Linux Academy

Live! Lab

# Use LDAP Credentials for Single Sign On

# Contents



## Lab Connection Information

- Labs may take up to five minutes to build
- The IP address of your server is located on the Live! Lab page
- Username: linuxacademy
- Password: 123456
- Root Password: 123456

### *Related Courses*

*Linux Academy Red Hat Certified Systems Administrator Prep*

### *Related Videos*

*Configure a System to Use an Existing Authentication Service*

### *Need Help?*

*Linux Academy Community*

*... and you can always send in a support ticket on our website to talk to an instructor!*

Using VNC, a provided LDAP server and a third Red Hat Enterprise Linux client server, this lab takes an existing LDAP server and allows an alternative RHEL client to authenticate using OpenLDAP. Additionally, an NFS share is used to mount the user's home directory upon initial log in.

# Connect to and Test the Environment

Once the lab server has finished provisioning, use a VNC viewer to connect to the client with the public IP provided on the Live! Lab page. Append the port *:5901* to the IP address. Connect to the server; continue past any warning about unencrypted connections, and exit any screens requesting an additional password for color-managed devices.

The overall *linuxacademy* user account password is *123456*.

You should now be connected to the client server through VNC, complete with a GUI interface.

From here, open the terminal and ensure you can communicate with the OpenLDAP server available for use. Do this through the use of the `ping` command:

```
ping ldap.linuxacademy.com
```

# Bind the Member Server to the LDAP Server

Through the use of the `authconfig` command, we can bind our RHEL 7 server to the existing LDAP server. Become *root*:

```
su -
```

The password for root is *123456*.

Install the `authconfig-gtk` package, which provides users with a graphical interface for managing authentication.

```
yum install -y authconfig-gtk
```

Once installed, open the **Authentication** program, located under **Applications** > **Sundry** > **Authentication**. Again, the root password is *123456*.

From the **Identity & Authentication** tab, select *LDAP* for **User Account Database**. An error notes that the `nss-pam-ldapd` package is required for LDAP to work. Open your terminal and install the needed package:

```
yum install -y nss-pam-ldapd
```

Return to the **Authentication** application.

Again, select *LDAP*. Once more, an error notes a required package for LDAP-use. Install the package:

```
yum install -y pam_krb5
```

Alternatively, both of these packages can be installed from the GUI, using the **Install** button within the error message.

With the LDAP dependencies installed, we can now enter our LDAP information under the **Identity & Authentication** tab. The **LDAP Search Base DN** is *dc=linuxacademy,dc=com*, and the **LDAP Server** is *ldap://ldap.linuxacademy.com*. Check the box for **Use TLS to encrypt connections**.

Press **Download CA Certificate...**. The URL for the certificate is *http://ldap.linuxacademy.com/pub/cert.pem*.

Leave **Authentication Method** as *Kerberos password*.

Move to the **Advanced Options** tab. Check **Create home directories on the first login**. **Apply** the changes.

# Auto-Mount a Home Directory

Install the `autofs`, `openldap-clients` and `nfs-utils` packages:

```
yum install -y autofs nfs-utils openldap-clients
```

Open the */etc/auto.master.d/ldap.autofs* file, and add the following line:

```
/home/guests /etc/auto.ldap
```

Save and exit.

Now create the */etc/auto.ldap* file, and add the following:

```
* -rw ldap.linuxacademy.com:/home/guests/&
```

Save and exit.

Additionally, we need to enable the ability to use LDAP credentials through SSH. Open the */etc/pam.d/sshd* file, and add the following lines to the top of the file:

```
auth sufficient pam_ldap.so
```

```
auth sufficient pam_permit.so
```

Start and enable the automounter daemon, then restart SSH:

```
systemctl start autofs && systemctl enable autofs
systemctl restart sshd
```

# Log in to the Server Using LDAP

Using SSH, we can log in to our RHEL 7 server using one of three provided users set up on the LDAP server:

**User 1**

- Username: ldapuser1
- Password: L1nUxAcaD3meee

**User 2**

- Username: ldapuser2
- Password: L1nUxAcaD3meee

**User 3**

- Username: ldapuser3
- Password: L1nUxAcaD3meee

SSH using the client server's public IP provided on the Live! Lab page:

```
ssh ldapuser1@publicip
```

Once successful, the lab is complete.