Introduction to LDAP

Day 3 – SS Track - SomNOG6

Introduction to LDAP

- Understanding LDAP
- LDAP Servers
- Information Structure
- Protocol Overview
- LDAP operations

UNDERSTANDING LDAP

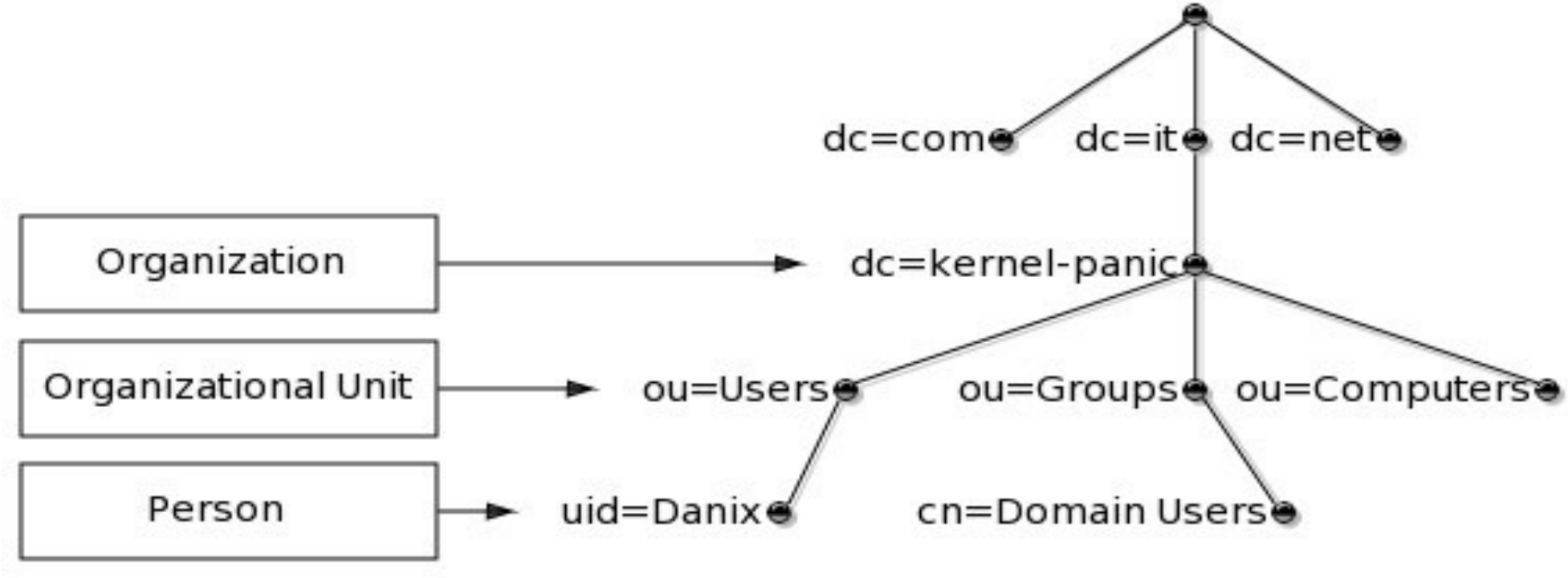
- LDAP stands for Lightweight Directory Access Protocol.
- It is an internet protocol for accessing distributed directory services.
- It uses the TCP/IP protocols for its operations
- It also forms the standard for allowing directories to be managed.

LDAP Servers

- OpenLDAP
- Active directory
- Apache Directory Server
- FreeIPA
- OpenDS
- Novell eDirectory
- Sun Java System Directory Server
- IBM Tivoli Directory Server

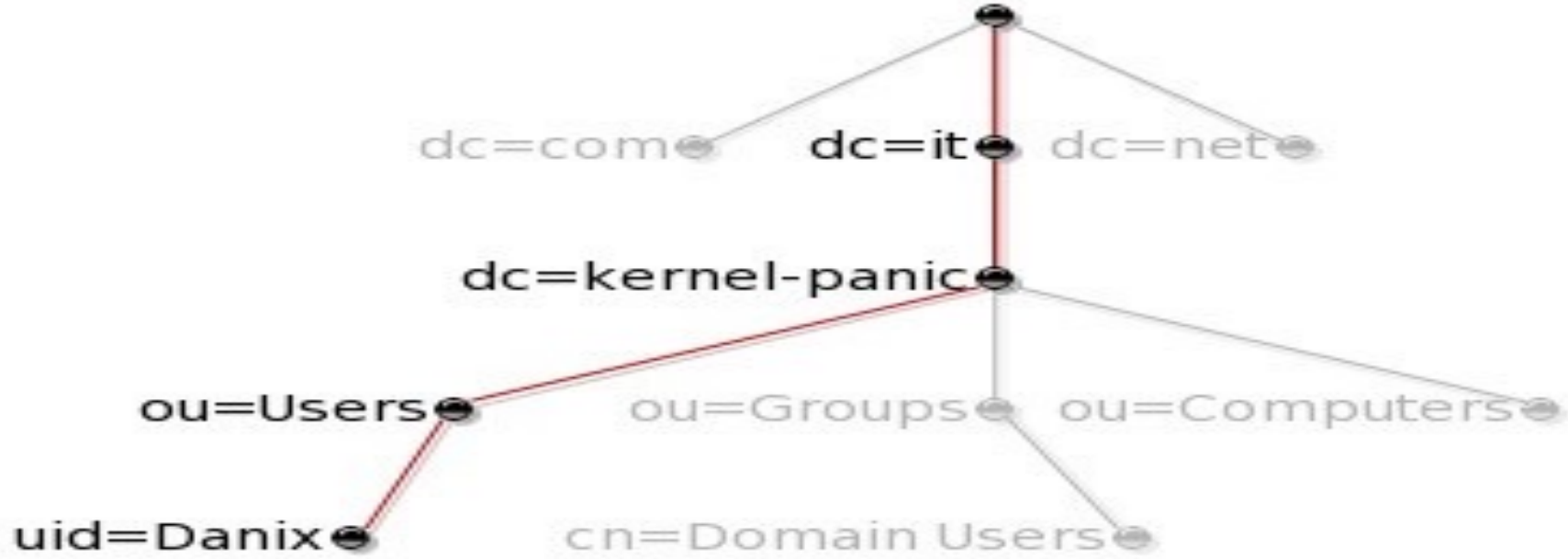
Information Structure

- It has a DIT (Directory Information Tree) which help present information in the hierarchical tree format
- Example of a DIT is as below.



Information Structure (Cont)

- Each node in the LDAP tree is called an entry and is uniquely identified by its Distinguished Name (DN)
- For instance, the DN of the entry highlighted in the following picture below.



Information Structure (Cont)

- The DN for the above tree can then be written as below
- “ui=Danix,ou=Users,dc=kernel-panic,dc=it” See RFC4514 for full description of the DN format.
- An entry consists of a set of attributes, each attribute has a name or type and one or more values.
- “dc” stands for Domain Component
- “cn” stands for Common Name
- Objectclasses define the attribute structure of an LDAP entry.
- Both ObjectClasses and Attributes are defined within schemas

Information Structure (Cont)

- O stands for organization
- OU stands for Organizational unit
- SN stands for Surname
- Givenname stands for First Name
- UID stands for Userid
- Mail stands for Email address
- C stands for country
- L stands for location
- St stands for Status

Information Structure (Cont)

- Entries can be represented in a human-readable format by using the LDIF format as in example below.

```
dn: uid=danix,ou=Users,dc=kernel-panic,dc=it
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
cn: Daniele Mazzocchio
sn: Mazzocchio
givenName: Daniele
uid: Danix
uidNumber: 2000
gidNumber: 513
homeDirectory: /home/danix
```

Protocol Overview

- Client starts an LDAP session by connecting to an LDAP Server
- The default TCP port is 389
- Bind to the server through an authentication process
- Client then sends an operation request to the server
- The Server sends responses in return

LDAP Operations

Operation	What it does
Search	Search directory for matching directory entries
Compare	Compare directory entry to a set of attributes
Add	Add a new directory entry
Modify	Modify a particular directory entry
Delete	Delete a particular directory entry
Rename	Rename or modify the DN
Bind	Start a session with an LDAP server
Unbind	End a session with an LDAP server
Abandon	Abandon an operation previously sent to the server
Extended	Extended operations command

LDAP Operation (Cont)

- Some useful LDAP operation commands are as below.
- Ldapadd
- Ldapsearch

- Some useful link to see example of such operation are below
- http://www.kernel-panic.it/openbsd/pdc/pdc2.html
- http://www.my-tiny.net/Lab06_WebLDAP.htm
- http://himanshu.gilani.info/blog/2013/01/12/introduction-to-ldap/

Thanks to Frank A. Kuse and AfNOG Team