LFCS: Users and Groups (10%)

This document covers user and group management, environment profiles, ACLs, resource limits, and LDAP integration.

Goals Coverage

Users and Groups 10%

1. Create and manage local user and group accounts
2. Manage personal and system-wide environment profiles
3. Configure user resource limits
4. Configure and manage ACLs
5. Configure the system to use LDAP user and group accounts

---

1. Create and Manage Local User Accounts

Learn

- Add, modify, and delete local users.
- Manage home directories and shells.

Commands

```
# Add user
sudo useradd -m -s /bin/bash username
sudo passwd username

# Modify user
sudo usermod -aG sudo username   # Add to group
sudo usermod -d /new/home username  # Change home directory

# Delete user
sudo userdel -r username   # Delete user and home directory
```

Exercises

1. Create a user with home directory and bash shell.
2. Add the user to the sudo group.
3. Remove a test user.

---

2. Create and Manage Groups

Learn

- Create, modify, and delete groups.
- Assign users to groups.

Commands

```
# Create group
sudo groupadd developers

# Modify group
sudo gpasswd -a username developers

# Delete group
sudo groupdel developers
```

```
# List groups
groups username
```

Exercises

1. Create a group `admins` and add a user.
2. Verify the user is part of the group.
3. Delete the group.

---

3. Manage Environment Profiles

Learn

- System-wide vs user-specific profiles.
- Configure PATH, variables, and shell startup files.

Commands

```
# Edit system-wide profile
sudo nano /etc/profile
sudo nano /etc/bash.bashrc

# Edit user profile
nano ~/.bashrc
source ~/.bashrc  # Reload changes
```

Exercises

1. Add a directory to PATH in `.bashrc` and reload.
2. Set a custom environment variable system-wide.

---

4. Configure User Resource Limits

Learn

- Use `ulimit` and `/etc/security/limits.conf` for limits on processes, open files, and memory.

Commands

```
# Temporary limit
ulimit -n 4096

# Persistent limit
sudo nano /etc/security/limits.conf
# user soft nofile 4096
# user hard nofile 8192
```

Exercises

1. Increase the maximum number of open files for a user.
2. Verify limits with `ulimit -a`.

---

5. Configure and Manage ACLs (Access Control Lists)

Learn

- Set fine-grained permissions beyond standard Unix mode bits.
- Commands: `getfacl` and `setfacl`.

Commands

```
# Check ACL
getfacl /path/to/file
```

```
# Set ACL for user
setfacl -m u:username:rwx /path/to/file

# Remove ACL
setfacl -x u:username /path/to/file
```

Exercises

1. Give read/write access to a specific file for a user without changing group ownership.
2. Remove the ACL and verify permissions.

---

6. Configure the System to Use LDAP for Users and Groups

Learn

- Integrate Linux system with LDAP server for centralized authentication.
- Configure NSS and PAM.

Commands

```
# Install LDAP client
sudo apt install libnss-ldap libpam-ldap ldap-utils

# Configure /etc/nsswitch.conf
sudo nano /etc/nsswitch.conf
# passwd: files ldap
group: files ldap
shadow: files ldap

# Test LDAP user
getent passwd ldapuser
id ldapuser
```

Exercises

1. Connect a Linux system to an LDAP server.
2. Verify that LDAP users can login.

Exam Tips

- Practice creating users and groups both locally and via LDAP.
- Understand persistent vs temporary environment variable settings.
- Familiarize with ACL commands for fine-grained permission control.

Revision #2
Created 2025-11-07 10:39:11 UTC by Loïc
Updated 2025-11-07 14:28:26 UTC by Loïc