



Project Report - Manual Exercises (Bac +2)

Submitted by: ALAGO CHIEMELA VICTOR

Projects Dates: 9th November, 2023 to 24th January 2024.

Completed in partial fulfillment of the requirements for the course:

INTRODUCTION TO ENTERPRISE NETWORKS

At:

EPITA, SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

Academic Year: 2023/2024

Paris, 23rd January 2024.

Personal Take On The Course:

Throughout the course, I was exposed to a variety of critical concepts, from the foundational structures of why network security is important to the advanced mechanisms of access control and security. The exercises, ranging from LDAP implementation to ACL configuration, were not just educational but also immensely practical. They provided a hands-on experience that transformed theoretical knowledge into tangible skills. These exercises were particularly enlightening, offering a clear view of the real-world applications and challenges in enterprise network management.

One of the key realizations from this course was the importance of structured organization and meticulous planning in network management. Setting up LDAP trees, managing users and groups, and implementing access control models showed me how crucial it is to have a well-thought-out plan and structure in place. It highlighted that security and accessibility are not just about the tools and technologies employed but also about how they are integrated and managed.

Moreover, the course underlined the significance of adaptability and continuous learning. The field of enterprise networks is ever-evolving, with new challenges and technologies emerging regularly. Staying updated and being able to adapt to new tools and methods, as seen in the shift from traditional LDAP management to using tools like LAM, is vital for anyone aspiring to excel in this field.

In essence, this course was more than just an academic pursuit; it was a journey that equipped me with both the knowledge and practical skills essential for navigating the complex world of enterprise networks. It has reinforced my understanding of how critical network infrastructure is to any organization and why it is essential.

As I present this report, which is a sum-up of the exercises and learning from the course, I am confident that the insights and experiences gained here will be invaluable in my future endeavors in network administration and management.

EXERCISE 2 – Access Control Matrix

Objective: The primary goal of this exercise was to design an Access Control Matrix (ACM) that categorizes my company employees by their department and assigns appropriate access rights to various digital assets.

Access Control Matrix is a model used in computer systems to know what files and permissions is available to who within an enterprise network. It defines the users and the permissions they have to either read, write or execute a file or digital asset. A user can have all rights (ie rwx) to a particular digital asset, some rights only(eg rw) or none at all(-).

ACM is essential in every enterprise network to boost the data security and integrity within the company. Employees should only access what they need to perform their job and not more, a concept known as the principle of least privilege. It is also essential for implementing user authentication, authorization and accountability for their privileges.

For this exercise,

- I assigned each of the 45 employees a unique first and last name.
- I allocated the employees to different departments, reflecting the organizational structure of my enterprise KodakTech Solutions Inc.
- I defined the digital assets available in my company and defined the ACM for each department and users in them.

I ensured permissions were logically assigned, reflecting how an employee in a certain department would interact with specific assets. For example, Finance Department employees having read and write access to "Financial Reports". I also made sure to use the principle of **Least Privilege** to assign these rights.

47°F

cloudy

Figure 1 - ACM Excel Screenshot

Conclusion

This exercise highlighted the practical aspects of implementing an ACM in a real-world scenario, teaching the importance of precise access control in organizational security and data management. It also showcased the effectiveness of ACM as a tool for visualizing and managing complex access relationships within an enterprise.

EXERCISE 3 – Installing and Setting Up OpenLDAP

Objective: The primary goal was to install OpenLDAP, a popular open-source implementation of LDAP (Lightweight Directory Access Protocol) and configure it for the organization 'epita'. I carried out this exercise in the terminal of my ubuntu linux system.

1. Installation of OpenLDAP:

- Installed OpenLDAP software on suitable server environment.
- This step involved downloading the OpenLDAP package and running the installation commands.

2. Configuration of Distinguished Names (DN):

- Configured the LDAP directory using a DN format of **dn=alago,dn=com**.
- Set up the organization name as 'epita' within the LDAP structure.
- This DN configuration was critical for structuring the LDAP directory tree appropriately for the organization.

3. Verification of Installation and DN Configuration:

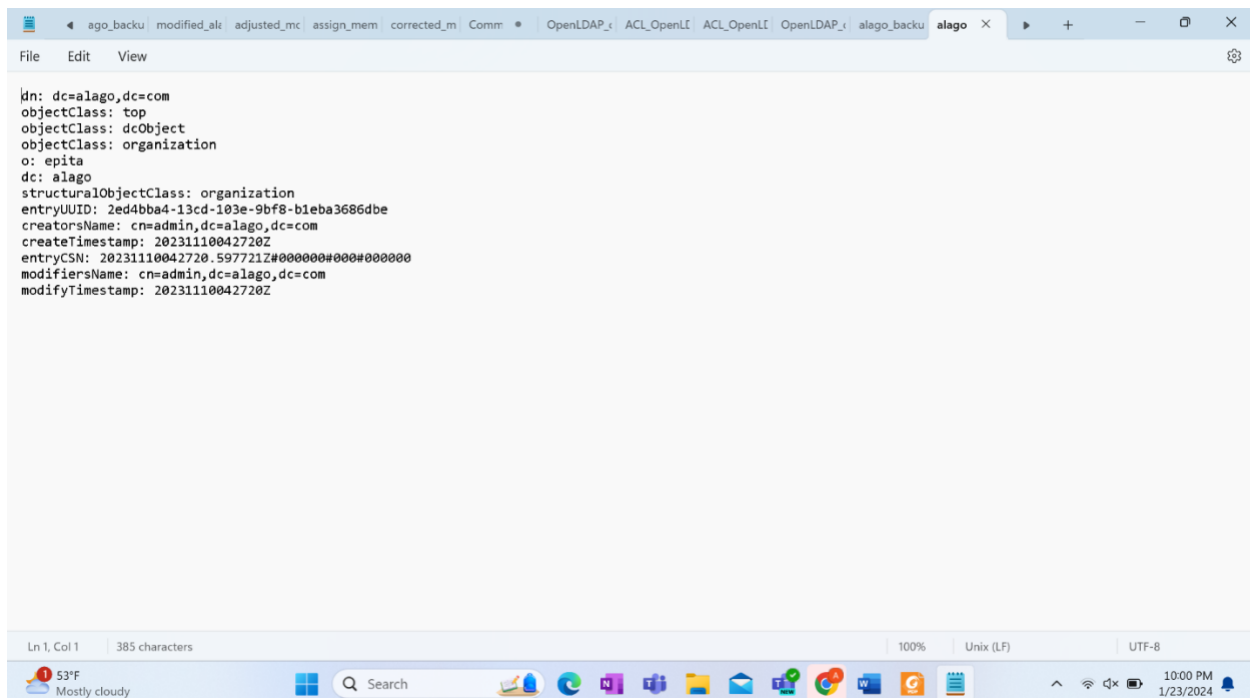
- Post-installation, verified the correct setup of OpenLDAP and the DN configuration.
- This step ensured that the LDAP server was operational and the directory structure was correctly established as intended.

4. Enabling Logging:

- Enabled logging in OpenLDAP to track operations and changes within the LDAP server.
- This was important for monitoring, troubleshooting, and ensuring the integrity of the LDAP implementation.

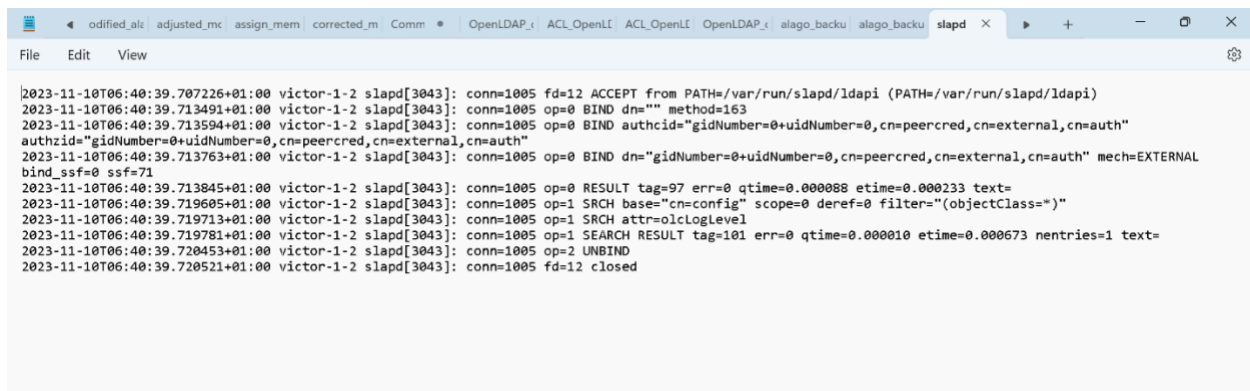
5. Backup of Directory:

- Created a backup of the LDAP directory in the form of an LDIF (LDAP Data Interchange Format) file named **alago_backup.ldif**.
- This backup was crucial for data recovery and ensuring the integrity of the LDAP directory.



```
dn: dc=alago,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: epita
dc: alago
structuralObjectClass: organization
entryUUID: 2ed4bba4-13cd-103e-9bf8-b1eba3686dbe
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231110042720Z
entryCSN: 20231110042720.597721Z#000000#000#000000
modifiersName: cn=admin,dc=alago,dc=com
modifyTimestamp: 20231110042720Z
```

Figure 2 - alago_backup.ldif file



```
2023-11-10T06:40:39.707226+01:00 victor-1-2 slapd[3043]: conn=1005 fd=12 ACCEPT from PATH=/var/run/slapd/ldapi (PATH=/var/run/slapd/ldapi)
2023-11-10T06:40:39.713491+01:00 victor-1-2 slapd[3043]: conn=1005 op=0 BIND dn="" method=163
2023-11-10T06:40:39.713594+01:00 victor-1-2 slapd[3043]: conn=1005 op=0 BIND authcid="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
2023-11-10T06:40:39.713763+01:00 victor-1-2 slapd[3043]: conn=1005 op=0 BIND dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" mech=EXTERNAL
2023-11-10T06:40:39.713845+01:00 victor-1-2 slapd[3043]: conn=1005 op=0 RESULT tag=97 err=0 qtime=0.000088 etime=0.000233 text=
2023-11-10T06:40:39.719605+01:00 victor-1-2 slapd[3043]: conn=1005 op=1 SRCH base="cn=config" scope=0 deref=0 filter="(objectClass=*)"
2023-11-10T06:40:39.719713+01:00 victor-1-2 slapd[3043]: conn=1005 op=1 SRCH attr=olcLogLevel
2023-11-10T06:40:39.719781+01:00 victor-1-2 slapd[3043]: conn=1005 op=1 SEARCH RESULT tag=101 err=0 qtime=0.000010 etime=0.000673 nentries=1 text=
2023-11-10T06:40:39.720453+01:00 victor-1-2 slapd[3043]: conn=1005 op=2 UNBIND
2023-11-10T06:40:39.720521+01:00 victor-1-2 slapd[3043]: conn=1005 fd=12 closed
```

Figure 3 - slapd.log

Conclusion

This exercise demonstrated the practical steps involved in setting up and managing an LDAP server, a foundational component in enterprise network management. It emphasized the importance of careful configuration, documentation, and the maintenance of backups and logs in managing directory services. This experience contributes significantly to understanding how LDAP operates in real-world scenarios and its role in organizational data management.

EXERCISE 4 - Adding Organizational Units and Users in LDAP

Objective: To structure the LDAP directory in alignment with the organizational hierarchy by creating Organizational Units (OUs) for different departments of my company and adding users (my employees) to these OUs.

1. Creation of Configuration File:

- Developed a configuration file named **MyCompany_alago.ldif**.
- This LDIF (LDAP Data Interchange Format) file served as the blueprint for modifications in the LDAP directory.

2. Creating the 'Departments' OU:

- Established a top-level Organizational Unit (OU) named 'Departments'.
- This OU acted as a container for various departmental units, reflecting the organizational structure.
- Under the 'Departments' OU, I created additional OUs corresponding to each department identified in earlier exercise.
- These OUs provided a structured and organized framework within LDAP, mirroring the functional divisions within the organization.

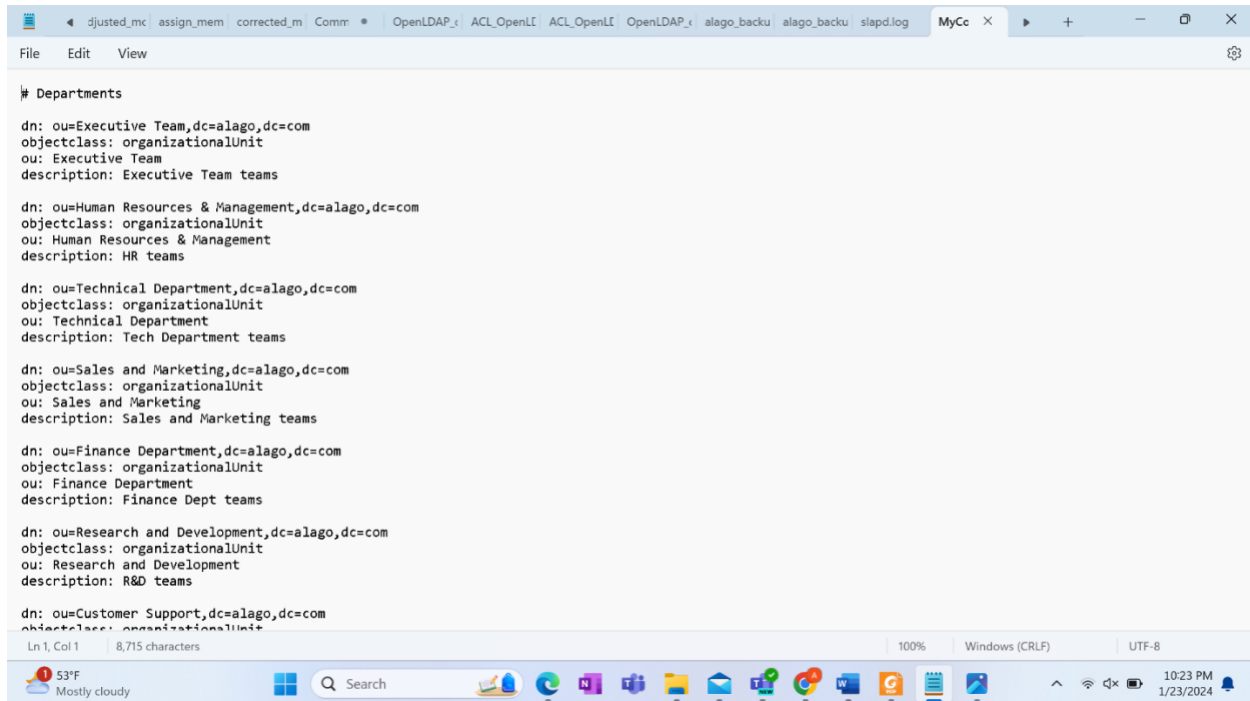


Figure 4 - MyCompany_alago.ldif



Figure 5 - screenshot adding OUs

3. Adding Users to Departments:

- Populated the departmental OUs with users that were defined previously.

- Each user was added to their respective departmental OU, ensuring that the directory structure accurately represented the real-world organizational layout.

```

# Employees

# Executive Team
dn: cn=John Smith,ou=Executive Team,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: John
sn: Smith
cn: John Smith
uid: js
userPassword: changeme

dn: cn=Sarah Johnson,ou=Executive Team,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: Sarah
sn: Johnson
cn: Sarah Johnson
uid: sj
userPassword: changeme

dn: cn=David Lee,ou=Executive Team,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: David
sn: Lee
cn: David Lee
uid: dl
userPassword: changeme

dn: cn=Amanda Smith,ou=Executive Team,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: Amanda
sn: Smith
cn: Amanda Smith
uid: as
userPassword: changeme

# Human Resources & Management
dn: cn=Lisa Davis,ou=Human Resources & Management,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: Lisa
sn: Davis
cn: Lisa Davis
uid: ld
userPassword: changeme

dn: cn=Michael Williams,ou=Human Resources & Management,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: Michael
sn: Williams
cn: Michael Williams
uid: mw
userPassword: changeme

# Technical Department
dn: cn=Emily Brown,ou=Technical Department,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: Emily
sn: Brown
cn: Emily Brown
uid: eb
userPassword: changeme

dn: cn=Jennifer Turner,ou=Technical Department,dc=alago,dc=com
objectClass: inetOrgPerson
givenName: Jennifer
sn: Turner
cn: Jennifer Turner
uid: jt
userPassword: changeme

```

Figure 6 - users in MyCompany_alago.ldif

```

victor@victor-1-2: ~
File Edit View Search Terminal Help

adding new entry "cn=Anderson Cooper,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Mira Casto,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Jeffery Zhan,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Chun-Li Harris,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Natalie Micheals,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Larry Bluebird,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Jonny O'Brien,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Jimmy Choo,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Naomi Suki,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Willie Docks,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Ben Jeffery,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Lago Biggs,ou=Research and Development,dc=alago,dc=com"
adding new entry "cn=Sharon Hall,ou=Customer Support,dc=alago,dc=com"
adding new entry "cn=Brian King,ou=Customer Support,dc=alago,dc=com"
adding new entry "cn=Malika Andrews,ou=Customer Support,dc=alago,dc=com"

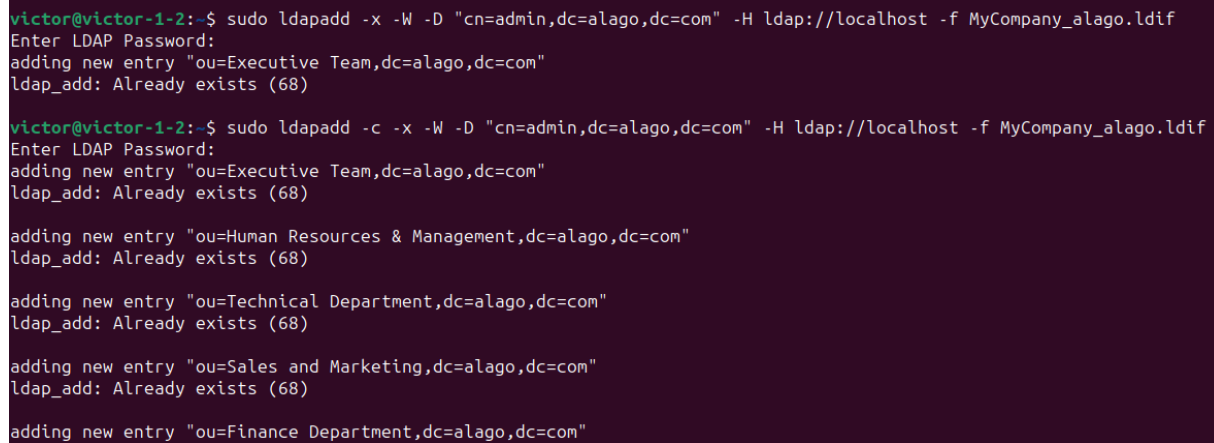
victor@victor-1-2:~$ sudo slapcat -b dc=alago,dc=com -l alago_backup.ldif
victor@victor-1-2:~$

```

Figure 7 - screenshot adding users

4. Verification of Modifications:

- Used the **sudo slapcat** command to verify the changes made to the LDAP directory.
- This step was crucial to ensure that all additions and organizational structures were correctly implemented in LDAP.



```
victor@victor-1-2:~$ sudo ldapadd -x -W -D "cn=admin,dc=alago,dc=com" -H ldap://localhost -f MyCompany_alago.ldif
Enter LDAP Password:
adding new entry "ou=Executive Team,dc=alago,dc=com"
ldap_add: Already exists (68)

victor@victor-1-2:~$ sudo ldapadd -c -x -W -D "cn=admin,dc=alago,dc=com" -H ldap://localhost -f MyCompany_alago.ldif
Enter LDAP Password:
adding new entry "ou=Executive Team,dc=alago,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=Human Resources & Management,dc=alago,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=Technical Department,dc=alago,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=Sales and Marketing,dc=alago,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=Finance Department,dc=alago,dc=com"
```

Figure 8 - screenshot of verification

5. Backup of Directory:

- Conducted a backup of the updated LDAP directory, saved as **alago_backup.ldif**.
- This backup ensured data integrity and provided a recoverable state of the LDAP directory post-modifications.

```
File Edit View

dn: dc=alago,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: epita
dc: alago
structuralObjectClass: organization
entryUUID: 2ed4bba4-13cd-103e-9bf8-b1eba3686dbe
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231110042720Z
entryCSN: 20231110042720.597721Z#000000#000#000000
modifiersName: cn=admin,dc=alago,dc=com
modifyTimestamp: 20231110042720Z

dn: ou=Executive Team,dc=alago,dc=com
objectClass: organizationalUnit
ou: Executive Team
description: Executive Team teams
structuralObjectClass: organizationalUnit
entryUUID: cf8b7d12-1b5c-103e-891f-718476b39ba1
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231119192306Z
entryCSN: 20231119192306.402651Z#000000#000#000000
modifiersName: cn=admin,dc=alago,dc=com
modifyTimestamp: 20231119192306Z

dn: ou=Human Resources & Management,dc=alago,dc=com
objectClass: organizationalUnit
ou: Human Resources & Management
description: HR teams
structuralObjectClass: organizationalUnit
entryUUID: cf903078-1b5c-103e-8920-718476b39ba1
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231119192306Z
entryCSN: 20231119192306.539710Z#000000#000#000000
modifiersName: cn=admin,dc=alago,dc=com
modifyTimestamp: 20231119192306Z

Ln 1, Col 1      23,657 characters
55°F Cloudy Search
```

```
File Edit View

dn: ou=Technical Department,dc=alago,dc=com
objectClass: organizationalUnit
ou: Technical Department
description: Tech Department teams
structuralObjectClass: organizationalUnit
entryUUID: cf967028-1b5c-103e-8921-718476b39ba1
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231119192306Z
entryCSN: 20231119192306.474464Z#000000#000#000000
modifiersName: cn=admin,dc=alago,dc=com
modifyTimestamp: 20231119192306Z

dn: ou=Sales and Marketing,dc=alago,dc=com
objectClass: organizationalUnit
ou: Sales and Marketing
description: Sales and Marketing teams
structuralObjectClass: organizationalUnit
entryUUID: cf9ef70c-1b5c-103e-8922-718476b39ba1
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231119192306Z
entryCSN: 20231119192306.530345Z#000000#000#000000
modifiersName: cn=admin,dc=alago,dc=com
modifyTimestamp: 20231119192306Z

dn: ou=Finance Department,dc=alago,dc=com
objectClass: organizationalUnit
ou: Finance Department
description: Finance Dept teams
structuralObjectClass: organizationalUnit
entryUUID: cfa064de-1b5c-103e-8923-718476b39ba1
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231119192306Z
entryCSN: 20231119192306.539710Z#000000#000#000000
modifiersName: cn=admin,dc=alago,dc=com
modifyTimestamp: 20231119192306Z

Ln 1, Col 1      23,657 characters
55°F Cloudy Search
```

Figure 9 - alago_backup.ldif

Conclusion

This exercise emphasized the practical aspects of managing an LDAP directory in an organized and efficient manner. It showcased how LDAP can be used to mirror an organization's structure and manage user data systematically. The process underscored the importance of careful planning and documentation in directory services management, providing valuable insights into LDAP's capabilities and applications in real-world organizational settings.

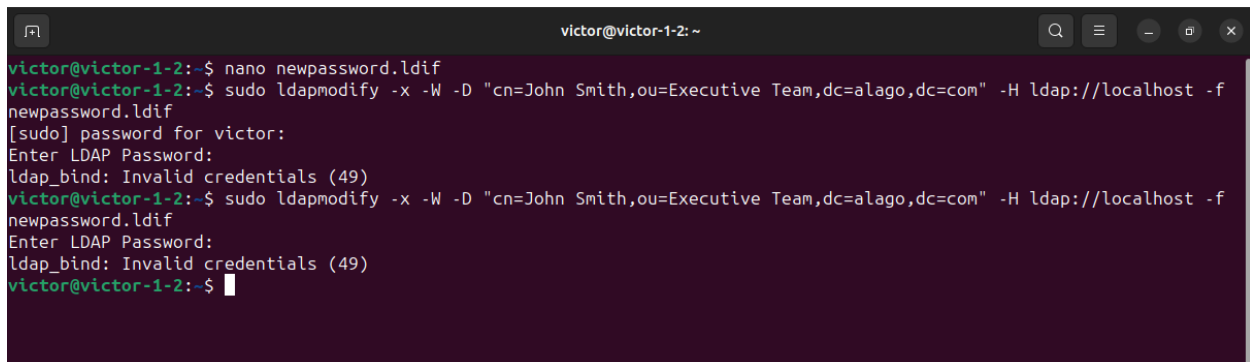
EXERCISE 5 - Using OpenLDAP ACLs for Password Management

Objective: The goal was to understand and implement ACL rules in OpenLDAP to enable users to change their own passwords while restricting them from altering others' passwords.

Step-by-Step Process and Observations

1. Initial Password Change Attempt:

- Selected a user, John Smith from the Executive Team, to test the password change process.
- Initially tried changing John Smith's password using his credentials. This step was to establish the baseline functionality before implementing any ACL changes. As expected, I wasn't allowed to.



```
victor@victor-1-2: ~  
victor@victor-1-2:~$ nano newpassword.ldif  
victor@victor-1-2:~$ sudo ldapmodify -x -W -D "cn=John Smith,ou=Executive Team,dc=alago,dc=com" -H ldap://localhost -f  
newpassword.ldif  
[sudo] password for victor:  
Enter LDAP Password:  
ldap_bind: Invalid credentials (49)  
victor@victor-1-2:~$ sudo ldapmodify -x -W -D "cn=John Smith,ou=Executive Team,dc=alago,dc=com" -H ldap://localhost -f  
newpassword.ldif  
Enter LDAP Password:  
ldap_bind: Invalid credentials (49)  
victor@victor-1-2:~$
```

Figure 10 - screenshot of failed attempt

2. Creating and Implementing ACL Rule:

- Developed an ACL rule that allows authenticated users to change their own password. This involved writing and applying the appropriate rule in the LDAP configuration.
- The implementation process highlights the specific syntax and logic used in crafting the ACL rule.



Figure 11 - newACLRule.ldif

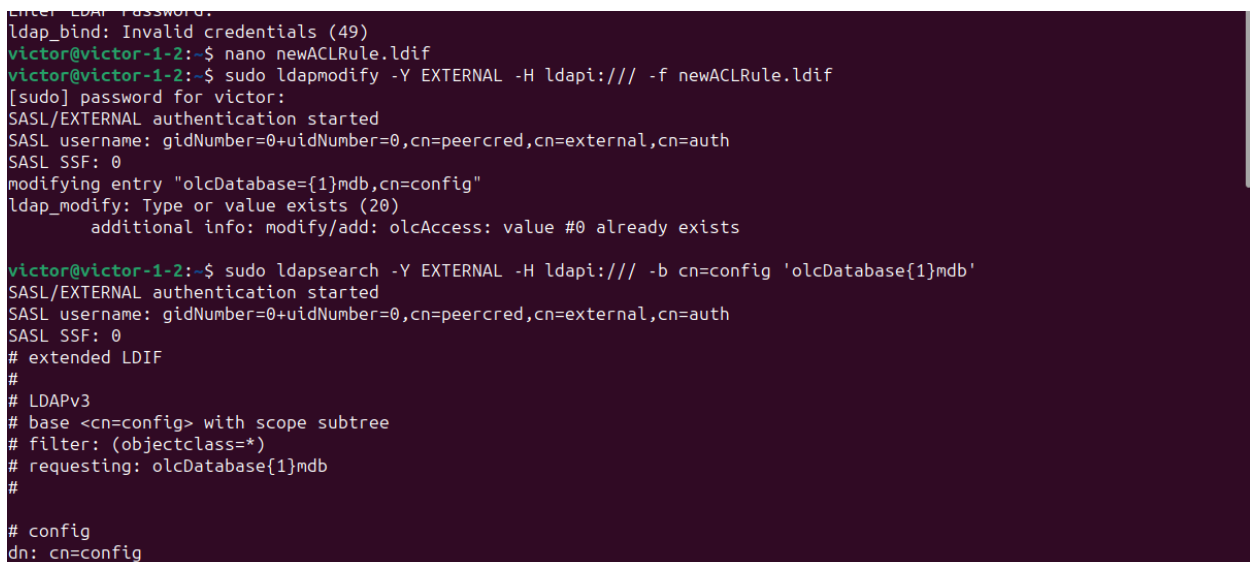


Figure 12 - screenshot to showing newACLRule rejected

It didn't work because there was already an ACL rule that was defined, and I verified this using the `ldapssearch` command. Then I created a `deleteACL.ldif` file to remove all existing ACL before re-running the `newACL.ldif` file.



Figure 13 - deleteACL.ldif

```

# {0}config, config
dn: olcDatabase={0}config,cn=config

# {1}mdb, config
dn: olcDatabase={1}mdb,cn=config

# search result
search: 2
result: 0 Success

# numResponses: 11
# numEntries: 10
victor@victor-1-2:~$ nano deleteACL.ldif
victor@victor-1-2:~$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f deleteACL.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"

victor@victor-1-2:~$

```

Figure 14 - screenshot on deleting existing ACL rules

```

# numEntries: 10
victor@victor-1-2:~$ nano deleteACL.ldif
victor@victor-1-2:~$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f deleteACL.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"

victor@victor-1-2:~$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f newACLRule.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"

victor@victor-1-2:~$

```

Figure 15 - newACLRule accepted.

3. Testing Password Change Post-ACL Implementation:

- Attempted to change John Smith's password again, this time with the new ACL rule in place.
- And this time it worked as expected.

4. Confirming Password Change:

- Used the **slapcat** command to verify that John Smith's password was indeed changed in the LDAP directory.
- This step served as a confirmation that the ACL rule allowed for self-password changes.

```
victor@victor-1-2:~$ sudo ldapmodify -x -W -D "cn=John Smith,ou=Executive Team,dc=alago,dc=com" -H ldap://localhost -f
newpassword.ldif
Enter LDAP Password:
modifying entry "cn=John Smith,ou=Executive Team,dc=alago,dc=com"

victor@victor-1-2:~$ sudo slapcat
dn: dc=alago,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: epita
dc: alago
structuralObjectClass: organization
entryUUID: 2ed4bba4-13cd-103e-9bf8-b1eba3686dbe
creatorsName: cn=admin,dc=alago,dc=com
createTimestamp: 20231110042720Z
```

Figure 16 - screenshot of John's password changed and slapcat

5. Testing Unauthorized Password Change:

- As a security check, tried changing another user's password using John Smith's credentials.
- The ACL rule did not allow this.

Conclusion

This exercise was pivotal in demonstrating the practical application of OpenLDAP ACLs in managing user-specific permissions, particularly in the context of password management. It highlighted the importance of precise ACL configuration for maintaining security while allowing users to have the autonomy to manage their own credentials. The exercise also underscored the need for thorough testing and verification of ACL rules to ensure they function as intended without unintended permissions being granted.

EXERCISE 6 - Installing LAM, Recreating LDAP Tree and Creating Groups

Objective: The aim was to gain hands-on experience with LDAP Account Manager (LAM), a web-based LDAP management tool, by backing up the existing LDAP tree, deleting it, and then recreating it using LAM.

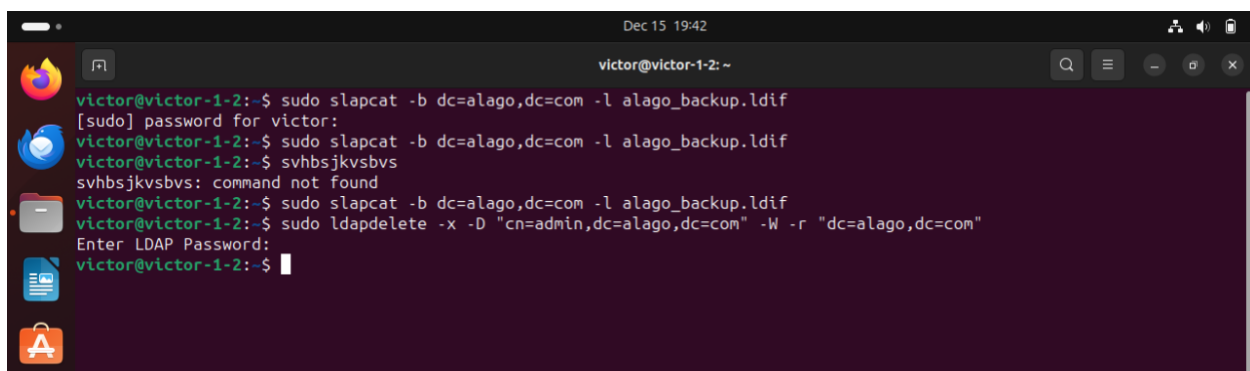
Step-by-Step Process and Observations

1. Backup Current LDAP Tree:

- Executed `sudo slapcat -b dc=alago,dc=com -l alago_backup.ldif` to backup the existing LDAP tree.
- This step ensured that all the current LDAP data was safely stored before making any changes.

2. Delete Current LDAP Tree:

- Performed deletion of the LDAP tree using `sudo ldapdelete`.
- This action cleared the existing structure, paving the way for a fresh setup with LAM.

A screenshot of a terminal window on a Linux system. The window title is "victor@victor-1-2: ~". The terminal shows the following commands and output:

```
victor@victor-1-2:~$ sudo slapcat -b dc=alago,dc=com -l alago_backup.ldif
[sudo] password for victor:
victor@victor-1-2:~$ sudo slapcat -b dc=alago,dc=com -l alago_backup.ldif
victor@victor-1-2:~$ svhbsjkvsbvs
svhbsjkvsbvs: command not found
victor@victor-1-2:~$ sudo slapcat -b dc=alago,dc=com -l alago_backup.ldif
victor@victor-1-2:~$ sudo ldapdelete -x -D "cn=admin,dc=alago,dc=com" -W -r "dc=alago,dc=com"
Enter LDAP Password:
victor@victor-1-2:~$
```

Figure 17 - screenshot of backup and deletion of LDAP

3. Installing and Configuring LAM:

- Followed the provided instructions to install and configure LDAP Account Manager.

- This process involved setting up LAM to interface correctly with the LDAP server.

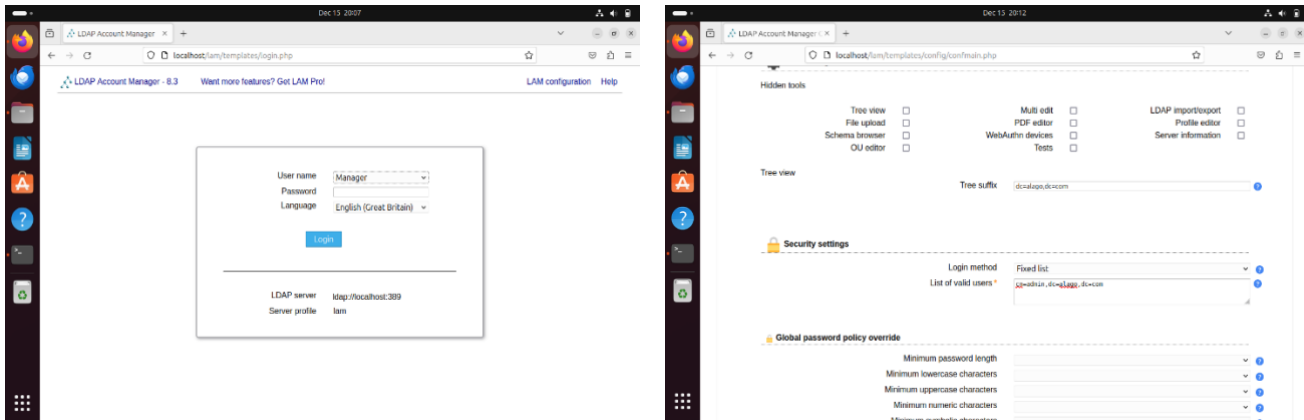


Figure 18 - LAM setup

4. Creating Organizational Units:

- Within LAM, created two Organizational Units (OUs): “Departments” and “Groups”.
- These OUs were essential for organizing the LDAP directory structure.

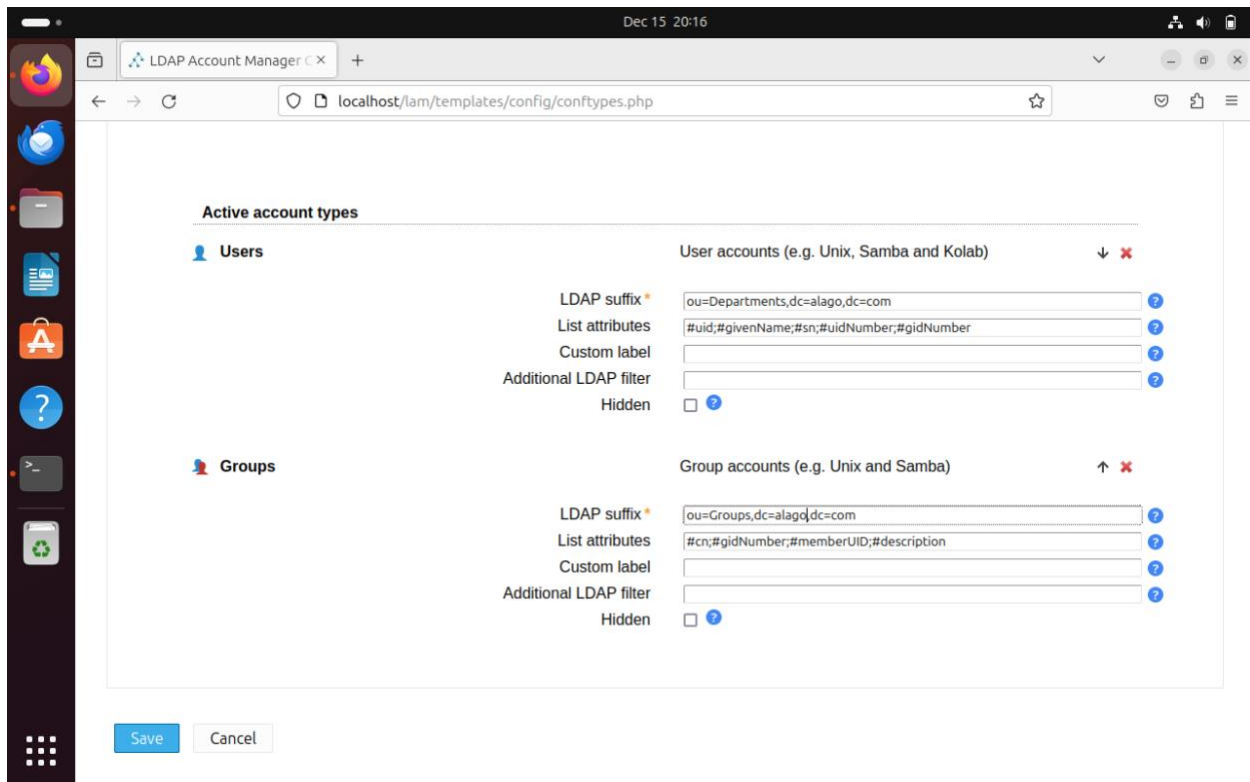


Figure 19 - creating Departments and Groups

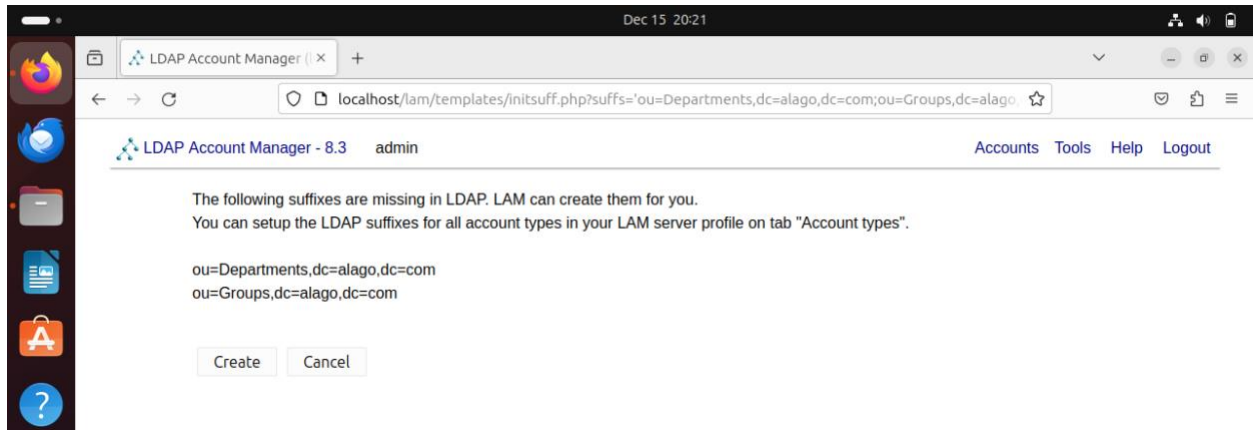


Figure 20 - creating Departments and Groups

5. Recreating Old OUs and Posix Groups:

- Under “Departments”, recreated the old OUs as they were in the previous LDAP setup.
- Under “Groups”, created respective posix groups corresponding to each department.

6. Adding Users to OUs and Groups:

- Populated the recreated OUs with the original users, assigning them to their respective departments and groups.
- This step was crucial for restoring the organizational structure within the LDAP directory and defining the role of each user within the company.

7. Verifying Tree Distribution:

- Utilized the “Tree View” in LAM to visually inspect the new LDAP tree structure.
- Took a screenshot of the full tree as a part of the documentation process.
- Also confirmed that the users were added to their appropriate groups.

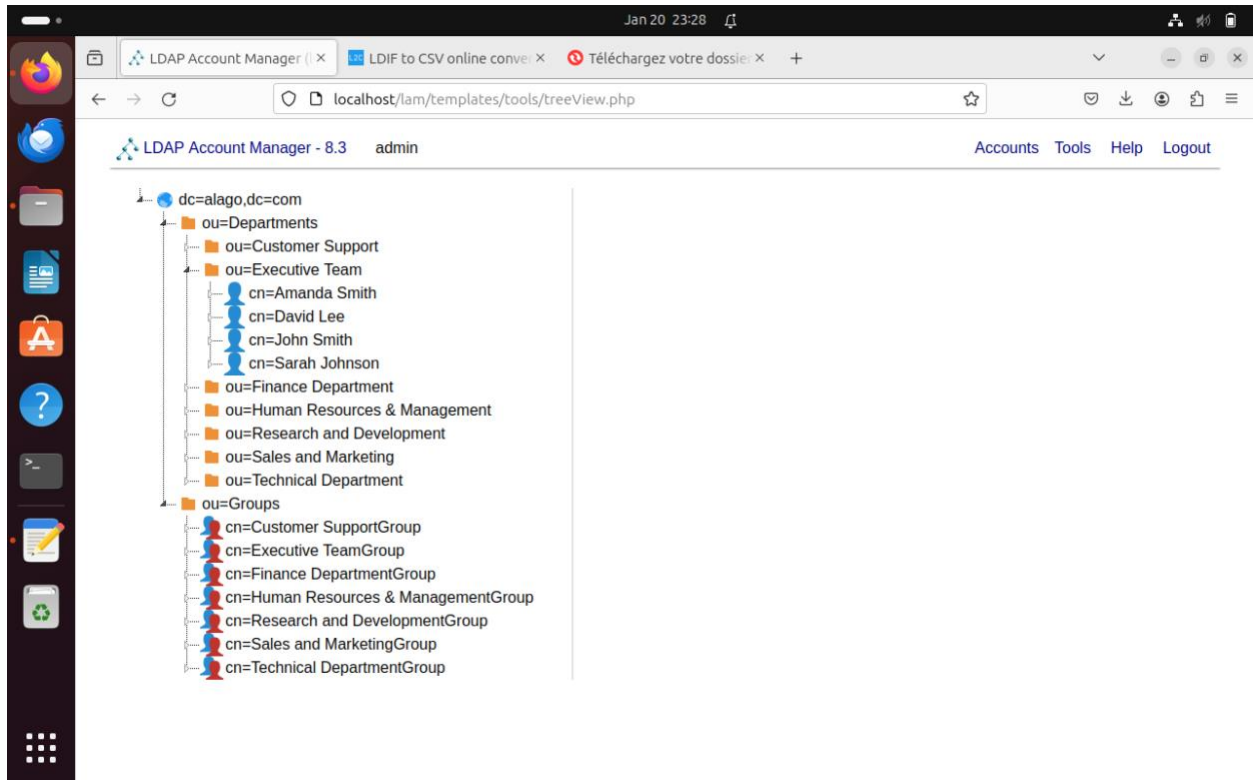


Figure 21 - screenshot of Tree showing Departments and Groups with some users

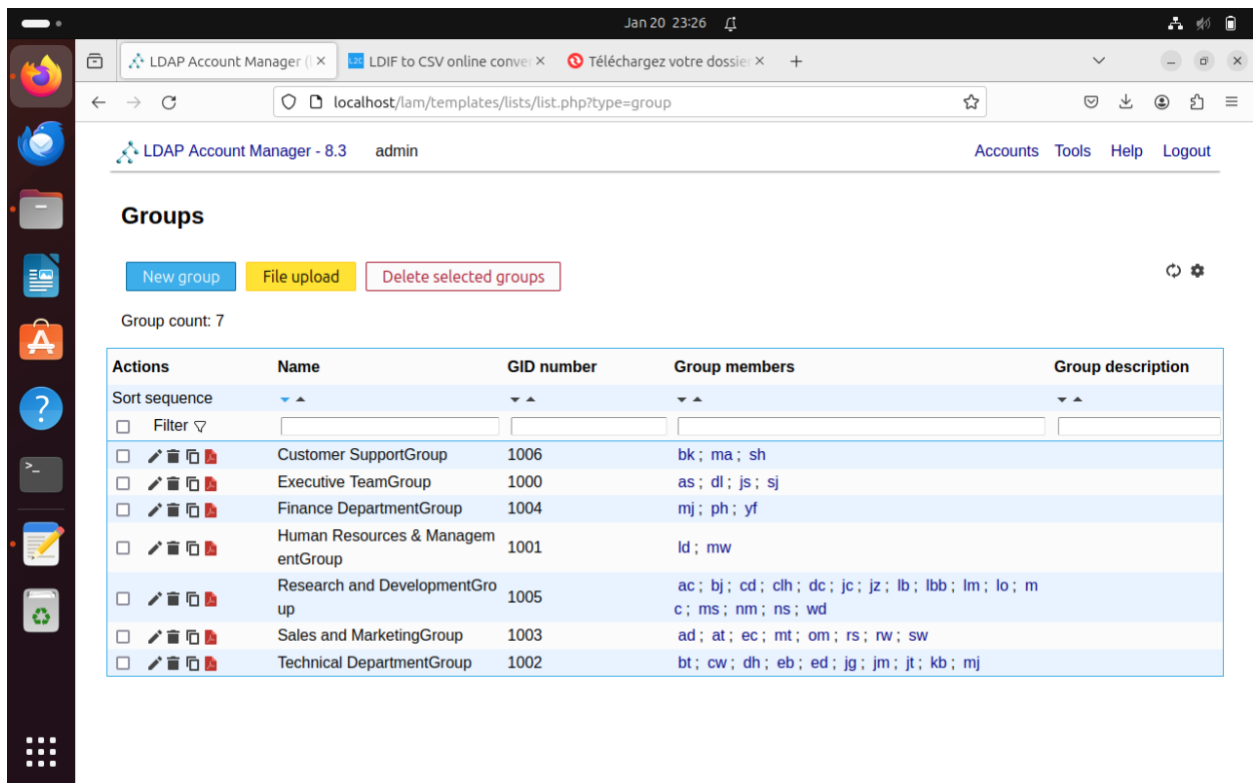


Figure 22 - screenshot verifying that users were added to their Groups too

8. Exporting New LDAP Tree:

- Exported the newly created LDAP tree, generating a file named **victor_alago_new.ldif**.
- This export served as a record of the new LDAP setup and could be used for restoration or analysis purposes. Like a backup file.
- It clearly shows the structure of the company by defining the users' credentials with their departments plus their addition to the different groups.



```
#
# Base DN: dc=alago,dc=com
# Search scope: sub
# Search filter: (objectClass=*)
# Total entries: 63
#
# Generated by LDAP Account Manager on 2024-01-20 22:19:09

version: 1

dn: dc=alago,dc=com
dc: alago
o: alago
objectclass: organization
objectclass: dcObject

dn: ou=Departments,dc=alago,dc=com
objectclass: organizationalUnit
ou: Departments

dn: ou=Customer Support,ou=Departments,dc=alago,dc=com
description: Customer Support teams
objectclass: organizationalUnit
ou: Customer Support

dn: cn=Brian King,ou=Customer Support,ou=Departments,dc=alago,dc=com
cn: Brian King
givenname: Brian
objectclass: inetOrgPerson
sn: King
uid: bk
userpassword: changeme
```



```
objectclass: posixGroup

dn: cn=Human Resources & ManagementGroup,ou=Groups,dc=alago,dc=com
cn: Human Resources & ManagementGroup
gidnumber: 1001
memberuid: ld
memberuid: mw
objectclass: posixGroup

dn: cn=Research and DevelopmentGroup,ou=Groups,dc=alago,dc=com
cn: Research and DevelopmentGroup
gidnumber: 1005
memberuid: dc
memberuid: lm
memberuid: ms
memberuid: cd
memberuid: ac
memberuid: mc
memberuid: jz
memberuid: clh
memberuid: nm
memberuid: lbb
memberuid: lo
memberuid: jc
memberuid: ns
memberuid: wd
memberuid: bj
memberuid: lb
objectclass: posixGroup

dn: cn=Sales and MarketingGroup,ou=Groups,dc=alago,dc=com
cn: Sales and MarketingGroup
gidnumber: 1003
memberuid: rs
memberuid: rw
```

Figure 23 - victor_alago_new.ldif.

Conclusion

This exercise was instrumental in demonstrating the practical use of LDAP Account Manager for managing LDAP directory services. It emphasized the importance of data backup and recovery, the utility of web-based management tools in simplifying complex directory setups, and the need for meticulous documentation and verification in system administration tasks. Through this exercise, the application of LAM in real-world LDAP management scenarios was clearly understood and documented. It is a more visual way of creating an LDAP similar to what we did using the terminal earlier.

EXERCISE 7 - Implementing Access Control Models

Objective: The aim was to practically implement access control in a Linux environment by creating a user group, assigning resources, and setting specific access permissions, thereby demonstrating an understanding of various access control models.

Step-by-Step Process and Observations

1. Creating a User Group:

- Created a group named **epita_users_AV**, replacing **\$name-initials** with my initials from Alago Victor.
- This step involved using group management commands to establish a new user group in the system.

```
victor@victor-1-2:~$  
victor@victor-1-2:~$  
victor@victor-1-2:~$ echo creating new group  
creating new group  
victor@victor-1-2:~$ sudo groupadd epita_users_AV  
victor@victor-1-2:~$  
victor@victor-1-2:~$
```

Figure 24 - creating new group

2. Adding Users to the Group:

- I created 5 new users in my linux terminal
- Added these 5 users to the **epita_users_AV** group.
- This process demonstrated the management of user-group associations in a Linux environment.

```
Jan 21 18:04  
victor@victor-1-2:~  
victor@victor-1-2:~$ echo creating new users  
creating new users  
victor@victor-1-2:~$ sudo adduser smith  
[sudo] password for victor:  
info: Adding user 'smith' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group 'smith' (1001) ...  
info: Adding new user 'smith' (1001) with group 'smith (1001)' ...  
info: Creating home directory '/home/smith' ...  
info: Copying files from '/etc/skel' ...  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
Changing the user information for smith  
Enter the new value, or press ENTER for the default  
Full Name []: John Smith  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] Y  
info: Adding new user 'smith' to supplemental / extra groups 'users' ...  
info: Adding user 'smith' to group 'users' ...
```

Figure 25 - creating new users for the purpose of this exercise

```
info: Adding user 'smith' to group 'users' ...  
victor@victor-1-2:~$ sudo adduser sarah  
info: Adding user 'sarah' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group 'sarah' (1002) ...  
info: Adding new user 'sarah' (1002) with group 'sarah (1002)' ...  
info: Creating home directory '/home/sarah' ...  
info: Copying files from '/etc/skel' ...  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
Changing the user information for sarah  
Enter the new value, or press ENTER for the default  
Full Name []: Sarah Johnson  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y  
info: Adding new user 'sarah' to supplemental / extra groups 'users' ...  
info: Adding user 'sarah' to group 'users' ...  
victor@victor-1-2:~$
```

```
victor@victor-1-2:~$  
victor@victor-1-2:~$  
victor@victor-1-2:~$ echo creating new group  
creating new group  
victor@victor-1-2:~$ sudo groupadd epita_users_AV  
victor@victor-1-2:~$  
victor@victor-1-2:~$  
victor@victor-1-2:~$  
victor@victor-1-2:~$  
victor@victor-1-2:~$  
victor@victor-1-2:~$  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV smith  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV sarah  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV emily  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV david  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV lisa  
victor@victor-1-2:~$  
victor@victor-1-2:~$
```

Figure 26 - adding users to epita_users_AV group

3. Creating a Directory and Adding Files:

- Created a directory named **epita_assets_AV** and created 5 files inside with the names code1, code2, tool1, tool2 and info1.
- Notice that currently only victor owns all the rights to the epita_assets_AV directory and all of it's files.

```
victor@victor-1-2:~$  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV smith  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV sarah  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV emily  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV david  
victor@victor-1-2:~$ sudo usermod -a -G epita_users_AV lisa  
victor@victor-1-2:~$  
victor@victor-1-2:~$ mkdir epita_assets_AV  
victor@victor-1-2:~$ cd epita_assets_AV/  
victor@victor-1-2:~/epita_assets_AV$ touch code1 code2 tool1 tool2 info1  
victor@victor-1-2:~/epita_assets_AV$ ls -la  
total 8  
drwxrwxr-x  2 victor victor 4096 Jan 21 18:19 .  
drwxr-x--- 19 victor victor 4096 Jan 21 18:17 ..  
-rw-rw-r--  1 victor victor   0 Jan 21 18:19 code1  
-rw-rw-r--  1 victor victor   0 Jan 21 18:19 code2  
-rw-rw-r--  1 victor victor   0 Jan 21 18:19 info1  
-rw-rw-r--  1 victor victor   0 Jan 21 18:19 tool1  
-rw-rw-r--  1 victor victor   0 Jan 21 18:19 tool2  
victor@victor-1-2:~/epita_assets_AV$  
victor@victor-1-2:~/epita_assets_AV$  
victor@victor-1-2:~/epita_assets_AV$
```

Figure 27 - new directory epita_assets_AV with victor owning all rights

4. Changing Group Ownership:

- Changed the group ownership of the **epita_assets_AV** directory and its contents to **epita_users_AV**
- Used the **ls -la** command to verify the ownership change, ensuring the directory and files were correctly associated with the group.


```

Jan 21 18:26
victor@victor-1-2: ~
victor@victor-1-2:~/epita_assets_AV$
victor@victor-1-2:~/epita_assets_AV$ cd ..
victor@victor-1-2:~$ sudo chgrp -R epita_users_AV epita_assets_AV/
victor@victor-1-2:~$ ls -la
total 180
drwxr-x--- 19 victor victor      4096 Jan 21 18:17 .
drwxr-xr-x  8 root   root       4096 Jan 21 18:09 ..
-rw-rw-r--  1 victor victor     1382 Jan 19 02:14 add_Users_to_Groups.txt
-rw-r--r--  1 root   root     23688 Dec 15 19:29 alago_backup.ldif
-rw-----  1 victor victor     3786 Jan 21 18:00 .bash_history
-rw-r--r--  1 victor victor       220 Jan  7  2023 .bash_logout
-rw-r--r--  1 victor victor     3771 Jan  7  2023 .bashrc
drwx----- 14 victor victor     4096 Nov 10 15:31 .cache
drwx----- 16 victor victor     4096 Jan 18 03:38 .config
-rw-rw-r--  1 victor victor     9933 Jan 17 02:22 corrected_modified_alago.ldif
-rw-rw-r--  1 victor victor        85 Nov 24 19:08 deleteACL.ldif
drwxr-xr-x  2 victor victor     4096 Nov  9 23:53 Desktop
drwxr-xr-x  2 victor victor     4096 Nov  9 23:53 Documents
drwxr-xr-x  3 victor victor     4096 Jan 20 23:24 Downloads
drwxrwxr-x  2 victor epita_users_AV 4096 Jan 21 18:19 epita_assets_AV
drwx-----  2 victor victor     4096 Nov 19 20:09 .gnupg
-rw-----  1 victor victor        20 Jan 21 01:25 .lesshtst
drwx-----  4 victor victor     4096 Nov  9 23:53 .local
-rw-rw-r--  1 victor victor        75 Nov 10 05:58 logEnable.ldif
drwx-----  3 victor victor     4096 Nov 10 15:31 .mozilla
drwxr-xr-x  2 victor victor     4096 Nov  9 23:53 Music
-rw-rw-r--  1 victor victor    9167 Jan 17 01:16 MyCompany_alago.ldif
-rw-rw-r--  1 victor victor     145 Nov 24 18:59 newACLRule.ldif
-rw-rw-r--  1 victor victor     121 Nov 24 20:30 newpassword.ldif
drwxr-xr-x  3 victor victor     4096 Nov 10 02:20 Pictures
-rw-r--r--  1 victor victor     807 Jan  7  2023 .profile
drwxr-xr-x  2 victor victor     4096 Nov  9 23:53 Public
drwx-----  7 victor victor     4096 Nov 10 15:32 snap

```

Figure 28 - changing ownership to epita_users_AV

```

-rw-rw-r--  1 victor victor     8489 Jan 19 01:48 users_alago.ldif
drwxr-xr-x  2 victor victor     4096 Nov  9 23:53 Videos
-rw-----  1 victor victor     1885 Nov 10 06:21 .viminfo
victor@victor-1-2:~$ cd epita_assets_AV/
victor@victor-1-2:~/epita_assets_AV$ ls -la
total 8
drwxrwxr-x  2 victor epita_users_AV 4096 Jan 21 18:19 .
drwxr-x--- 19 victor victor      4096 Jan 21 18:17 ..
-rw-rw-r--  1 victor epita_users_AV   0 Jan 21 18:19 code1
-rw-rw-r--  1 victor epita_users_AV   0 Jan 21 18:19 code2
-rw-rw-r--  1 victor epita_users_AV   0 Jan 21 18:19 info1
-rw-rw-r--  1 victor epita_users_AV   0 Jan 21 18:19 tool1
-rw-rw-r--  1 victor epita_users_AV   0 Jan 21 18:19 tool2
victor@victor-1-2:~/epita_assets_AV$

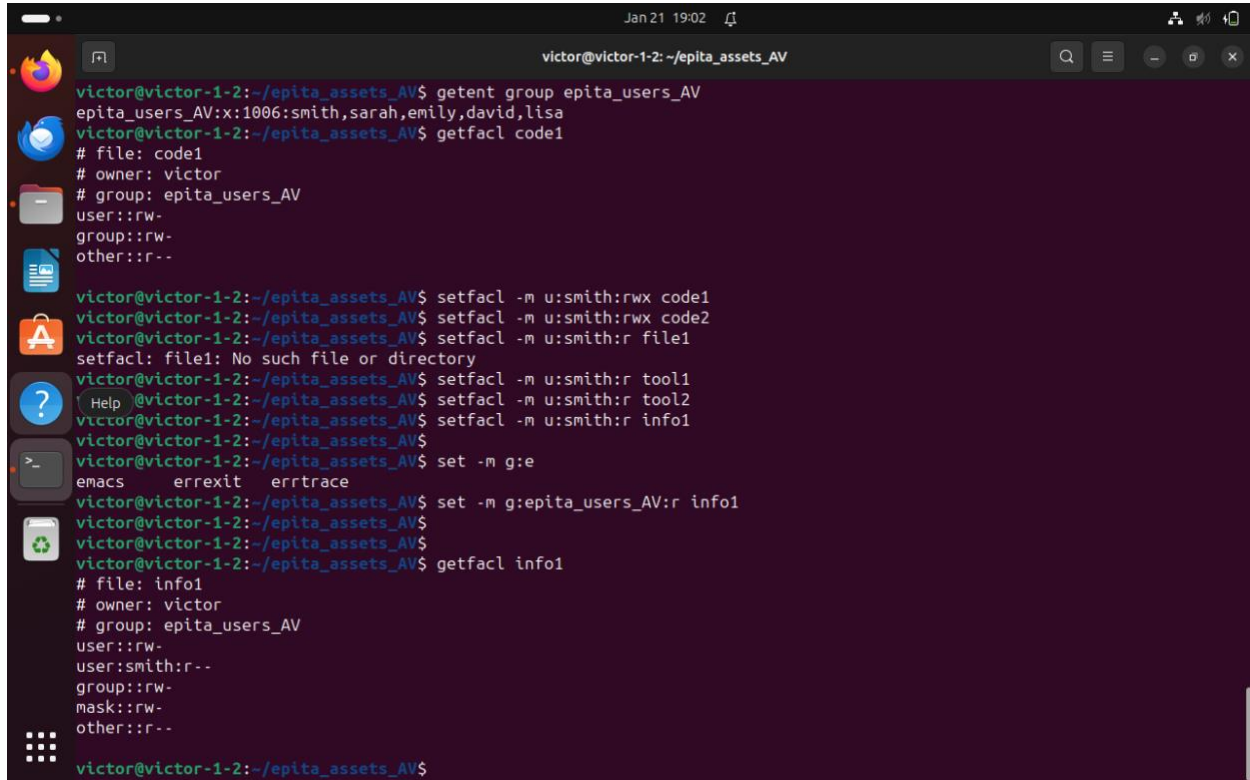
```

Figure 29 - more evidence, victor and epita_users_AV now have rights

5. Assigning Access Rights via setfacl:

- Utilized **setfacl** to assign access rights to the files in the **epita_assets_AV** directory.
- Restricted access to certain permissions (read, write, execute) for users in the **epita_users_AV** group, demonstrating a practical application of discretionary access control.

- For example, I gave the user smith rwx (read, write and execute) rights to code1 and code2 while I gave him only read access to the other files tool1, tool2 and info1.



```

victor@victor-1-2: ~/epita_assets_AV
victor@victor-1-2:~/epita_assets_AV$ getent group epita_users_AV
epita_users_AV:x:1006:smith,sarah,emily,david,lisa
victor@victor-1-2:~/epita_assets_AV$ getfacl code1
# file: code1
# owner: victor
# group: epita_users_AV
user::rw-
group::rw-
other::r--

victor@victor-1-2:~/epita_assets_AV$ setfacl -m u:smith:rwx code1
victor@victor-1-2:~/epita_assets_AV$ setfacl -m u:smith:rwx code2
victor@victor-1-2:~/epita_assets_AV$ setfacl -m u:smith:r file1
setfacl: file1: No such file or directory
victor@victor-1-2:~/epita_assets_AV$ setfacl -m u:smith:r tool1
victor@victor-1-2:~/epita_assets_AV$ setfacl -m u:smith:r tool2
victor@victor-1-2:~/epita_assets_AV$ setfacl -m u:smith:r info1
victor@victor-1-2:~/epita_assets_AV$ set -m g:e
emacs  errexit  errtrace
victor@victor-1-2:~/epita_assets_AV$ set -m g:epita_users_AV:r info1
victor@victor-1-2:~/epita_assets_AV$
victor@victor-1-2:~/epita_assets_AV$
victor@victor-1-2:~/epita_assets_AV$ getfacl info1
# file: info1
# owner: victor
# group: epita_users_AV
user::rw-
user:smith:r--
group::rw-
mask::rw-
other::r--
victor@victor-1-2:~/epita_assets_AV$

```

Figure 30 - using setfacl to assign rights particularly for John Smith

6. Explanation of Access Control Models:

- **MAC (Mandatory Access Control):** This is a strict access control model where access rights are regulated by a central authority based on multiple levels of security. The user cannot modify the access controls; they are set and enforced by a system administrator.

Advantages: Highly secure due to its rigid structure. Prevents users from making unauthorized changes to access controls.

Limitations: Can be inflexible and may not be user-friendly in environments where quick changes in access rights are needed.

- **DAC (Discretionary Access Control):** In this model, the owner of the resource (file or directory) controls who has access to it. Users have discretion over their own resources. Users with certain permissions, such as file owners, can grant or restrict access to those resources to other users.

Advantages: Provides flexibility and ease of use, suitable for many commercial applications.

Limitations: Greater risk of data leakage or unauthorized access, as users might not always follow the best security practices.

- **RBAC (Role-Based Access Control):** Access decisions are based on the roles that users have within the system and the permissions attached to these roles. For example, a role like 'Manager' might have different access rights than a 'Technician'.

Advantages: Reduces the complexity of access management, especially in larger organizations. It allows for easy modification of user roles without the need to reconfigure access rights for each user individually.

Limitations: Less granular control compared to DAC; roles must be well-defined and managed to ensure proper access rights are granted.

Which Model Fits the Implementation in Step 5?:

- The implementation in step 5 aligns with **Discretionary Access Control (DAC)**. This is because the resource owner (me, in this case ie victor) is setting specific permissions on files and directories for certain users or groups. DAC allows users to grant and revoke access to their resources, which is what's being done with **setfacl**.

Conclusion

This exercise showcased the practical application of access control mechanisms in a Linux environment. By creating groups, managing resources, and setting specific permissions, it highlighted the significance of understanding and implementing appropriate access controls in system administration. This hands-on experience underlines the importance of access control in securing and managing resources effectively in an IT infrastructure.

Concluding Reflections on My Enterprise Networks Course Experience

As I conclude this project report, I find myself reflecting on the comprehensive and enlightening journey I have undertaken through the Enterprise Networks course. This educational voyage has not only expanded my understanding of network infrastructures but has also significantly enhanced my practical skills in managing and securing enterprise networks.

The series of exercises, from LDAP installations to the implementation of access control models, served as a real-world application of theoretical concepts. They provided valuable insights into the complexities and nuances of network administration. Through these hands-on experiences, I have gained a deeper appreciation for the meticulous planning, attention to detail, and the strategic foresight required in network management.

One of the most significant takeaways from this course is the critical role of security in network management. Implementing ACLs and managing user access privileges underscored the delicate balance between accessibility and security. This has instilled in me a heightened sense of responsibility and a keen awareness of the implications of every decision in the realm of network security.

Furthermore, the course has reinforced the importance of continuous learning and adaptability in this ever-evolving field. Staying abreast of emerging technologies and trends is not just an academic requirement but a professional necessity. The skills and knowledge I have acquired are a solid foundation, but I recognize that they are just the starting point in a lifelong journey of learning and growth in network administration.

As I move forward in my career, the experiences and lessons from this course will be invaluable. They have shaped my approach to network management and security, preparing me for the challenges and opportunities that lie ahead in the dynamic and essential field of enterprise networks.

In summary, this course has been a transformative experience, equipping me with both theoretical knowledge and practical expertise. I am eager to apply these learnings in my professional life, contributing to the development and management of robust, efficient, and secure network infrastructures.

Thank you.