AINUX

—TASTE OF LINUX—

WELCOME TO THE WORLD OF LINUX

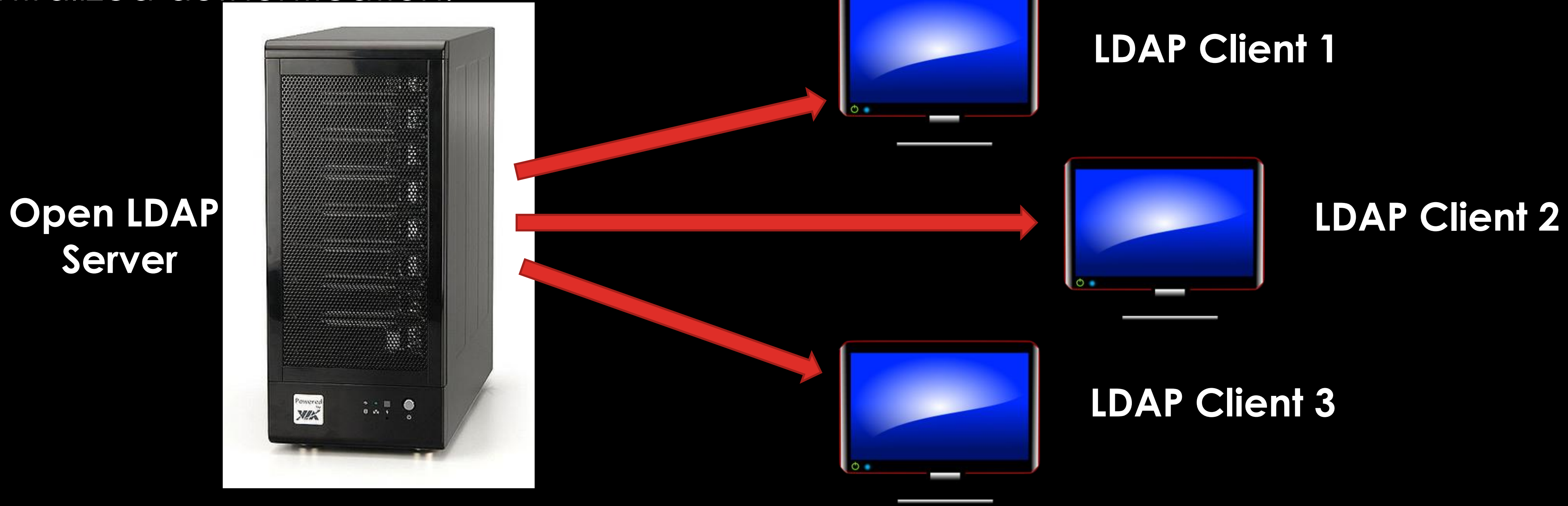
CREATED BY : ARYAN M.P

Connecting to Network-Defined Users and Groups

The ***LDAP (Lightweight Directory Access Protocol)*** is a protocols used to access centrally stored information over a network. this reason, LDAP is sometimes referred to as "***X.500 Lite***." The X.500 standard is a directory that contains hierarchical and categorized information, which could include information such as names, addresses, and phone numbers.

Why Use LDAP?

The main benefit of using LDAP is that, It stores all the information of an organization into a central repository which can be accessible from anywhere on the network. It provides centralized authentication.



Open LDAP Server

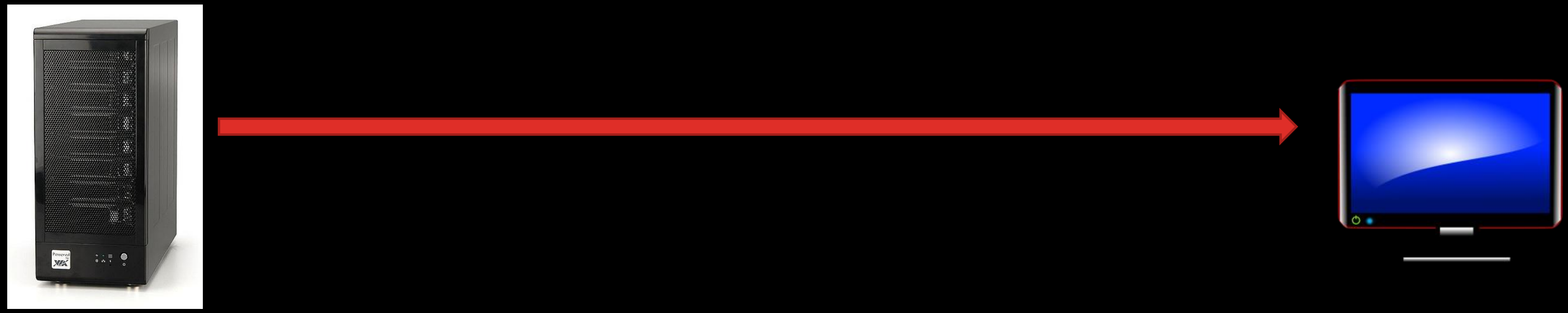
LDAP Client 1

LDAP Client 2

LDAP Client 3

Connecting to Network-Defined Users and Groups

LAB Scenario



Host Name: SRV
Role: Open LDAP Server
IP Address: 10.10.10.1

Host Name: CLI-1
Role: Open LDAP Client
IP Address: 10.10.10.2

The main benefit of using LDAP is that, It stores all the information of an organization into a central repository which can be accessible from anywhere on the network. It provides centralized authentication.

Connecting to Network-Defined Users and Groups

Step Involved

1. Install the required LDAP Packages “Openldap”
2. Create a LDAP root password for administration purpose.
3. Edit the OpenLDAP Server Configuration.
4. Provide the Monitor privileges.
5. Enable and Start the SLAPD Service.
6. Configure the LDAP Database.
7. Create the self-signed certificate.
8. Create base objects in OpenLDAP.
9. Generate a base.ldif (Logical date Interchange Format)file for your Domain.
10. Create a local Users
11. Import Users in to the LDAP database.
12. Test the configuration.

Connecting to Network-Defined Users and Groups

Installing OpenLDAP Packages

```
# yum  install  openldap*   compat-openldap  migrationtools        [Install the LDAP Packages]
```

Create a LDAP root password for administration purpose

```
# slappasswd                                                      [To add make LDAP password]
```

Note: - Copy entire password and save it into a file.

Edit the OpenLDAP Server Configuration

Note: - OpenLDAP configuration files are stored into "/etc/openldap/slapd.d/cn=config" directory

```
# cd /etc/openldap/slapd.d/cn=config
# ll
# vim  olcDatabase\=\{2\}hdb.ldif
```

Edit the following

olcSuffix: dc=**iant**,dc=**com**
olcRootDN: cn=Manager,dc=**iant**,dc=**com**

Add the following line at the end with the password which you have copied before.

olcRootPW: {SSHA}wHql9biTWclkkgHP4W5lGZBTw1RvcsYH

Save and Exit

CREATED BY : ARYAN M.P

Connecting to Network-Defined Users and Groups

Provide the Monitor privileges

```
# vim olcDatabase\=\{1\}monitor.ldif
```

Edit the following

```
 olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,dc=iant,dc=com" read by * none
```

```
# slaptest  -u                                        [To check the configuration]
```

Enable and Start the SLAPD Service

```
# systemctl  start slapd.service
# systemctl  enable  slapd.service
# firewall-cmd --permanent --add-service=ldap
# firewall-cmd  -–reload
```

Configure the LDAP Database

```
# cp "/usr/share/openldap-servers/DB_CONFIG.example"  "/var/lib/ldap/DB_CONFIG"
# cd  /var/lib/ldap
# chown  -R   ldap:ldap   DB_CONFIG
```

Connecting to Network-Defined Users and Groups

Add Schema entry into the Database

```
# ldapadd  -Y  EXTERNAL  -H  ldapi:///  -f  /etc/openldap/schema/cosine.ldif
# ldapadd  -Y  EXTERNAL  -H ldapi:///   -f  /etc/openldap/schema/nis.ldif
# ldapadd  -Y  EXTERNAL  -H ldapi:///   -f  /etc/openldap/schema/inetorgperson.ldif
```

Create the self-signed certificate

```
# cd  /etc/pki/tls/certs/
# openssl  req  -new  -x509  -nodes  -out  /etc/pki/tls/certs/iant.pem  -keyout
    /etc/pki/tls/certs/iantkey.pem  -days 365
```

Note: - It will ask you few questions

```
# IN
# UP
# LKO
# IANT
# IT
# SRV.IANT.COM
# subhamcts@gmail.com
```

Now the certificate and key file is generated successfully.

```
# ll                                                    [To check the key files]
```

Connecting to Network-Defined Users and Groups

Edit the OpenLDAP Server Configuration to add the certificate details

```
# cd /etc/openldap/slapd.d/cn=config
# ll
# vim  olcDatabase\=\{2\}hdb.ldif
```

Add the following line at the end with the password which you have copied before.

```
olcTLSCertificateFile: /etc/pki/tls/certs/iant.pem
olcTLSCertificateKeyFile: /etc/pki/tls/certs/iantkey.pem
```

Save and Exit

AINUX

— TASTE OF LINUX —

THANK YOU

CREATED BY : ARYAN M.P