Ubuntu Server LDAP Configuration

Drew Baker s222292111 Redback Operations

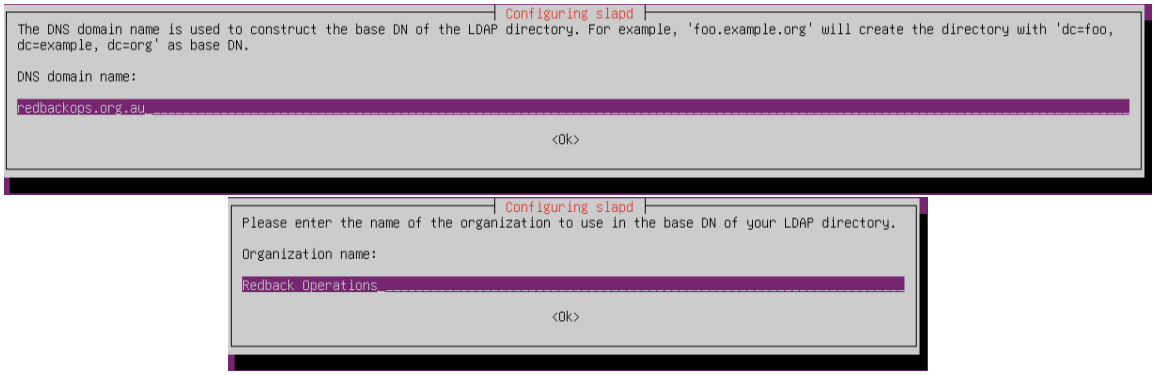
Ubuntu Server LDAP Configuration

Introduction

This document provides a comprehensive guide for setting up an LDAP directory using an Ubuntu server. The images provided in this document are designed to visually represent the various stages of the LDAP environment configuration, from the installation process to the configuration and integration of LDAP directory objects. This setup is designed to help users understand how to build and manage LDAP servers while expanding upon the company's infrastructure.

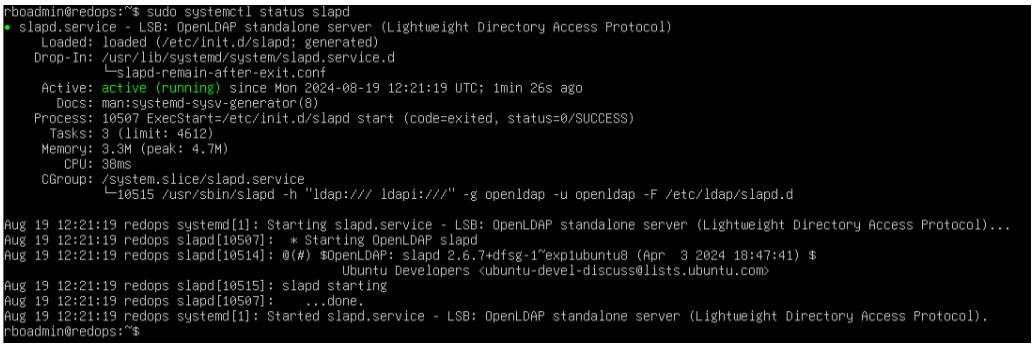
LDAP Setup Overview

The setup begins with updating and upgrading the Ubuntu server to ensure that all necessary system components are up to date. Next, the installation of LDAP packages ‘slapd’ and ‘ldap-utils’ is required to interact with the LDAP server using specialised utilities. This can be done with the following commands:



- `sudo apt update && sudo apt upgrade`
- `sudo apt install slapd ldap-utils`
- `sudo dpkg-reconfigure slapd`

Following the installation, it's important to manage the LDAP service using the ‘systemctl’ commands:



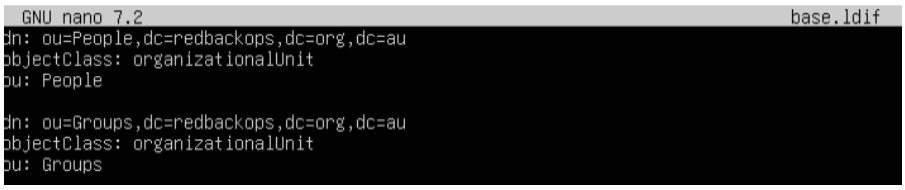
- `sudo systemctl status slapd`
- `sudo systemctl start slapd`
- `sudo systemctl stop slapd`
- `sudo systemctl restart slapd`

Ubuntu Server LDAP Configuration

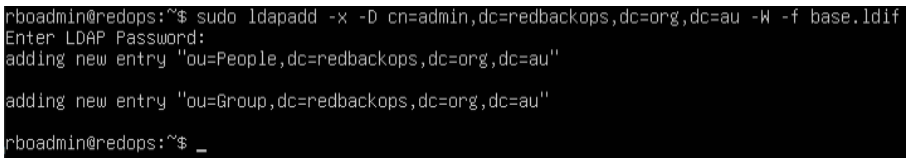
Configuring LDAP Structure

The directory structure can now be created, starting with the 'ldapsearch' command to search for the base domain ('dc=NAME,dc=TLD'). The following LDIF data structures are then added:

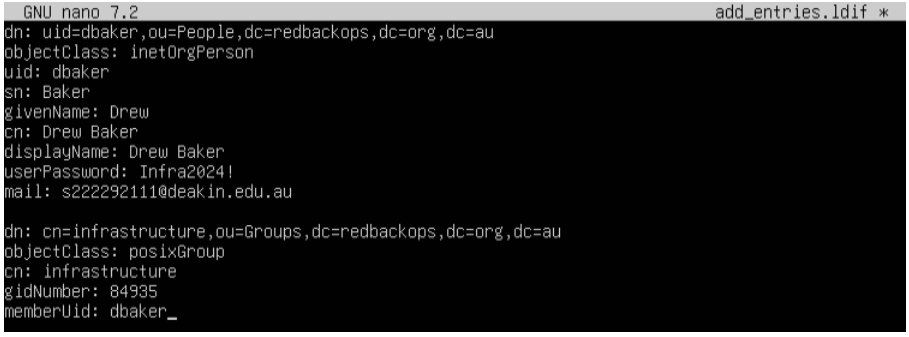
1. Creating Organizational Units (OUs): This defines the 'People' and 'Groups' units within the directory.




```
dn: ou=People,dc=example,dc=com

objectClass: organizationalUnit

ou: People


dn: ou=Groups,dc=example,dc=com

objectClass: organizationalUnit

ou: Groups
```



2. Adding Users and Groups: A user, 'jdoe', is added along with a group called developers. These entries are created using the following LDIF format:

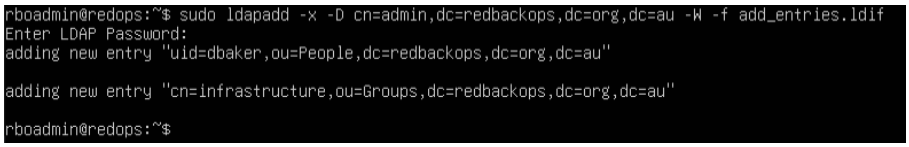



```
dn: uid=jdoe,ou=People,dc=example,dc=com

objectClass: inetOrgPerson

uid: jdoe

sn: Doe

givenName: John

cn: John Doe
```

```
displayName: John Doe
userPassword: secret
mail: jdoe@example.com

dn: cn=developers,ou=Groups,dc=example,dc=com
objectClass: posixGroup
cn: developers
gidNumber: 5000
memberUid: jdoe
```

These entries are added using the following command:

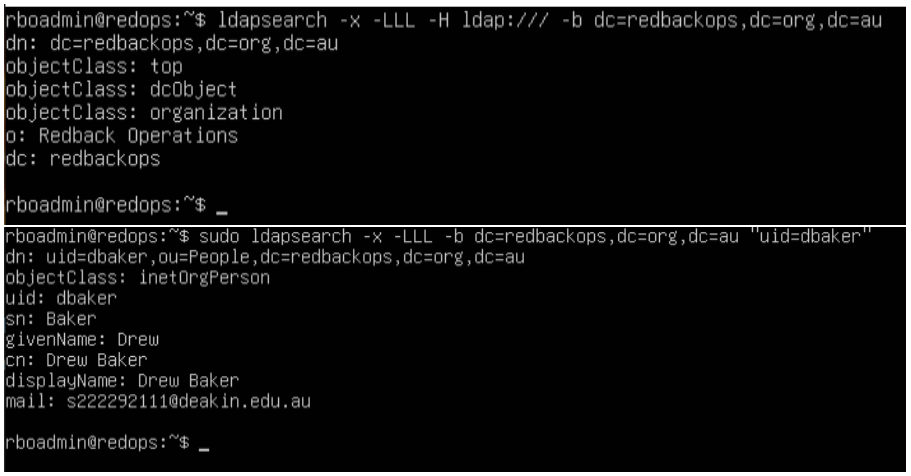
- sudo ldapadd -x -D cn=admin,dc=example,dc=com -W -f add_entries.ldif



Verifying LDAP Configuration

To ensure that the configuration is successful, LDAP searches are performed using the following command:

- ldapsearch -x -LLL -H ldap:/// -b dc=example,dc=com
- ldapsearch -x -LLL -b dc=example,dc=com 'uid=jdoe'



Ubuntu Server LDAP Configuration

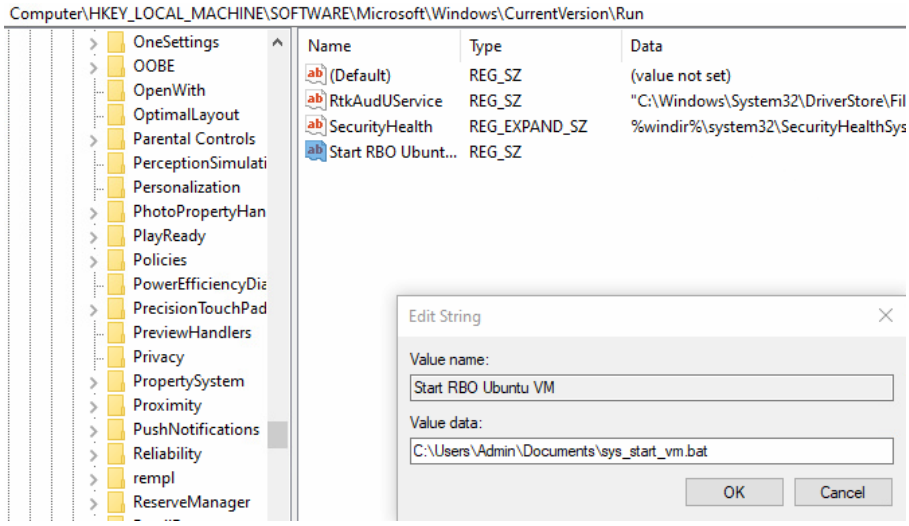
Useful LDAP utilities command flags

- -x (Simple Authentication):
  This flag disables SASL and uses simple authentication instead, meaning the command will use a straightforward username and password for authentication. This is useful when you don't want or need to configure a more complex authentication mechanism.
- -LLL (Suppress Output Formatting):
  This flag removes all additional information from the output, such as version numbers, comments, and DN (Distinguished Name) listings. It provides a clean and minimal output by only showing the LDAP entries. This is often used when the raw data is needed, or when the output needs to be parsed by another tool.
- -H ldap:/// (LDAP Server URI):
  This flag specifies the URI of the LDAP server you want to query. In this case, ldap:/// means the search will be executed on the default local LDAP server running on the machine. If querying a remote server, this could be ldap://server-address/.
- -b dc=NAME,dc=TLD (Search Base):
  This flag defines the base Distinguished Name (DN) from which to start searching in the directory. dc=NAME,dc=TLD represents the domain components (e.g., dc=example,dc=com), and the search will start from this point in the directory hierarchy. It restricts the search scope to this particular branch of the directory.
- -D cn=admin,dc=example,dc=com (Bind DN):
  This flag specifies the Distinguished Name (DN) of the user who is authenticating (i.e., the "bind" DN). In this case, the admin user (cn=admin) is used to bind to the LDAP server and make changes. The DN must be provided in full, with domain components (e.g., dc=example,dc=com).
- -W (Password Prompt):
  This flag tells the command to prompt for the password of the specified bind DN. This prevents the password from being passed directly in the command, enhancing security by not exposing the password in the command history.
- -f base.ldif (LDIF File):
  This flag specifies the LDIF file to be used. The LDIF file contains the directory entries (like organizational units, users, or groups) that are being added to the LDAP directory. In this example, the file base.ldif contains entries to be added.
- -Q (Quiet Mode for SASL Authentication):
  This flag enables quiet mode for SASL authentication. When used, it suppresses the interactive prompts and authentication state messages that are normally displayed during SASL authentication. This is useful when you want to avoid unnecessary output during SASL binding.
- -Y EXTERNAL (SASL External Authentication):
  This flag specifies that SASL external authentication should be used. The EXTERNAL mechanism typically relies on an identity established through the client's connection instead of requiring a username and password. It's commonly used with local connections (ldapi:///) where the server trusts the client's identity from the connection itself.

Ubuntu Server LDAP Configuration

Automating the Virtual Machine (VM) Startup

For teams using a Windows-based host for the Ubuntu server, an optional script is provided to automatically start the VM when the host machine boots up:



"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" startvm "Ubuntu Server Workspace"

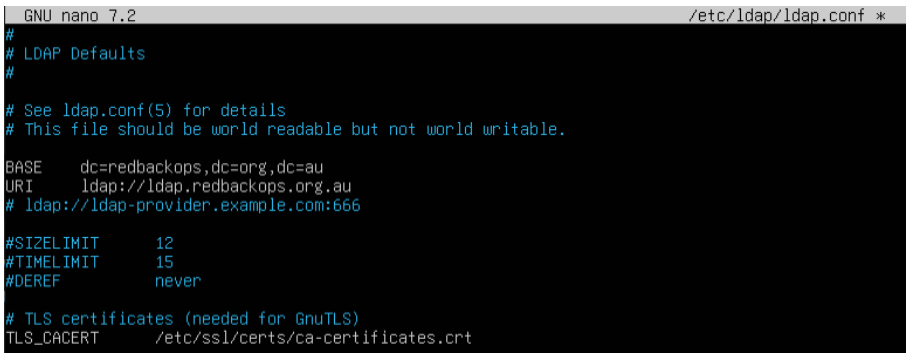
By adding the path to this '.bat' file as a string in the Windows registry 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run', the VM can be automatically launched during system startup.

LDAP Customization

LDAP can be further customized by adding custom schemas or integrating SSL for secure communication. An example command for adding a custom schema is provided:

- sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /path/to/custom-schema.ldif

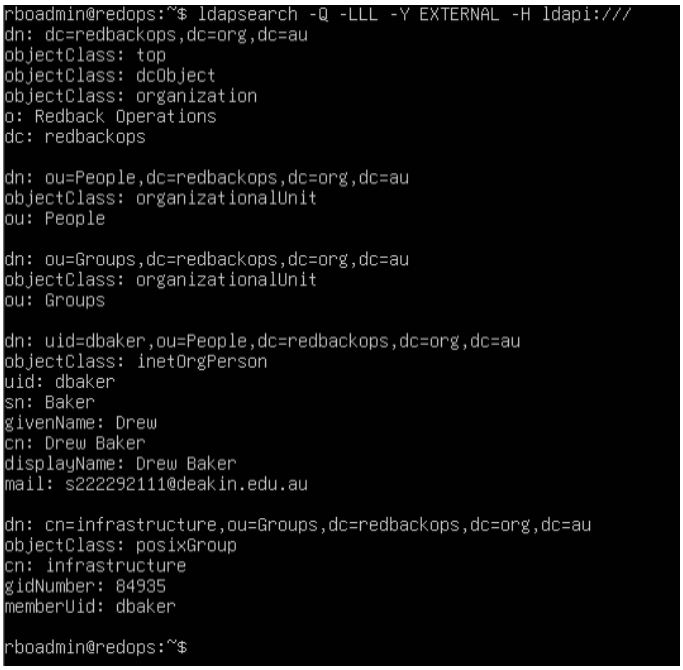
For a convenience standpoint the configuration file located at '/etc/ldap/ldap.conf' has been modified to help reduce the values that need to entered to perform operations (see below).



So if we were to perform an LDAP search query it would now look like the following:

- ldapsearch -Q -LLL -Y EXTERNAL -H ldap:///

Ubuntu Server LDAP Configuration



Conclusion

Each of these steps, paired with the provided images, visually represents the LDAP setup and management process. From installation to creating users and groups, this guide offers a detailed explanation of how to configure and verify an LDAP server in an Ubuntu environment.