, the file is located at /etc/pki/tls /certs/ca-bundle.crt. The hostname in the certificate must match the hostname entered in the conf.php file further down. If your certificate does not have the correct hostname in it, you can put an entry in /etc/hosts for the hostname in the certificate.
- After adding the certificate, restart httpd:

  service httpd restart

- You can verify that the certificate is properly installed using this command:

  openssl s_client -showcerts -CAfile /etc/pki/tls/certs/ca-bundle.crt -connect your.ldap.server.here:636

  If you see "Verify return code: 0 (ok)" at the end of the output then it is installed correctly. If you see a different return code, then you'll need to troubleshoot the problem.
- You may need to add a line to **/etc/openldap/ldap.conf** to point to the ca-bundle.crt file. If so, add the following:

```
TLS_CACERT /etc/pki/tls/certs/ca-bundle.crt
```

Adding LDAP Authentication to the Web Code

- You will need to manually add an entry to the affiliation table in the VCL database. Choose a name for the affiliation. This will be appended to all userids for the affiliation to distinguish them from other affiliations you may configure later. **Do not** use the Global affiliation for this. Initials or a short name of your organization are a good idea. The affiliation name cannot contain spaces. Use the following to add the affiliation, replacing 'EXAMPLE' with the name you chose. Take note of the id from the 2nd SQL statement as you will need it later. It is the numerical id for this affiliation.

  mysql vcl

  INSERT INTO affiliation (name) VALUES ('EXAMPLE');

  SELECT id FROM affiliation WHERE name = 'EXAMPLE';

  exit

- Edit **conf.php** and search for "EXAMPLE1 LDAP"
- Uncomment the "EXAMPLE1 LDAP" section by removing the '/*' before it and the '*/' at the end of 'to use this login mechanism'
- Change 'EXAMPLE1 LDAP' to something to match your location, for example at NCSU, it is 'NCSU LDAP'. This string is what users will see where they select the authentication mechanism to use when logging in.
- Modify the following fields:
  - **server** - this is the hostname of your LDAP server - this must match the hostname in the certificate.
  - **binddn** - typically, you'll want to use the base DN of your LDAP server; for Active Directory, this is usually dc= for each of your domain name components. For example, your your domain name was ad.example.org, it would be "dc=ad,dc=example,dc=org"
  - **userid** - this is a string that is added to the userid a user enters on the login page. Place a '%s' where the entered userid should go. Some examples are:
    - %s@example.org
    - %s@ad.example.org
    - uid=%s,ou=accounts,dc=example,dc=org'
  - **unityid** - this is the ldap field that contains a user's login id (for Active Directory, this is usually sAMAccountName)
  - **firstname** - this is the ldap field that contains a user's first name
  - **lastname** - this is the ldap field that contains a user's last name
  - **email** - this is the ldap field that contains a user's email address
  - **defaultemail** - if an email address is not provided by the ldap server, this will be appended to the end of the userid to create an email address. In this case, email notifications will be disabled by default.

    - **masterlogin** - this is the vcllookup account referred to in the "Prerequisites for your LDAP server" section - comment out this line if using anonymous binds
    - **masterpwd** - password for the masterlogin account - comment out this line if using anonymous binds
    - **affiliationid** - this is the id from the SELECT statement in the first step
    - **lookupuserbeforeauth** - Some LDAP servers will only allow the full DN of a user to be used when authenticating. If this is the case, you will need to set this to 1 and set a value for **lookupuserfield**. You can probably start out with this set to 0. If your LDAP server has users in multiple containers, you will probably need to set this to 1.
    - **lookupuserfield** - If you need to set **lookupuserbeforeauth** to 1, set this to the attribute to use to search for the user in ldap. Typical values are 'cn', 'uid', and 'samaccountname'.
    - **help** - this is some text that will show up on the page where users select the authentication method explaining why they would select this option
- Uncomment the **require_once** line for **ldapauth.php** toward the bottom of the file