Active Directory: The need and the benefit from proper management

Stoyan Bulanov

- 10 years experience as Sys Admin
- 3 years experience as Computer Repair Technician
- Makes excellent Cocktails

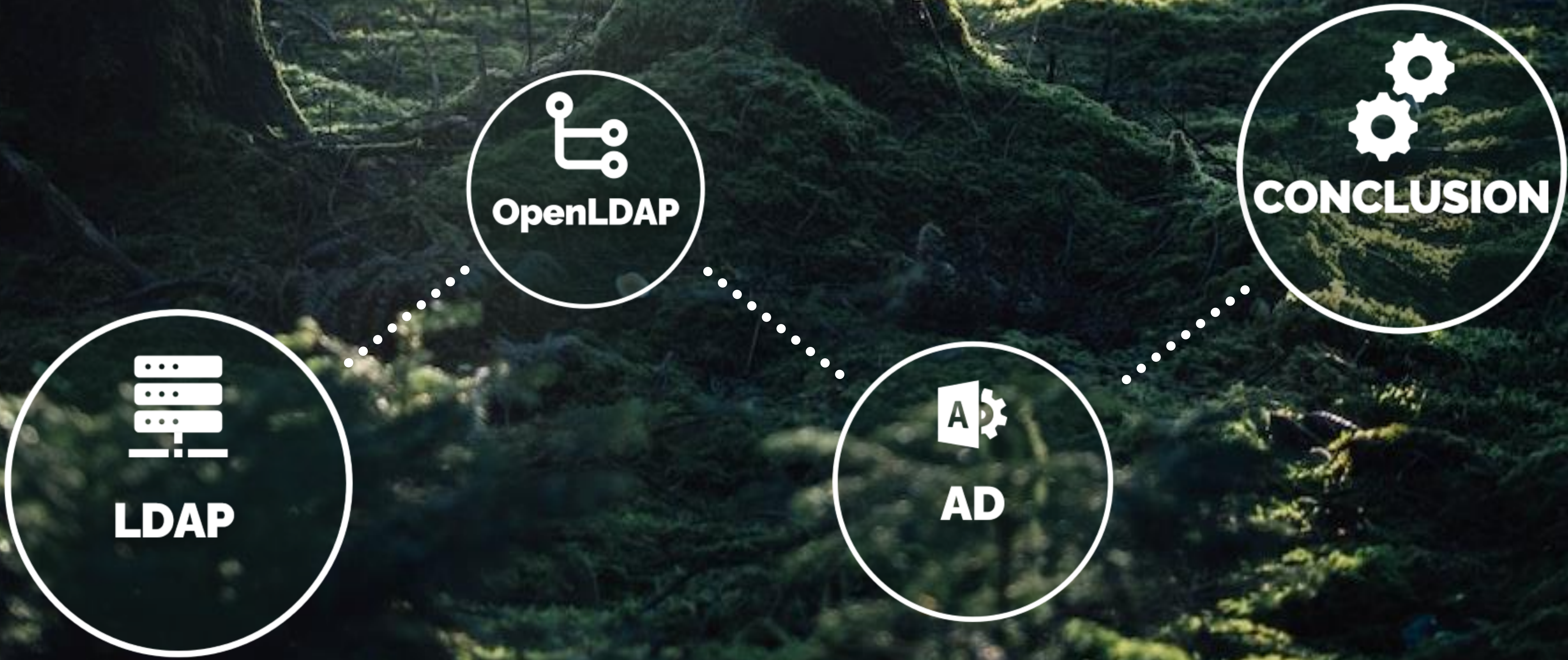
Contacts :
s.m.bulanov@gmail.com

Questions ?
www.slido.com
#seminar

Content

- What is Sys Admin
- AD vs LDAP vs OpenLDAP
- Best Practices while managing AD
- Q&A

AD vs LDAP vs OpenLDAP



LDAP

OpenLDAP

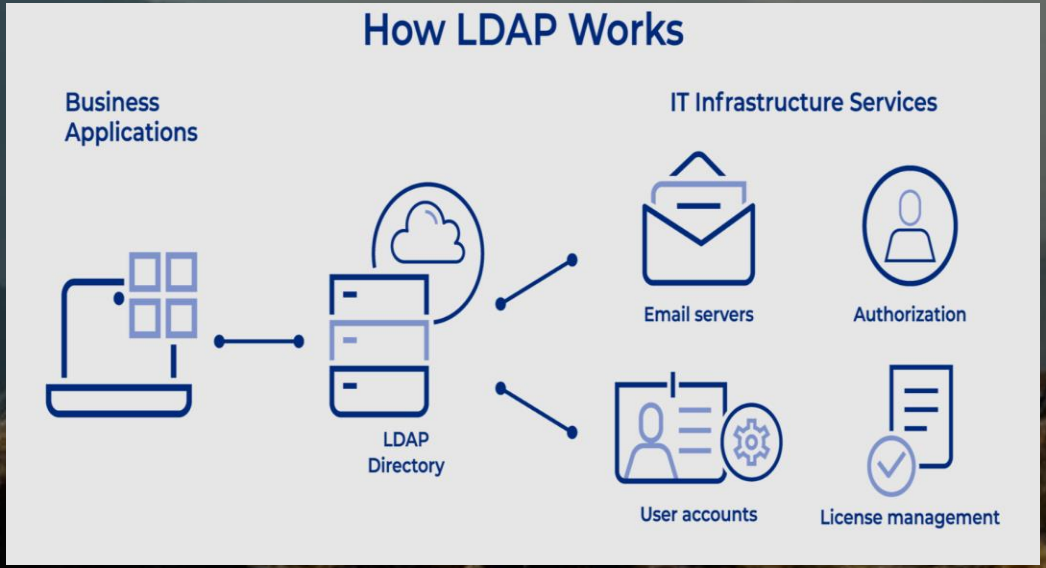
AD

CONCLUSION

LDAP

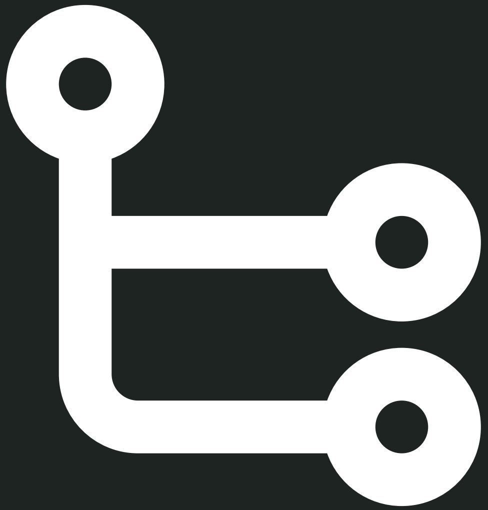
LDAP

Lightweight directory access protocol, commonly known as an LDAP, is a protocol tool that aids in discovering data and information about a specific industry, firm, or even individuals in a network. It is also used to find valuable resources such as files, documents, and appropriate devices for that specific network.



The LDAP authentication process is a client-server model of authentication, and it consists of these key players:

- **Directory System Agent (DSA):** a server running the LDAP on its network
- **Directory User Agent (DUA):** accesses DSAs as a client (ex. a user’s PC)
- **DN:** the distinguished name, which contains a path through the directory information tree (DIT) for LDAP to navigate through (ex. cn=Susan, ou=users, o=Company)
- **Relative Distinguished Name (RDN):** each component in the path within the DN (ex. cn=Susan)
- **Application Programming Interface (API):** lets your product or service communicate with other products and services without having to know how they’re implemented



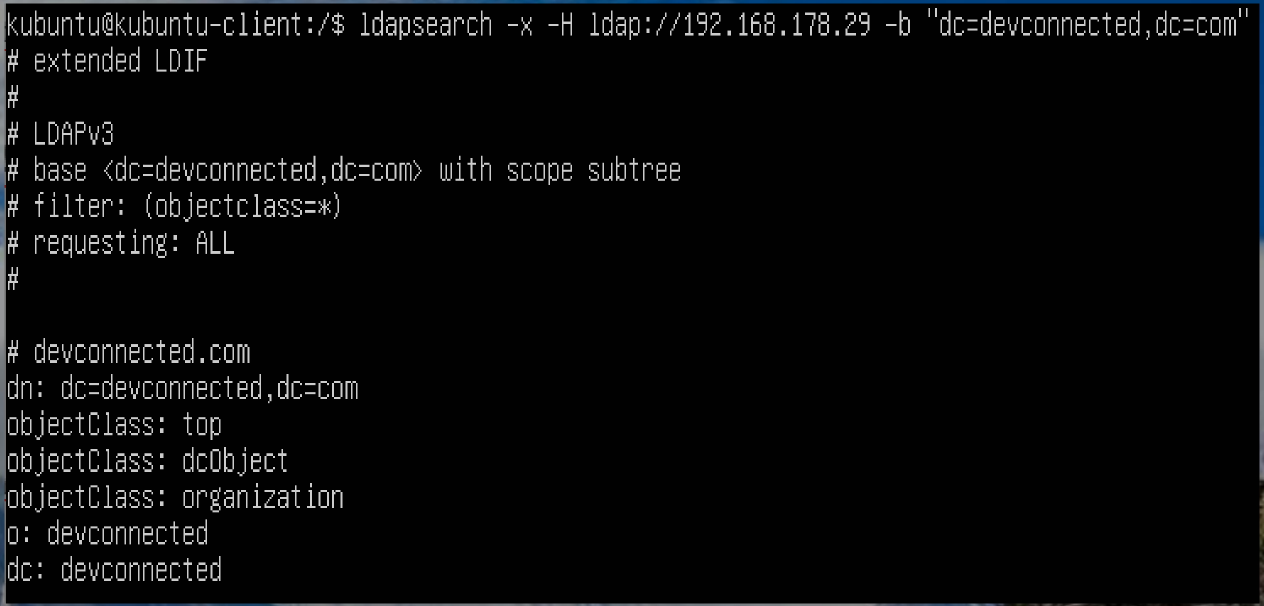
OpenLDAP

OpenLDAP

OpenLDAP is a free, open-source implementation of the Lightweight Directory Access Protocol (LDAP) developed by the OpenLDAP Project. It is released under its own BSD-style license called the OpenLDAP Public License.

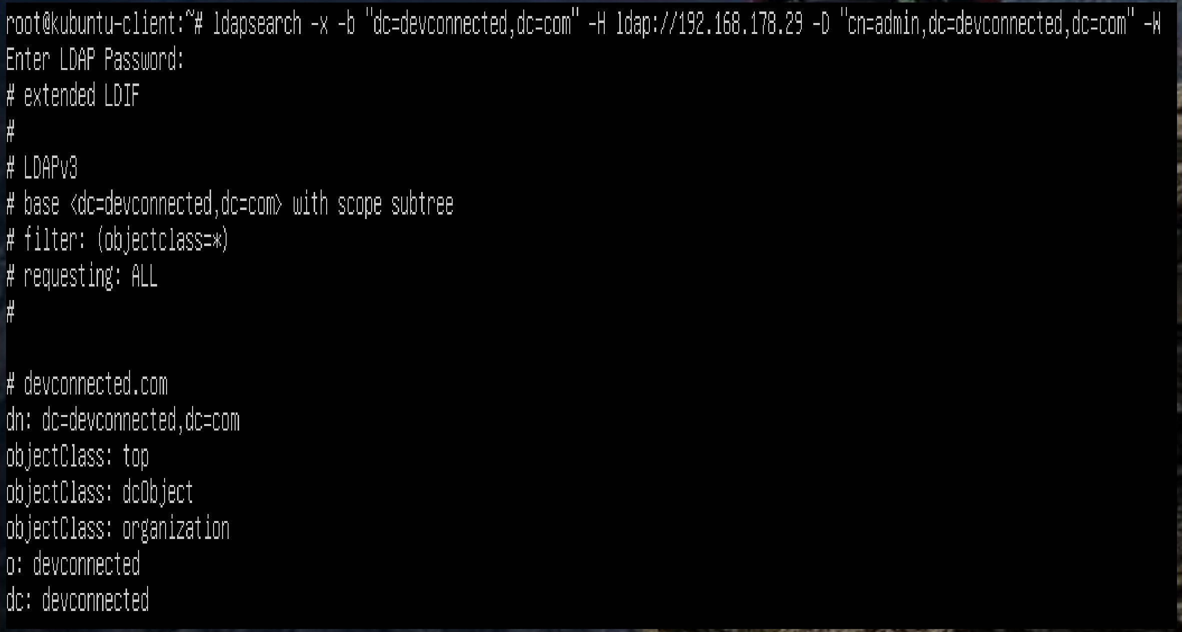
LDAP is a platform-independent protocol. Several common Linux distributions include OpenLDAP Software for LDAP support. The software also runs on BSD-variants, as well as AIX, Android, HP-UX, macOS, OpenVMS, Solaris, Microsoft Windows

OpenLDAP is designed to function via CLI. Because it is open-source, commands and tools are available online. For example, **here’s what it takes to set up OpenLDAP via CLI**.



```
kubuntu@kubuntu-client:/$ ldapsearch -x -H ldap://192.168.178.29 -b "dc=devconnected,dc=com"
# extended LDIF
#
# LDAPv3
# base <dc=devconnected,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# devconnected.com
dn: dc=devconnected,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: devconnected
dc: devconnected
```

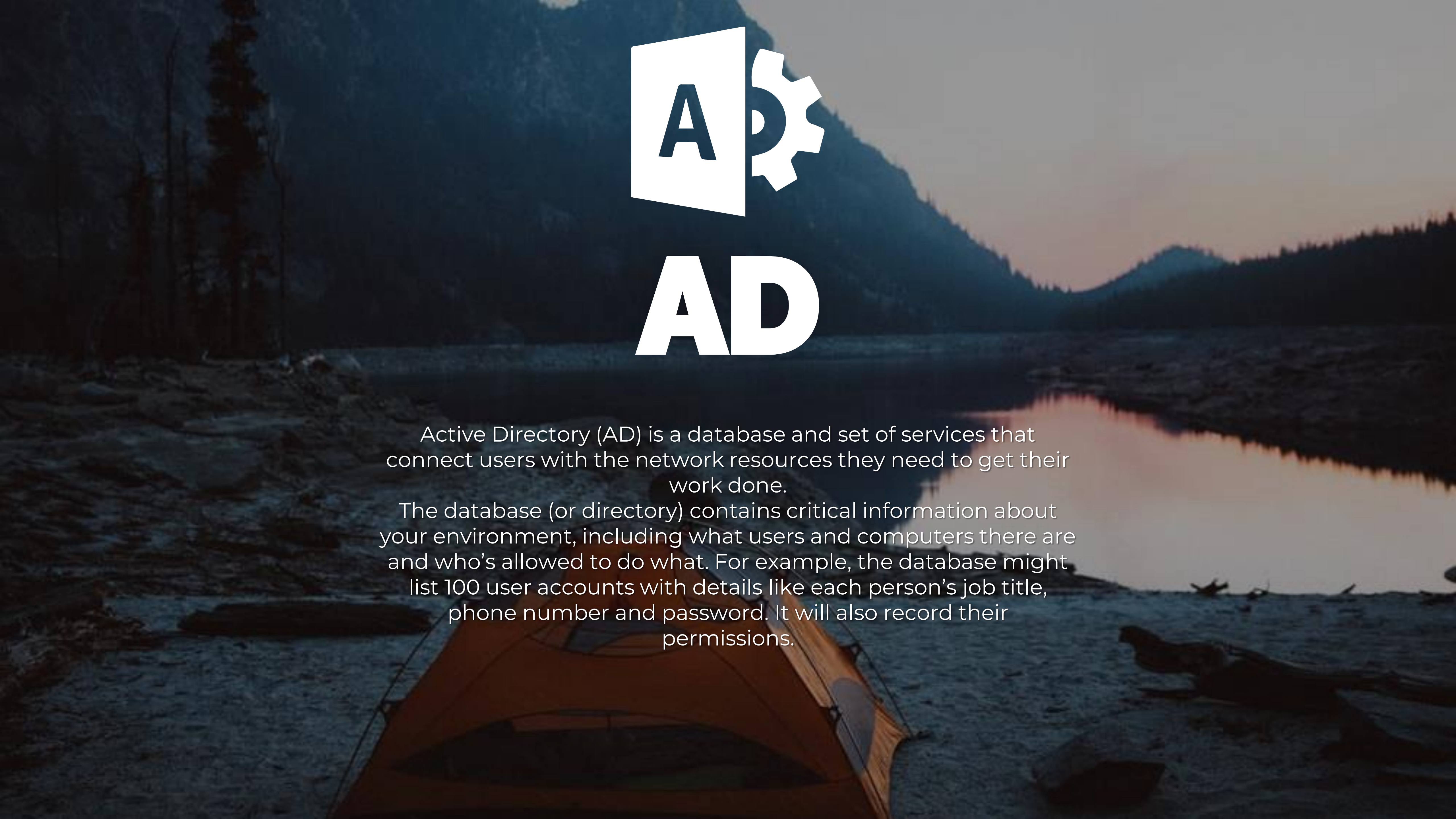


```
root@kubuntu-client:~# ldapsearch -x -b "dc=devconnected,dc=com" -H ldap://192.168.178.29 -D "cn=admin,dc=devconnected,dc=com" -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=devconnected,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# devconnected.com
dn: dc=devconnected,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: devconnected
dc: devconnected
```

This format is the most simplified and leaves OpenLDAP in its most flexible form. It’s ideal for highly technical teams and those that aim to create unique or highly customized configurations.

AD

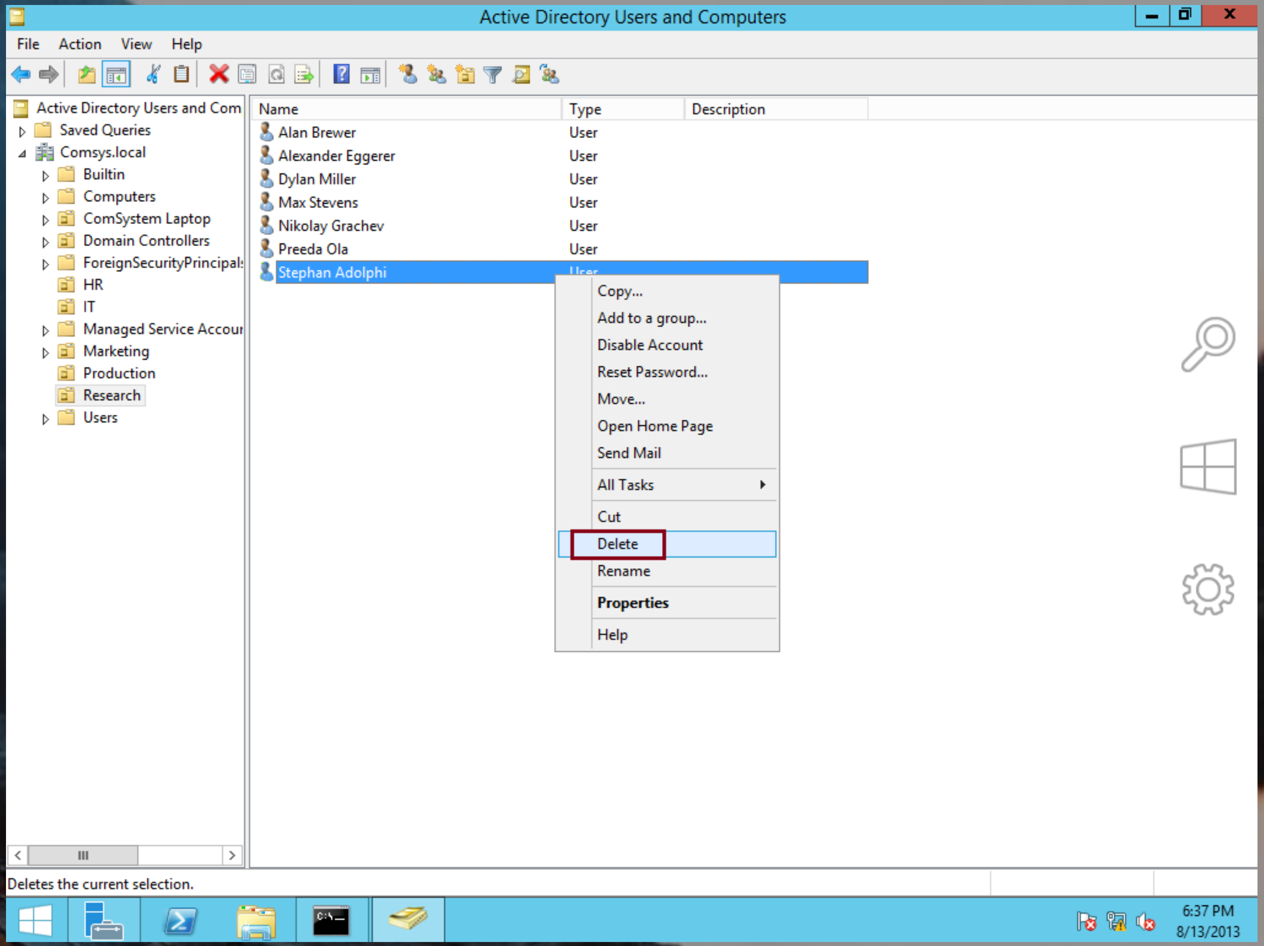


AD

Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.

The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what. For example, the database might list 100 user accounts with details like each person's job title, phone number and password. It will also record their permissions.

Domain is a collection of users, computers, and devices that are part of the same Active Directory database. If an organization has multiple locations, they may have a seperate domain for each one. For example, an international organization could have a domain for their London office, another one for their New York office, and a third one for their Tokyo office. IT admins also sometimes isolate their user accounts into a separate forest to maximize security. These configurations aren’t rudimentary and oftentimes require hiring external resources to set up.



Name	Type	Description
Alan Brewer	User	
Alexander Eggerer	User	
Dylan Miller	User	
Max Stevens	User	
Nikolay Grachev	User	
Preeda Ola	User	
Stephan Adolphi	User	

Deletes the current selection.

CONCLUSION

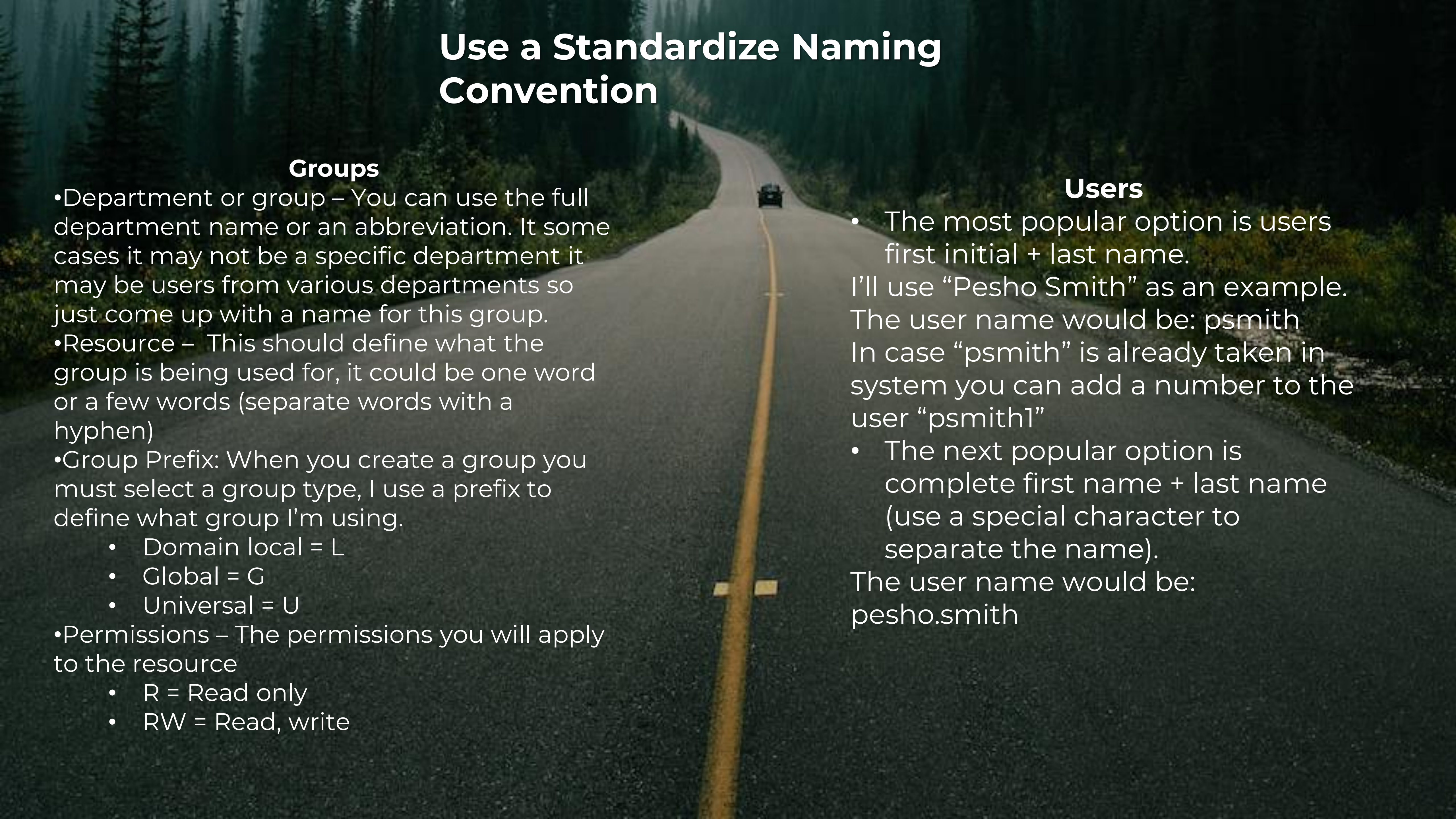
CONCLUSION

LDAP and Active Directory are often used in tandem. They share few commonalities and should not be treated as competitive solutions. Since Active Directory and other LDAP servers like OpenLDAP act as centralized identity providers, it is of utmost importance to protect them with comprehensive safeguards like Multi-Factor Authentication (MFA).

Best practices while managing AD

Key concepts

- Proper and strict adherence to Naming Conventions.
- Descriptions
- Create a lot of OUs (containers)
- Regular cleanup of AD
- Automate whenever possible



Use a Standardize Naming Convention

Groups

- Department or group – You can use the full department name or an abbreviation. It some cases it may not be a specific department it may be users from various departments so just come up with a name for this group.
- Resource – This should define what the group is being used for, it could be one word or a few words (separate words with a hyphen)
- Group Prefix: When you create a group you must select a group type, I use a prefix to define what group I'm using.
  - Domain local = L
  - Global = G
  - Universal = U
- Permissions – The permissions you will apply to the resource
  - R = Read only
  - RW = Read, write

Users

- The most popular option is users first initial + last name.

I'll use "Pesho Smith" as an example.
The user name would be: psmith
In case "psmith" is already taken in system you can add a number to the user "psmith1"

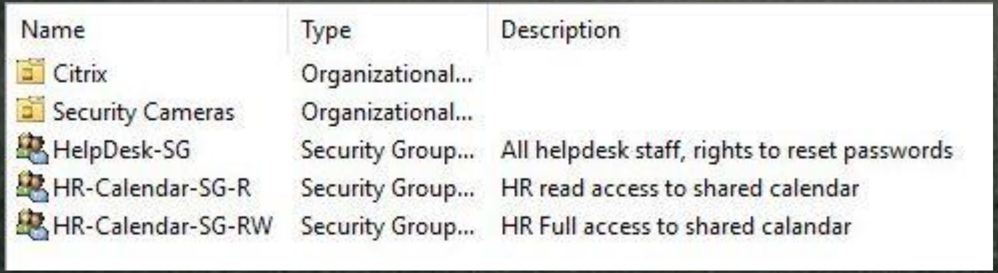
- The next popular option is complete first name + last name (use a special character to separate the name).

The user name would be:
pesho.smith

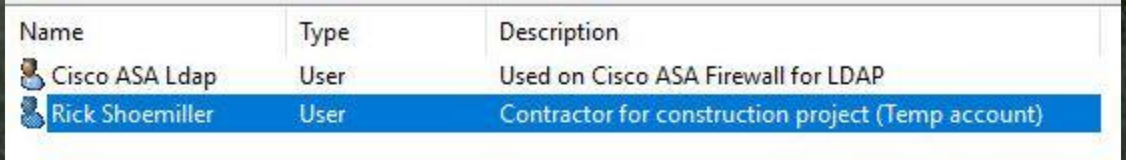
Descriptions to Active Directory Objects

Even if you are using a good naming convention I still like to add descriptions to objects. Obviously not all objects, but servers, groups, service accounts, and generic accounts I put descriptions on them.

Not only does this help me quickly identify the use of the object it helps the whole team understand.

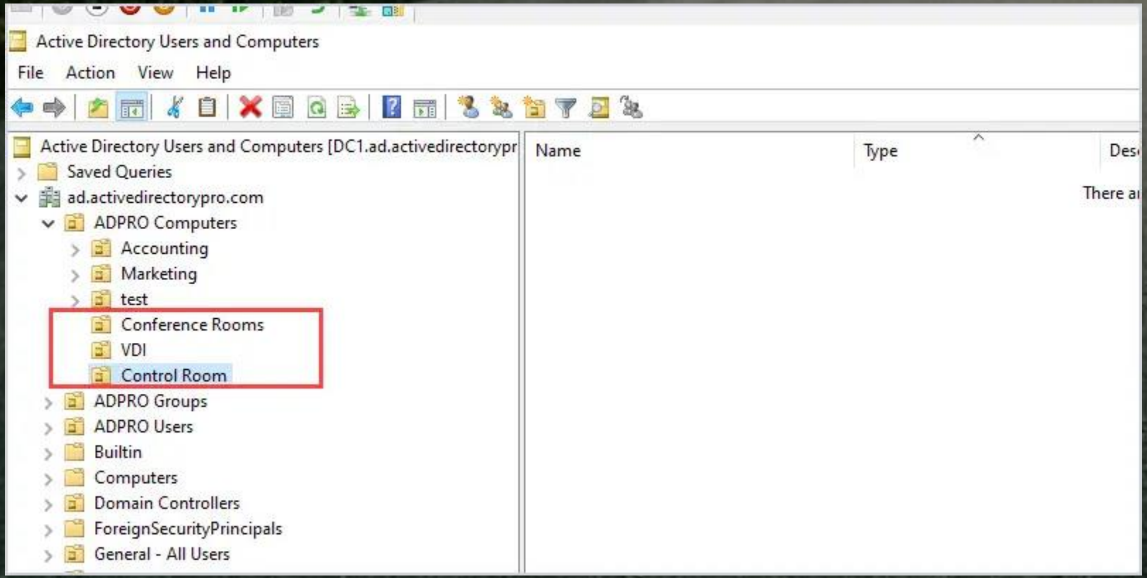


Name	Type	Description
Citrix	Organizational...	
Security Cameras	Organizational...	
HelpDesk-SG	Security Group...	All helpdesk staff, rights to reset passwords
HR-Calendar-SG-R	Security Group...	HR read access to shared calendar
HR-Calendar-SG-RW	Security Group...	HR Full access to shared calandar



Name	Type	Description
Cisco ASA Ldap	User	Used on Cisco ASA Firewall for LDAP
Rick Shoemiller	User	Contractor for construction project (Temp account)

Create a lot of OUs (containers)



- Active Directory Users and Computers [DC1.ad.activedirectorypr
  - Saved Queries
  - ad.activedirectorypro.com
    - ADPRO Computers
      - Accounting
      - Marketing
      - test
      - Conference Rooms
      - VDI
      - Control Room
    - ADPRO Groups
    - ADPRO Users
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - General - All Users

- ❖ OU Best Practice #1: Separate Users and Computers
- ❖ OU Best Practice #2: Create an OU for Security Groups
- ❖ OU Best Practice #3: Create an OU for Servers

Automate Common Active Directory Tasks

Most routine tasks can be automated to make you more efficient at your job. Here are some common tasks that you should automate:

- User account creation
- Account removal
- Account modifications
- Group Membership Management
- AD cleanup
- File copies, directory cleanups
- Software deployment
- Windows and 3rd party patches
- Inventory
- Decommission of assets

Q&A