LINUX SERVER ADMINISTRATOR EXAM REPORT

Full Name	Nikhil Patidar
Email ID	nikhilpatidar132@gmail.com
Mobile No.	7489306252
Date	08 June 2025

Exam Question

An institute looking to establish a secure and efficient Linux server environment for database management must follow several key steps. Begin by setting up an LDAP server to centralize user authentication. Then, deploy PostgreSQL with LDAP-based authentication to ensure secure database access. Next, configure Joomla to be securely accessible over HTTPS on port 443 using a designated domain name. Additionally, implement a file-sharing service to manage user home directories via FTP with LDAP authentication, and set up an SSH server to authenticate users through LDAP.

Server and Client User and Password

Role	User	Password
LDAP Server	root	Root
LDAP User	Nikhil	-------@123
SSH User	Nikhil	-------@123
Client	root	Root
Client User	Patidar	123
Joomla Admin	admin	-------@123456

Server and Client User and Password

SERVER DETAILS	
OS	Debian 12
IPv4	192.168.169.130
Hostname	ns.armour.local
Domain	armour.local, ns.armour.local www.armour.local
CLIENT DETAILS	
OS	Debian 12
IPv4	192.168.169.132
Hostname	cn.client.local
Domain	client.local cn.client.local

LDAP SERVER Basic Configuration

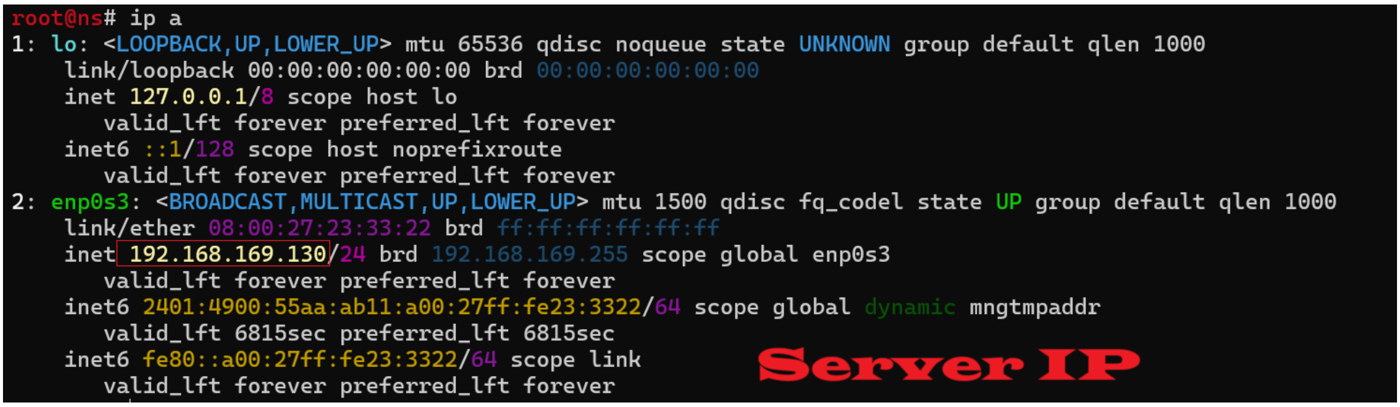
Machine Name Debian for Exam Linux

Set IP and Gateway

nano /etc/network/interfaces

ip 192.168.169.130

gateway 192.168.169.135



```
root@ns# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:23:33:22 brd ff:ff:ff:ff:ff:ff
    inet 192.168.169.130/24 brd 192.168.169.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 2401:4900:55aa:ab11:a00:27ff:fe23:3322/64 scope global dynamic mngtmpaddr
       valid_lft 6815sec preferred_lft 6815sec
    inet6 fe80::a00:27ff:fe23:3322/64 scope link
       valid_lft forever preferred_lft forever
```

Server IP

Hostname Name Set on Ldap Server Site
hostnamectl set-hostname ns.armour.local
reboot

Check
hostname
ns.armour.local

vim /etc/resolv.conf
# Add this line
nameserver 8.8.8.8
nameserver 8.8.4.4

Disable IPv6
vim /etc/sysctl.conf

# Add this Line
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1

Apply Changes Immediaelty
sysctl -p

DEBIAN CLIENT Basic Configuration

Machine Name Debian Client for Exam Linux

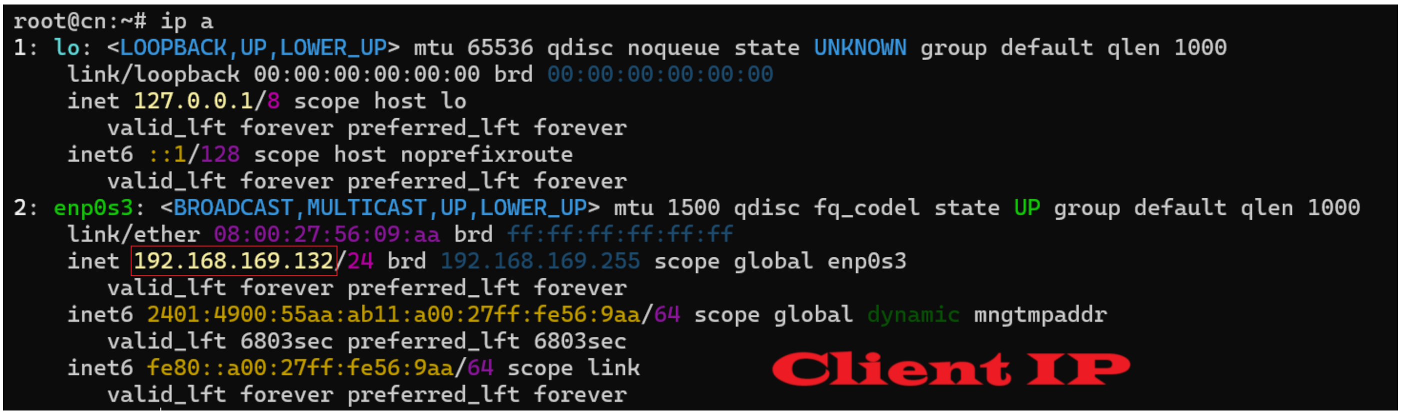
Root Credentials :

- **Username :** root
- **Password :** root

User Credentials:

- **Username:** patidar
- **Password:** 123

Set IP and Gateway
vim /etc/network/interfaces
ip 192.168.169.132
gateway 192.168.169.135



```
root@cn:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:56:09:aa brd ff:ff:ff:ff:ff:ff
    inet 192.168.169.132/24 brd 192.168.169.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 2401:4900:55aa:ab11:a00:27ff:fe56:9aa/64 scope global dynamic mngtmpaddr
       valid_lft 6803sec preferred_lft 6803sec
    inet6 fe80::a00:27ff:fe56:9aa/64 scope link
       valid_lft forever preferred_lft forever
```

Hostname Name Set on Client Site

hostnamectl set-hostname cn.client.local

reboot

Check hostname

cn.client.local

vim /etc/resolv.conf

# Add this line

nameserver 192.168.169.130 //LDAP Server IP

nameserver 8.8.8.8

Disable IPv6

vim /etc/sysctl.conf

#Add this Line

net.ipv6.conf.all.disable_ipv6 = 1

net.ipv6.conf.default.disable_ipv6 = 1

net.ipv6.conf.lo.disable_ipv6 = 1

Apply Changes Immediaelty

sysctl -p

Ldap Server site Configuration

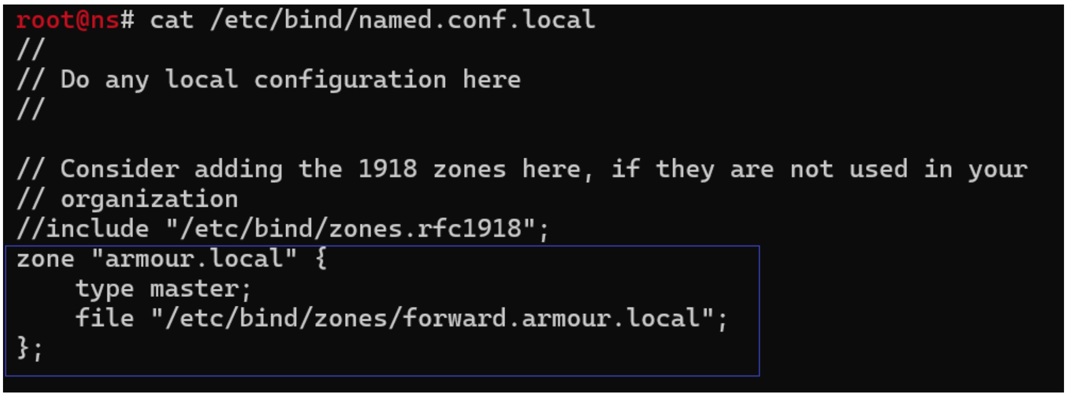
1. Configuration of DNS (Domain Name System)

Step -1. Install DNS Required Packages

apt install bind9 dnsutils

Step -2. Create Zone

vim /etc/bind/named.conf.local



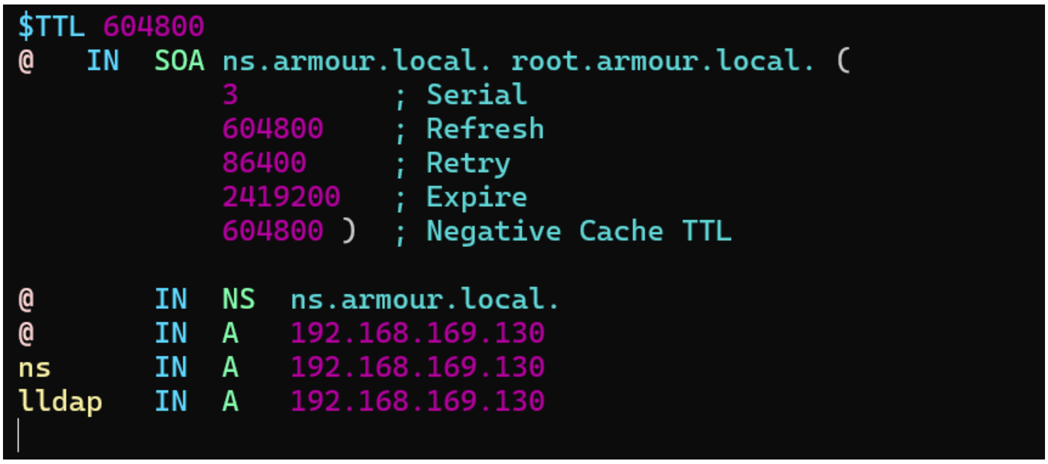
```
root@ns# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "armour.local" {
    type master;
    file "/etc/bind/zones/forward.armour.local";
};
```

Step-3. Create Forward Zone Records

mkdir /etc/bind/zones

vim /etc/bind/zones/forward.server.local



```
$TTL 604800
@   IN  SOA ns.armour.local. root.armour.local. (
            3          ; Serial
            604800     ; Refresh
            86400      ; Retry
            2419200    ; Expire
            604800 )   ; Negative Cache TTL

@       IN  NS   ns.armour.local.
@       IN  A    192.168.169.130
ns      IN  A    192.168.169.130
lldap   IN  A    192.168.169.130
```

named-checkzone armour.local /etc/bind/zones/forward.armour.local

Step -4. Update Hosts

vim /etc/hosts

192.168.169.130 armour.local ns.armour.local ldap.armour.local

Step-5. Restart DNS Services

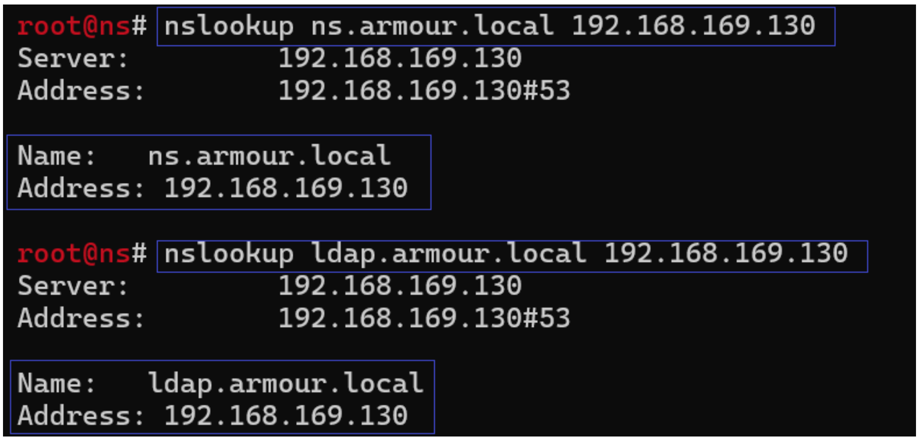
systemctl restart bind9

systemctl enable named.service

Step-6. Verify Domain Resolution

nslookup server.local 192.168.169.130

nslookup ldap.server.local 192.168.169.130



```
root@ns# nslookup ns.armour.local 192.168.169.130
Server:         192.168.169.130
Address:        192.168.169.130#53

Name:   ns.armour.local
Address: 192.168.169.130

root@ns# nslookup ldap.armour.local 192.168.169.130
Server:         192.168.169.130
Address:        192.168.169.130#53

Name:   ldap.armour.local
Address: 192.168.169.130
```

LDAP (Lightweight Directory Access Protocol) Server Configuration.

Step-1. Package Install

apt install slapd ldap-utils

Administrator Password Set -------@123

Step-2. Reconfigure LDAP

Answer the prompts:

- Omit OpenLDAP server configuration? → No
- DNS Domain Name → armour.local
- Organization name → armour
- Administrator Password → -------@123
- Confirm Password → -------@123
- Do you want the database removed when slapd is purged? → No
- Move old database? → Yes

Step-3. Edit /etc/ldap/ldap.conf

vim /etc/ldap/ldap.conf

# Add this line

BASE dc=armour, dc=local

URI ldap://ldap.armour.loca

Check LDAP Configuration Checks

- ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn
- ldapsearch -x -LLL -H ldap:/// -b dc=armour, dc=local dn
- ldapwhoami –x
- ldapwhoami -x -D cn=admin,dc=armour,dc=local –W
- ldapwhoami -Y EXTERNAL -H ldapi:/// -Q

Step -4. Create LDAP User

Genrate Hashed Password

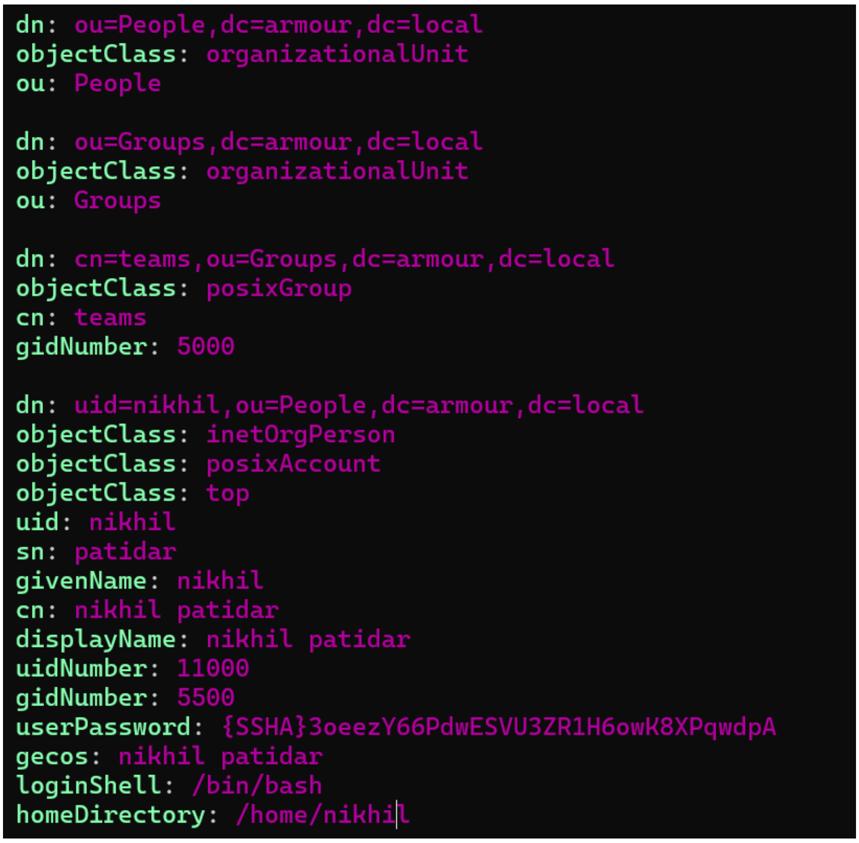
slappasswd

{SSHA}3oeezY66PdwESVU3ZR1H6owK8XPqwdpA (-------@123)

vim users.ldif

add user and groups to LDAP

ldapadd -x -D cn=admin,dc=armour,dc=local -W -f users.ldif



```
dn: ou=People,dc=armour,dc=local
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=armour,dc=local
objectClass: organizationalUnit
ou: Groups

dn: cn=teams,ou=Groups,dc=armour,dc=local
objectClass: posixGroup
cn: teams
gidNumber: 5000

dn: uid=nikhil,ou=People,dc=armour,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: nikhil
sn: patidar
givenName: nikhil
cn: nikhil patidar
displayName: nikhil patidar
uidNumber: 11000
gidNumber: 5500
userPassword: {SSHA}3oeezY66PdwESVU3ZR1H6owK8XPqwdpA
gecos: nikhil patidar
loginShell: /bin/bash
homeDirectory: /home/nikhil
```

Verify

ldapsearch -x -LLL -b dc=armour,dc=local '(uid=nikhil)' cn gidNumber

Step-5. Edit PAM Auth File

vim /etc/pam.d/common-auth

# Add this line

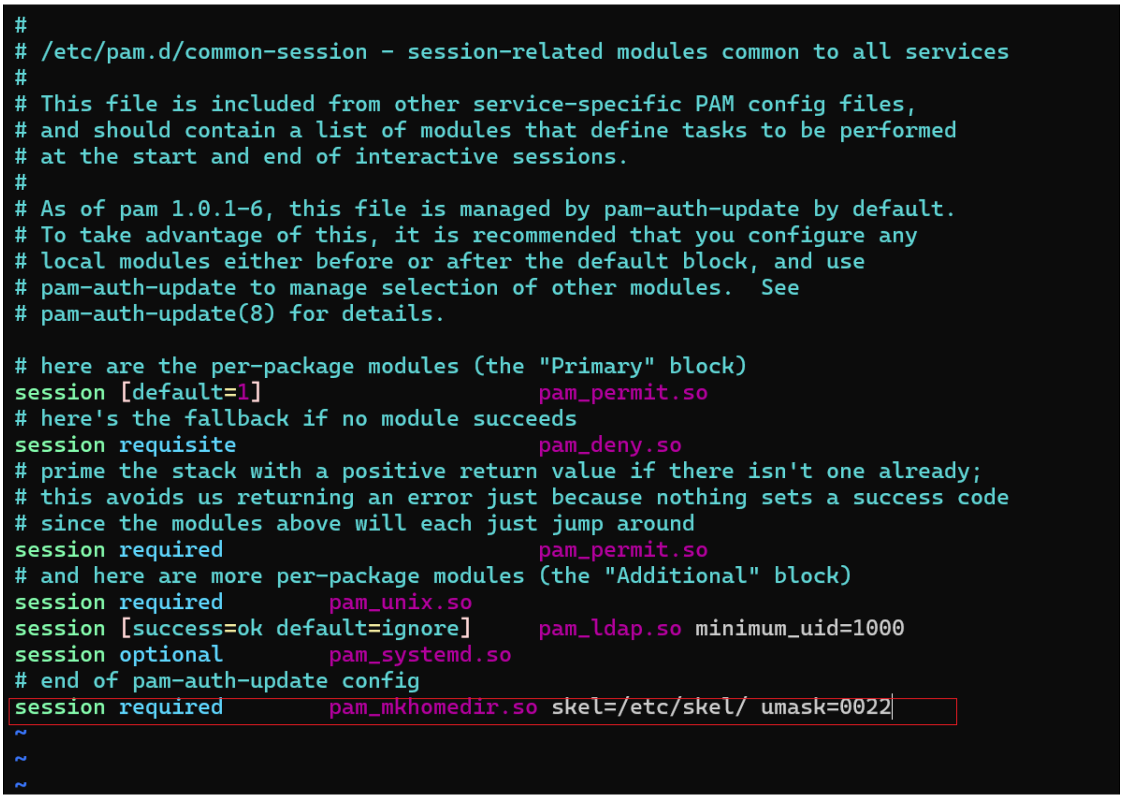
auth sufficient pam_ldap.so

# Enable Home directory creatioin

vim /etc/pam.d/common-session

add this line

session required pam_mkhomedir.so skel=/etc/skel/ umask=0022



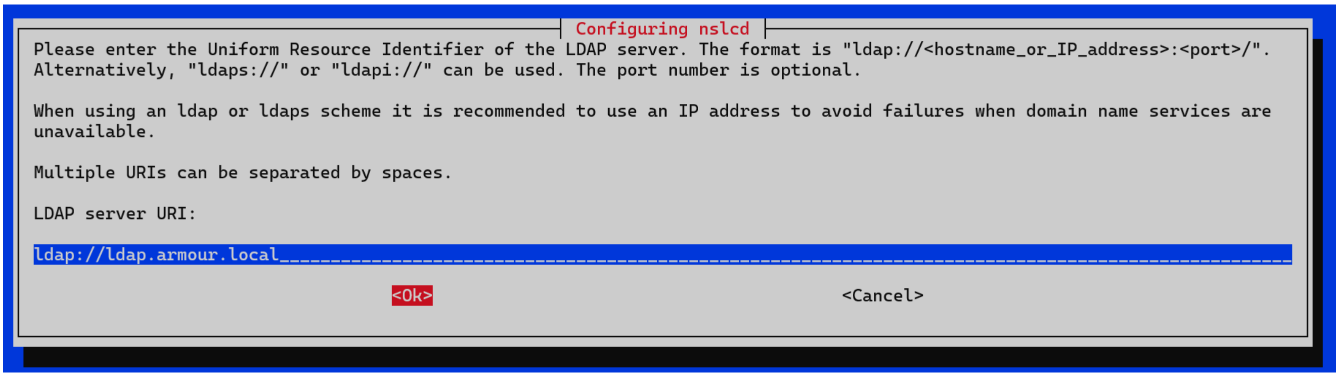
```
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]                     pam_permit.so
# here's the fallback if no module succeeds
session requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session [success=ok default=ignore]     pam_ldap.so minimum_uid=1000
session optional        pam_systemd.so
# end of pam-auth-update config
session required        pam_mkhomedir.so skel=/etc/skel/ umask=0022
~
~
~
```

Step-6. Install LDAP PAM Packages

apt install nslcd libpam-ldapd

- LDAP server URI: ldap://ldap.armour.local
- LDAP server search base: dc=armour,dc=local
- Name service to configure: select passwd, group, shadow



Configuring nslcd

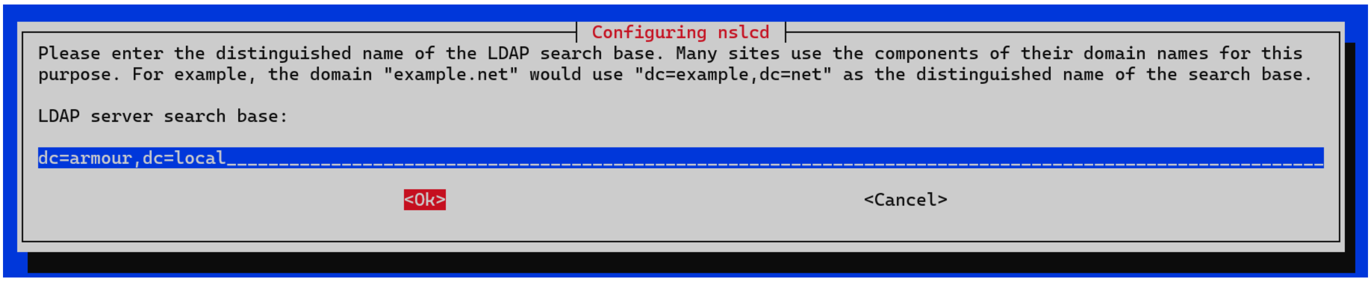
Please enter the Uniform Resource Identifier of the LDAP server. The format is "ldap://<hostname_or_IP_address>:<port>/". Alternatively, "ldaps://" or "ldapi://" can be used. The port number is optional.

When using an ldap or ldaps scheme it is recommended to use an IP address to avoid failures when domain name services are unavailable.

Multiple URIs can be separated by spaces.

LDAP server URI:

ldap://ldap.armour.local



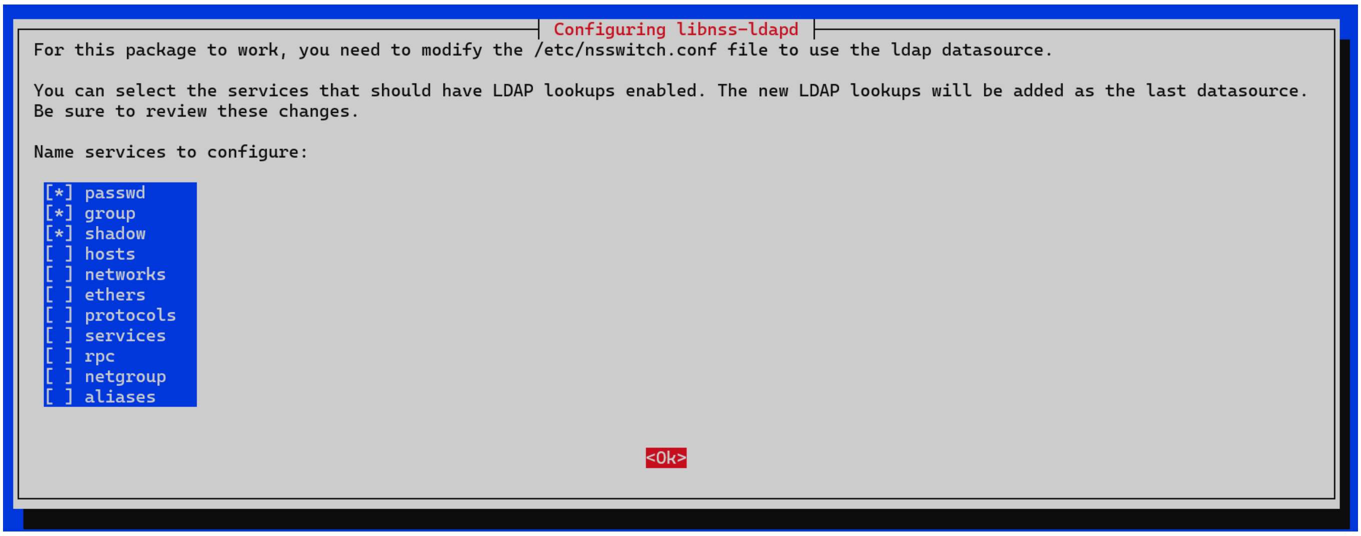
```
Configuring nslcd

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this
purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

LDAP server search base:

dc=armour,dc=local_______________________________________________________________________________________________

                      <Ok>                                                <Cancel>
```



```
Configuring libnss-ldapd

For this package to work, you need to modify the /etc/nsswitch.conf file to use the ldap datasource.

You can select the services that should have LDAP lookups enabled. The new LDAP lookups will be added as the last datasource.
Be sure to review these changes.

Name services to configure:

 [*] passwd
 [*] group
 [*] shadow
 [ ] hosts
 [ ] networks
 [ ] ethers
 [ ] protocols
 [ ] services
 [ ] rpc
 [ ] netgroup
 [ ] aliases

                                          <Ok>
```

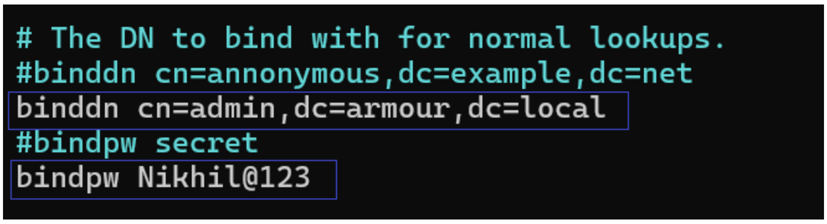
Step-7. Add Admin

vim /etc/nslcd.conf

# Add this line

binddn cn=admin,dc=armour,dc=local

bindpw -------@123



```
# The DN to bind with for normal lookups.
#binddn cn=annonymous,dc=example,dc=net
binddn cn=admin,dc=armour,dc=local
#bindpw secret
bindpw Nikhil@123
```

systemctl restart nslcd.service

getent passwd nikhil

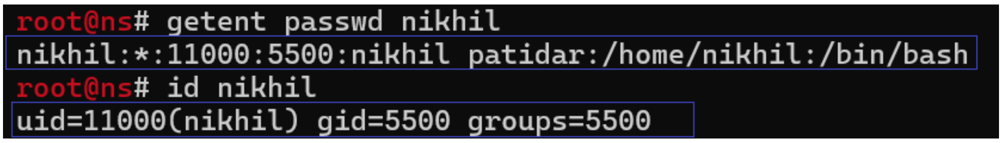
# Output

nikhil:*:11000:5500:nikhil patidar:/home/nikhil:/bin/bash

id nikhil

# Output

uid=11000(nikhil) gid=5500 groups=5500



```
root@ns# getent passwd nikhil
nikhil:*:11000:5500:nikhil patidar:/home/nikhil:/bin/bash
root@ns# id nikhil
uid=11000(nikhil) gid=5500 groups=5500
```

LDAP Client Configuration

Step-1. Install Packages on Client

apt install libnss-ldapd libpam-ldapd ldap-utils

Installation Prompts:

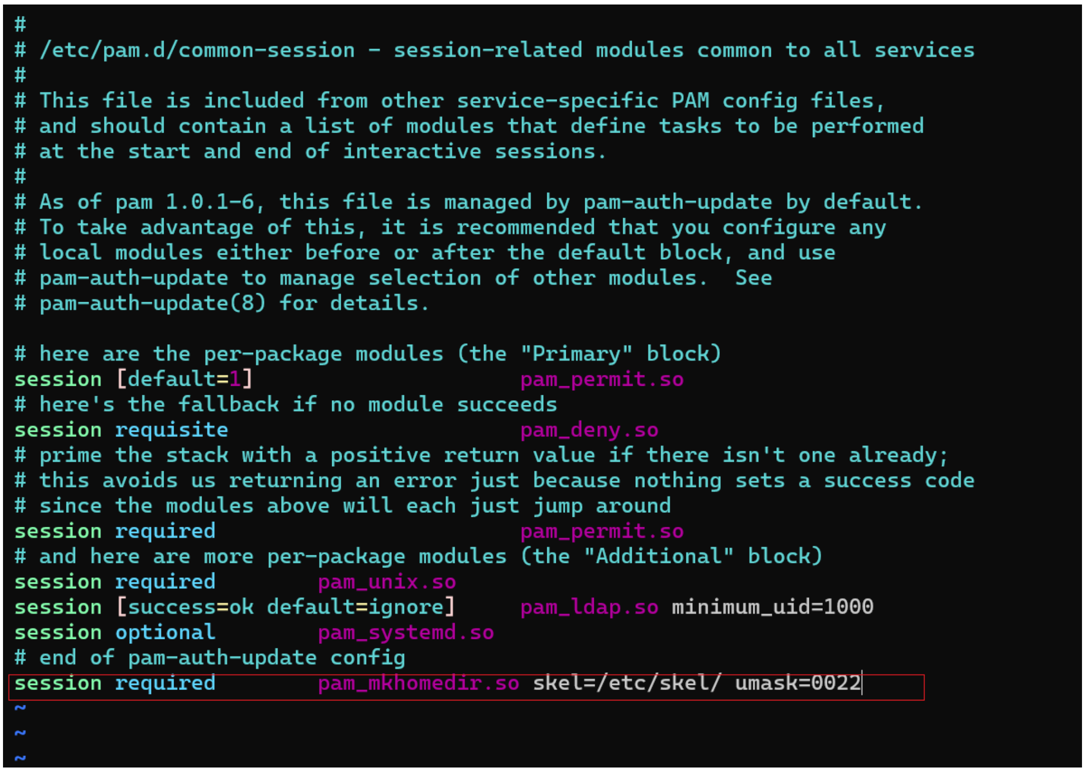
- LDAP server URI: ldap://ldap.armour.local
- LDAP search base: dc=armour,dc=local
- Name service to configure: Select → passwd, group, shadow

Step-2. Home Directory Create and Enable

vim /etc/pam.d/common-session

# Add this Line

session required pam_mkhomedir.so skel=/etc/skel/ umask=0022



```
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]                     pam_permit.so
# here's the fallback if no module succeeds
session requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session [success=ok default=ignore]     pam_ldap.so minimum_uid=1000
session optional        pam_systemd.so
# end of pam-auth-update config
session required        pam_mkhomedir.so skel=/etc/skel/ umask=0022
~
~
~
```

# LDAP User Test Login

su – nikhil

SSH Access for LDAP Users

Step-1. Edit SSH Configuration

vim /etc/ssh/sshd_config

Set to YES

UsePAM yes

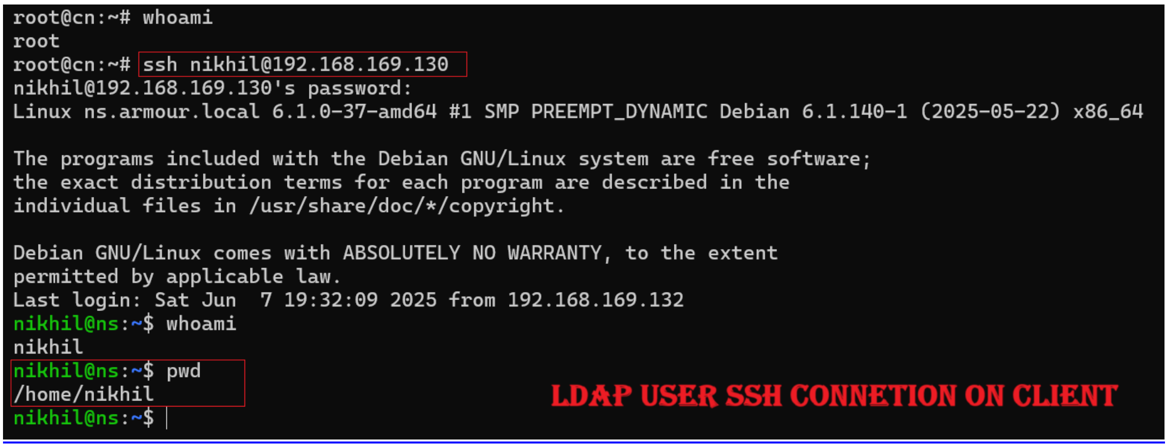
Step-2. Restart SSH Service Both Server and Client

systemctl restart sshd

Step-3. SSH into Server Using LDAP User

From Client Machine site

ssh nikhil@192.168.169.130



```
root@cn:~# whoami
root
root@cn:~# ssh nikhil@192.168.169.130
nikhil@192.168.169.130's password:
Linux ns.armour.local 6.1.0-37-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.140-1 (2025-05-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jun  7 19:32:09 2025 from 192.168.169.132
nikhil@ns:~$ whoami
nikhil
nikhil@ns:~$ pwd
/home/nikhil
nikhil@ns:~$
```

LDAP USER SSH CONNETION ON CLIENT

FTP Server Configuration with LDAP Intergration

Step-1. Install FTP Packages on Server

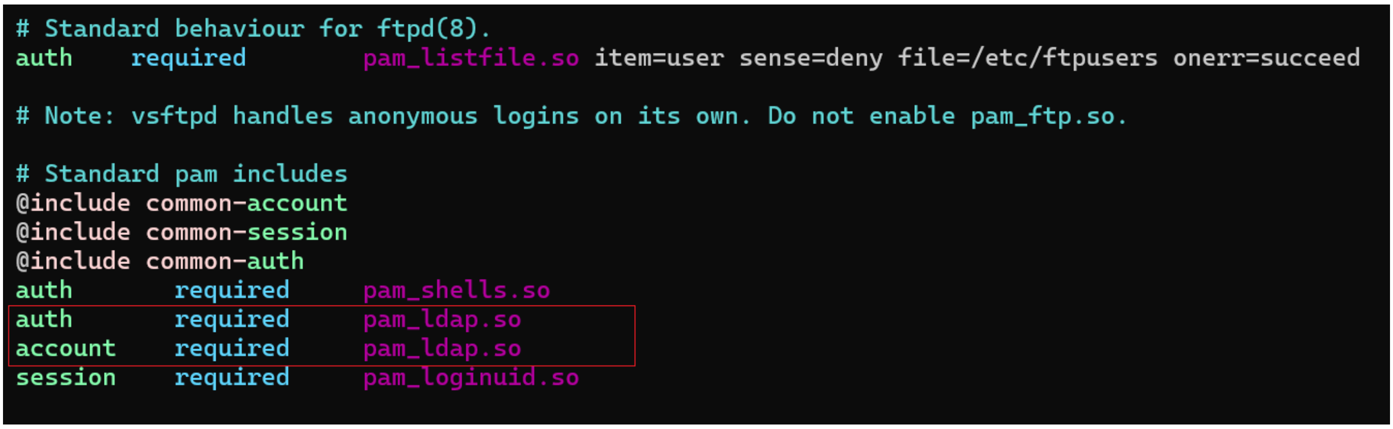
apt install vsftpd

Step.2. Configure PAM for vsftpd Authentication

vim /etc/pam.d/vsftpd

# Add this Lines

- auth required pam_ldap.so
- account required pam_ldap.so
- session required pam_loginuid.so



```
# Standard behaviour for ftpd(8).
auth    required        pam_listfile.so item=user sense=deny file=/etc/ftpusers onerr=succeed

# Note: vsftpd handles anonymous logins on its own. Do not enable pam_ftp.so.

# Standard pam includes
@include common-account
@include common-session
@include common-auth
auth        required    pam_shells.so
auth        required    pam_ldap.so
account     required    pam_ldap.so
session     required    pam_loginuid.so
```

# Explanation:

- **auth required pam_ldap.so** — Uses LDAP for user authentication.
- **account required pam_ldap.so** — Verifies account details via LDAP.
- **session required pam_loginuid.so** — Manages session logging.

Step-3. FTP Server Main File Configuration

vim /etc/vsftpd.conf

# Ensure the following Settings

- local_enable=YES
- write_enable=YES
- pam_service_name=vsftpd

# Explanation:

- local_enable=YES — Allows local (LDAP-authenticated) users to login.
- write_enable=YES — Allows users to upload, modify, and delete files.
- pam_service_name=vsftpd — Uses /etc/pam.d/vsftpd for authentication.

Step-4. Restart the FTP Service

systemctl restart vsftpd

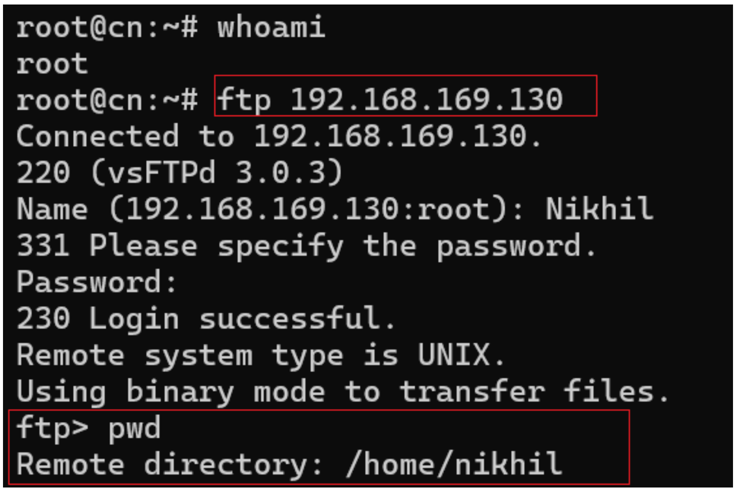
Step-5. Install FTP Client Tool on Both Server and Client

apt install ftp

Step-6. Connet to FTP Server as LDAP User (Client Machine Side)

ftp 192.168.169.130

- **LDAP User** –Nikhil
- **Password**- -------@123



```
root@cn:~# whoami
root
root@cn:~# ftp 192.168.169.130
Connected to 192.168.169.130.
220 (vsFTPd 3.0.3)
Name (192.168.169.130:root): Nikhil
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/nikhil
```

PostgreSQL Installation and Configuration

Step-1. Install PostgreSQL

apt update
apt install postgresql postgresql-contrib

Step-2. Check PostgreSQL Service

systemctl status postgresql

Step-3. Configure LDAP Authentication

vim /etc/postgresql/*/main/pg_hba.conf

# Add this line at the bottom

host all all 0.0.0.0/0 ldap ldapserver=192.168.169.130 ldapbasedn="ou=People,dc=armour,dc=local"

Step-4. Allow External Connections

vim /etc/postgresql/*/main/postgresql.conf

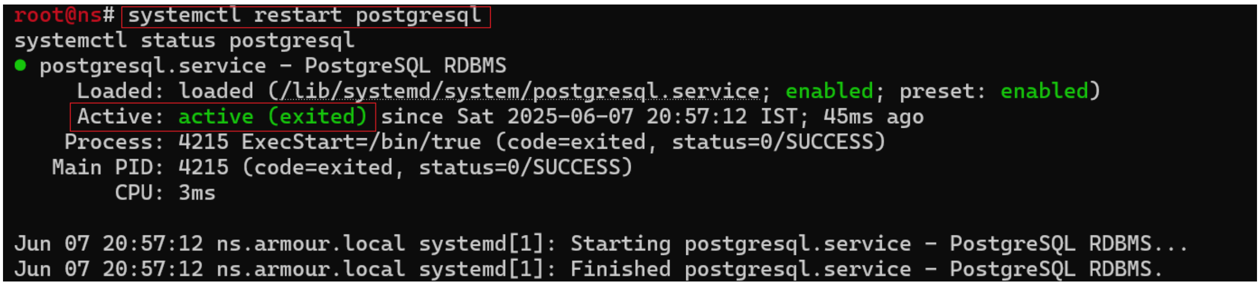
#Uncomment and set:

listen_addresses = '*'

Step-5. Restart and Verify Postgresql Services

systemctl restart postgresql

systemctl status postgresql

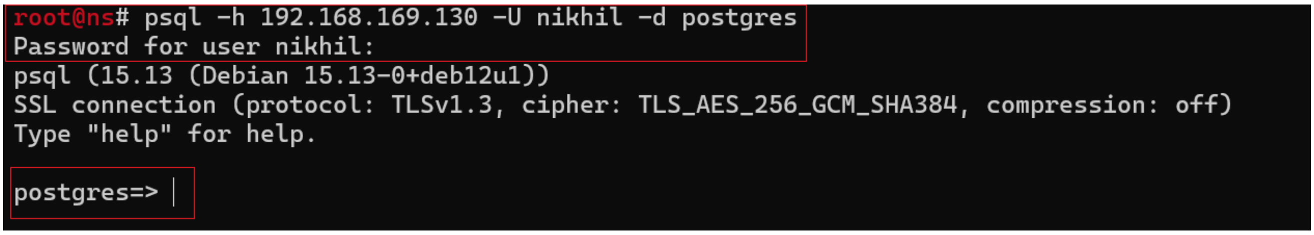


```
root@ns# systemctl restart postgresql
systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; preset: enabled)
     Active: active (exited) since Sat 2025-06-07 20:57:12 IST; 45ms ago
    Process: 4215 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 4215 (code=exited, status=0/SUCCESS)
        CPU: 3ms

Jun 07 20:57:12 ns.armour.local systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Jun 07 20:57:12 ns.armour.local systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
```

Step-6. Connect to PostgreSQL via LDAP user

psql -h 192.168.169.130 -U nikhil -d postgres



```
root@ns# psql -h 192.168.169.130 -U nikhil -d postgres
Password for user nikhil:
psql (15.13 (Debian 15.13-0+deb12u1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

postgres=>
```

PostgreSQL Basic Commands

S.No	Command	Description
1	su – postgres	Access the PostgreSQL system user shell.
2	Psql	Start the PostgreSQL interactive terminal (psql).
3	\l	List all PostgreSQL databases.
4	\c dbname	Connect to a specific database.
5	\du	List all roles and their privileges.
6	\q	Quit the PostgreSQL terminal.
7	\dt	List all tables in the current database.
8	CREATE TABLE tablename (...);	Create a new table.
9	INSERT INTO tablename (...) VALUES (...);	nsert data into a table.
10	SELECT * FROM tablename;	View all data from a table.

Joomla Installation with HTTPS (Post 443)

Step-1. Install Required Packages

```
apt update
apt install apache2 php php-mysql php-ldap php-xml php-mbstring php-zip php-curl libapache2-mod-php mariadb-server unzip
apt install php-pgsql
```

Step-2. Restart Apache2

```
systemctl restart apache2
```

Step-3. Download and Etract Joomla

```
cd /var/www/html
mkdir joomla
cd joomla
wget https://downloads.joomla.org/cms/joomla5/5-3-1/Joomla_5-3-1-Stable-Full_Package.zip
unzip Joomla_5-3-1-Stable-Full_Package.zip
chown -R www-data:www-data /var/www/html/joomla
```

Step-4. Create SSL Certificate for Joomla

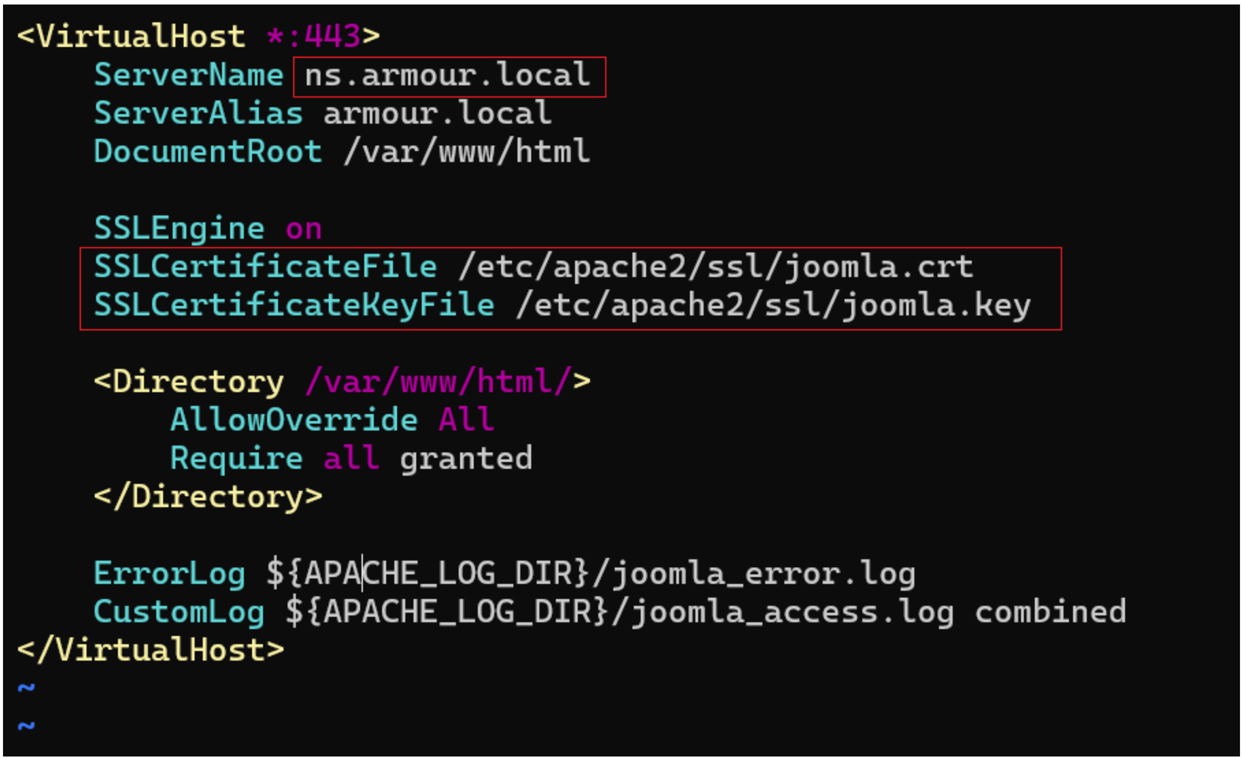
```
mkdir -p /etc/apache2/ssl
```

# Genrate Certificate

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/joomla.key -out /etc/apache2/ssl/joomla.crt
```

Step-5. Configure Virtual Host

vim /etc/apache2/sites-available/joomla.conf



```
<VirtualHost *:443>
    ServerName ns.armour.local
    ServerAlias armour.local
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/joomla.crt
    SSLCertificateKeyFile /etc/apache2/ssl/joomla.key

    <Directory /var/www/html/>
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/joomla_error.log
    CustomLog ${APACHE_LOG_DIR}/joomla_access.log combined
</VirtualHost>
~
~
```

On Client Windows PC

# Edit host file this Location
C:\Windows\System32\drivers\etc\hosts

# Add this line
192.168.169.130 ns.armour.local armour.local www.armour.local

Step-6. Enable SSL and Virual Host

```
a2enmod ssl
a2enmod rewrite
a2ensite joomla.conf
systemctl reload apache2
```

# Final Joomla Access

# By IP with Https
https://192.168.169.130/joomla

# By Domain Name with Https
https://www.armour.local/joomla

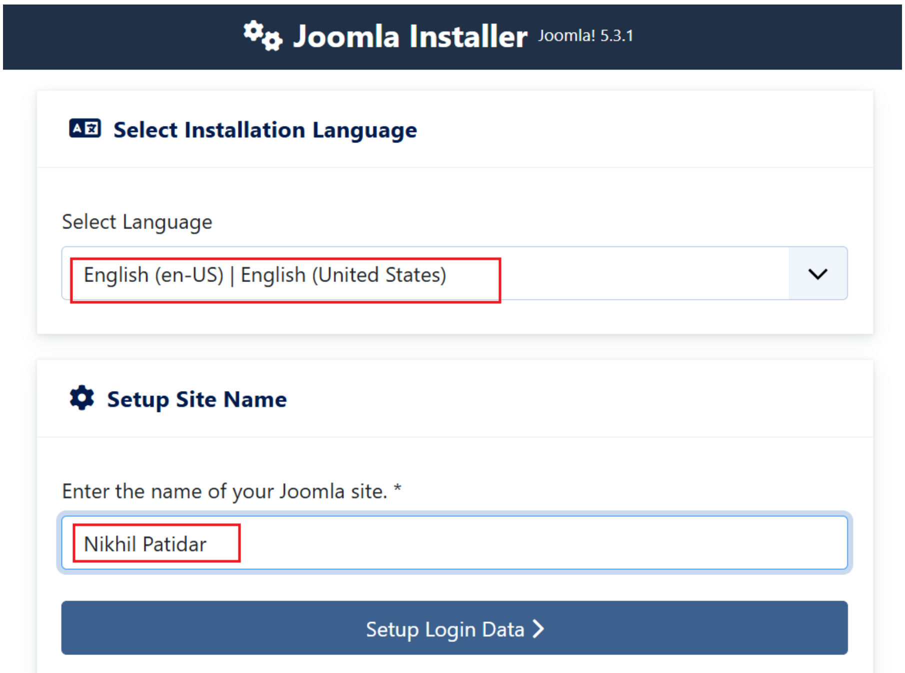
Joomla Installer 5.3.1

#Succefully Run Joomla this URL
https://www.armour.local/joomla/administrator/

#Joomla Admin Detials:

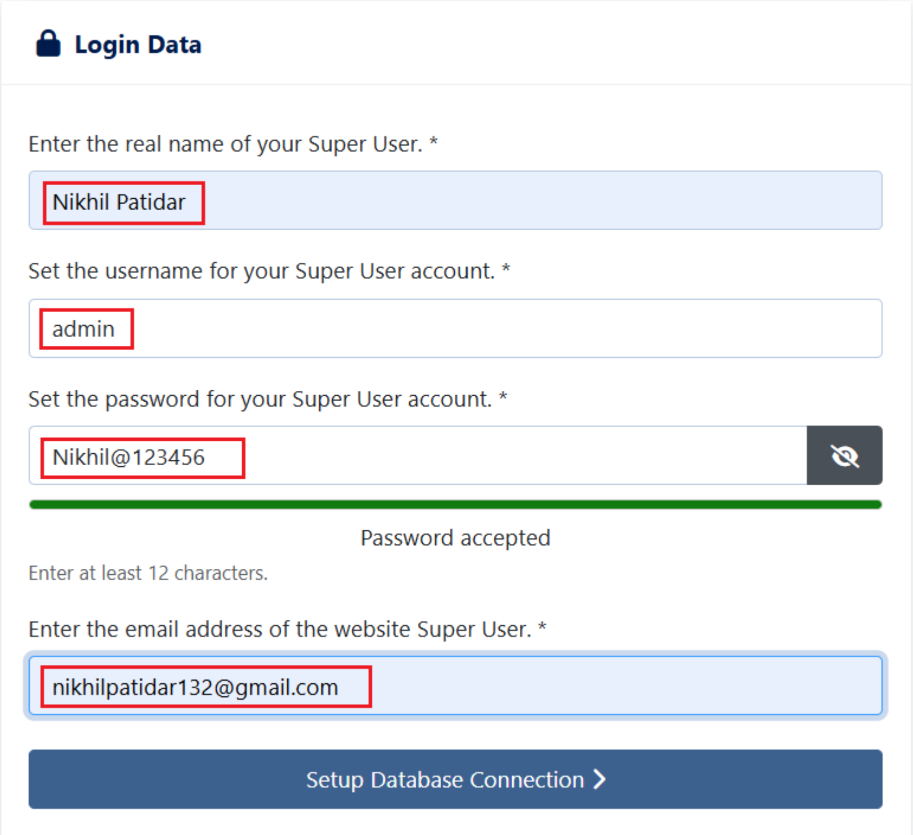
- **Username:** admin
- **Password:** -------@123456

https://www.armour.local/joomla/



Select Language: English (en-US) | English (United States)

Enter the name of your Joomla site. *: Nikhil Patidar



Login Data

Enter the real name of your Super User. *

Nikhil Patidar

Set the username for your Super User account. *

admin

Set the password for your Super User account. *

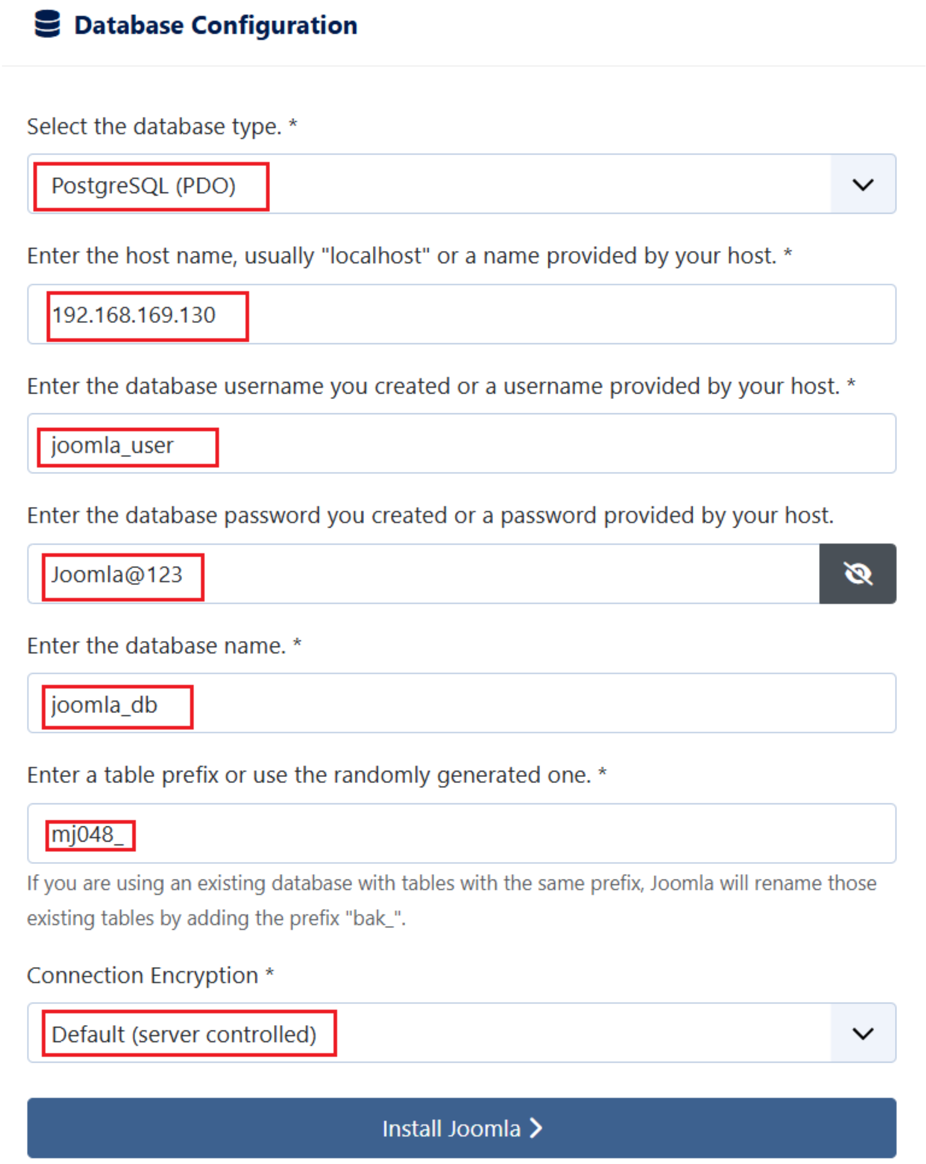
Nikhil@123456

Password accepted

Enter at least 12 characters.

Enter the email address of the website Super User. *

nikhilpatidar132@gmail.com



Database Configuration

Select the database type. *

PostgreSQL (PDO)

Enter the host name, usually "localhost" or a name provided by your host. *

192.168.169.130

Enter the database username you created or a username provided by your host. *

joomla_user

Enter the database password you created or a password provided by your host.

Joomla@123

Enter the database name. *

joomla_db

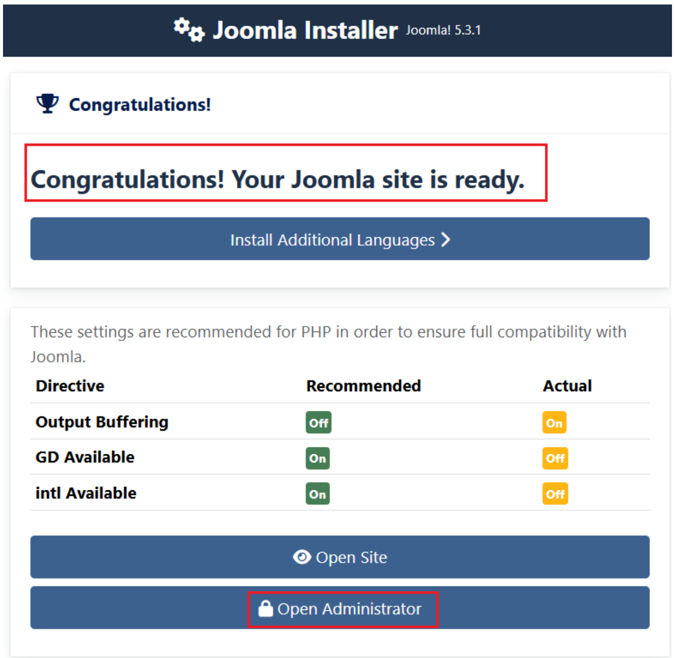
Enter a table prefix or use the randomly generated one. *

mj048_

If you are using an existing database with tables with the same prefix, Joomla will rename those existing tables by adding the prefix "bak_".

Connection Encryption *

Default (server controlled)



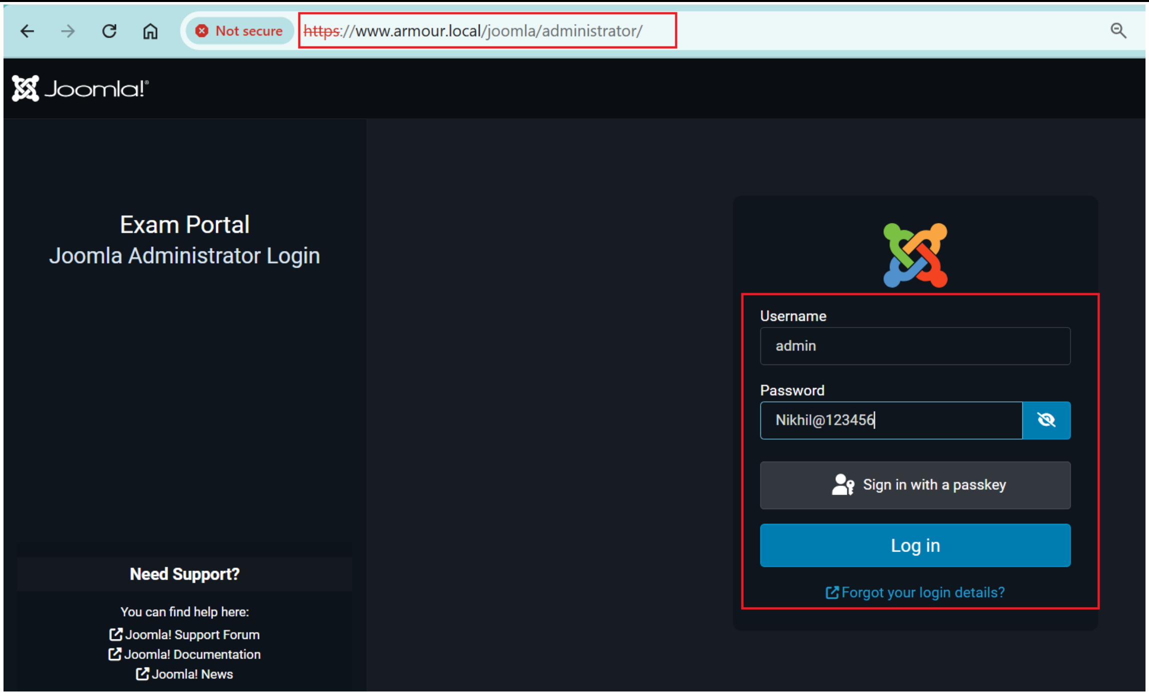
Joomla Installer Joomla! 5.3.1

Congratulations!

Congratulations! Your Joomla site is ready.

These settings are recommended for PHP in order to ensure full compatibility with Joomla.

Directive	Recommended	Actual
Output Buffering	Off	On
GD Available	On	Off
intl Available	On	Off



Not secure https://www.armour.local/joomla/administrator/

Joomla!

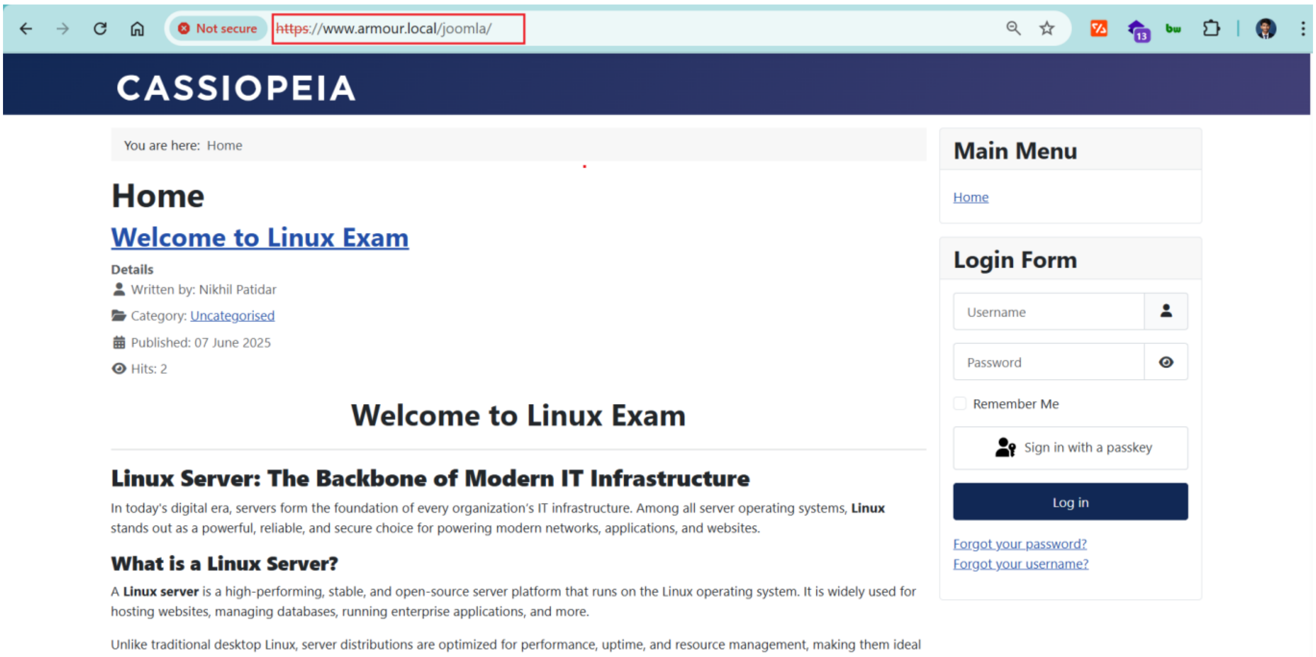
Exam Portal
Joomla Administrator Login

Username: admin

Password: Nikhil@123456

Need Support?

You can find help here:
Joomla! Support Forum
Joomla! Documentation
Joomla! News



Not secure https://www.armour.local/joomla/

CASSIOPEIA

You are here: Home

Home

Welcome to Linux Exam

Details
Written by: Nikhil Patidar
Category: Uncategorised
Published: 07 June 2025
Hits: 2

Welcome to Linux Exam

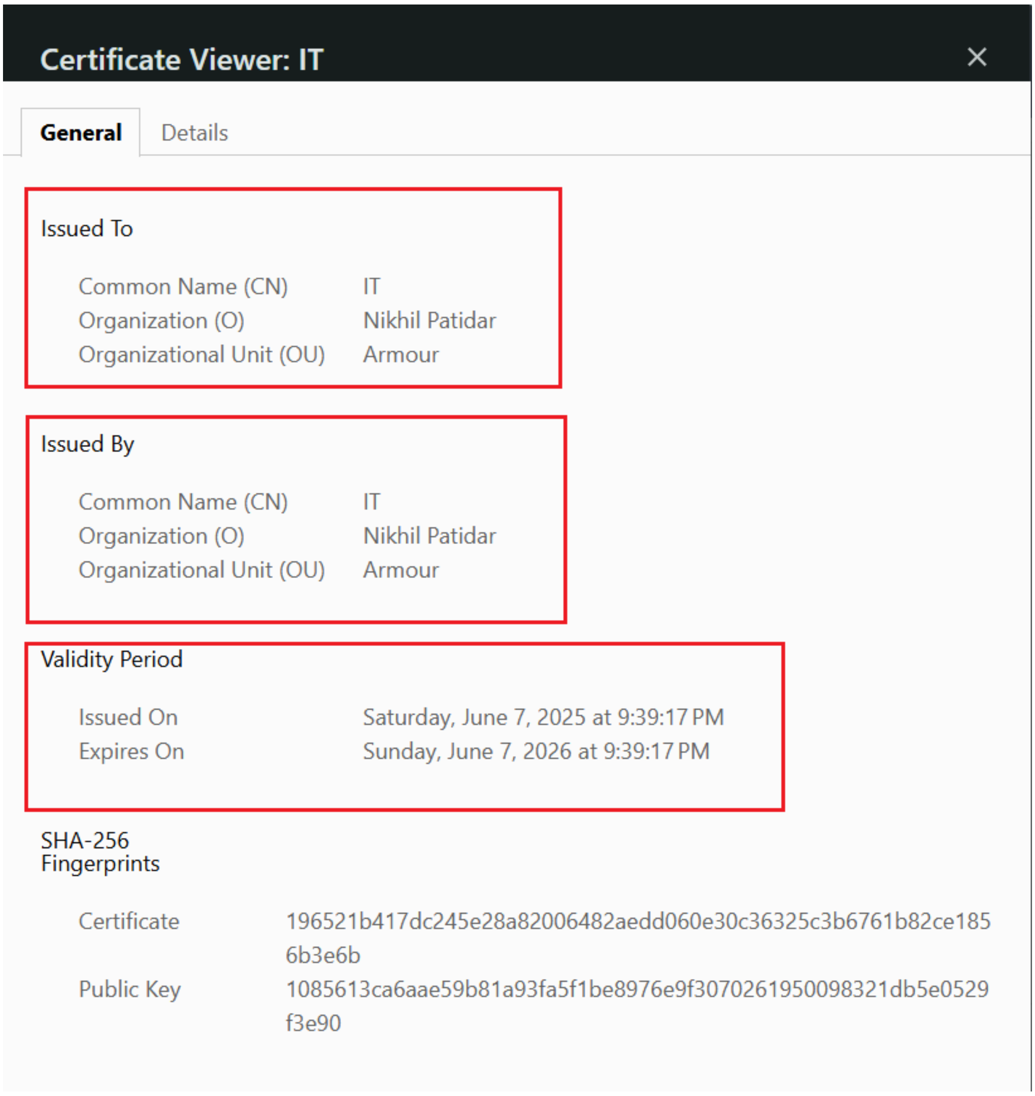
Linux Server: The Backbone of Modern IT Infrastructure

In today's digital era, servers form the foundation of every organization's IT infrastructure. Among all server operating systems, **Linux** stands out as a powerful, reliable, and secure choice for powering modern networks, applications, and websites.

What is a Linux Server?

A **Linux server** is a high-performing, stable, and open-source server platform that runs on the Linux operating system. It is widely used for hosting websites, managing databases, running enterprise applications, and more.

Unlike traditional desktop Linux, server distributions are optimized for performance, uptime, and resource management, making them ideal



Issued To

Common Name (CN)	IT
Organization (O)	Nikhil Patidar
Organizational Unit (OU)	Armour

Issued By

Common Name (CN)	IT
Organization (O)	Nikhil Patidar
Organizational Unit (OU)	Armour

Validity Period

Issued On	Saturday, June 7, 2025 at 9:39:17 PM
Expires On	Sunday, June 7, 2026 at 9:39:17 PM

SHA-256 Fingerprints

Certificate	196521b417dc245e28a82006482aedd060e30c36325c3b6761b82ce1856b3e6b
Public Key	1085613ca6aae59b81a93fa5f1be8976e9f3070261950098321db5e0529f3e90

Report Completed

All the necessary components of the Linux server environment have been configured and documented. This marks the successful completion of the server setup exam report.