Jong Park
CS 312 – System Architecture
HW 6 – Active Directory and DNS
May 13, 2019

Linux Equivalents to Active Directory

What are some possible equivalent services or implementations of the following Active Directory services that could be run on Linux: (20 points)

> **Domain Services**: Tracks information about members of the domain, including computers and users, in various directories. Also defines access rights to the devices, files, and services on the domain (Hint: Look into LDAP).

Name: OpenLDAP (Lightweight Directory Access Protocol).
Advantage: It's free as beer, AND it's free as speech. Microsoft AD will charge you a minimum of $1/user/month (exception of free tier). [1]
Disadvantage: Microsoft AD has a GUI tools to get you started as soon as you install it. Whereas OpenLDAP's Directory Information Tree (DIT) will have to be hand configured. It also could be used as an advantage if you want to design the DIT in a way it could be different from AD or make it fit to the existing AD network. [2]

> **Certificate Services**: Generates and maintains a private/public key infrastructure.

Name: Kerberos (Network Protocol, UDP port 88) [3]
Description: The protocol of the same name is used by both Windows and nix systems. However Windows does not use the program that was developed by MIT.
Advantage: It requires a user account, user clients and services on the server to all have trusted relationship to the Kerberos token server. Which means, unknown/untrusted clients without a user account will be denied.
Disadvantage: The authentication is limited by how many users the server can handle. Each server can use a different administration protocol and depending on the size of the network, the protocol will not be compatible between networks.

> **Federation Services**: Also known as Single-Sign-On, or SSO, this allows authenticating in just one place, and having access to all resources across the domain and with other connected services, domains, or technologies (websites, other domains, etc.). For example, your ONID access is federated across Google, OSU infrastructure, your Box account, etc.

Name: Distributed Access Control System (DACS)
Description: "DACS is a light-weight SSO and attribute-based access control system for web servers and server-based software." It runs on FreeBSD, Linux, and macOS. [4]
Advantage: Open-source. Lots of functionalities are available as web-based API as well as command-line interfaces. "User passwords, imported user account names, and other potentially sensitive information are either not stored by DACS or are stored in encrypted form." [5] It could be used with both LDAP and Microsoft AD account.
Disadvantage: As far as I could tell, there are not much drawbacks of DACS.

Rights Management Services: Encrypted file management and access services.

Name: JumpCloud Directory-as-a-Service [6]

Advantage: It is cross compatible with all systems and it could be used with both physical and cloud servers (AWS, GSP) as well as legacy web-based applications (JIRA, Sales force). It even has support for Dropbox, NAS and Samba file servers. It could be used wired and wireless since it is a service.

Disadvantage: Since it is a service, free tier only supports 10 users. This is a great service for small businesses but when the business or network grows, you will have to use the paid version of $3/user/month or pro version of $9/month that have full cross compatibility of all systems described above. [7]

DNS Questions

1) **What is a DNS A record? Give an example of one. (5 points)**
   DNS A record (Address Record) points a domain or subdomain to an IP address. It is used to point a logical domain. For example, "google.com" is pointed to their hosting server "216.58.194.206 (SFO server)" and "localhost" will be directed to "127.0.0.1." [8]

2) **What is a DNS SRV record? Give an example of one. (5 points)**
   DNS Service record (SRV record) is a specification of data in DNS to define location (the hostname & its port number) of servers for specified services. Session Initiation Protocol (SIP) and Extensible Messaging and Presence Protocol (XMPP) are some of the protocol that requires SRV support. The example of a SRV record in text format is:
   ```
   _sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.example.com.
   ```
   It means SIP protocol services is using TCP protocol to points to `sipserver.example.com` with port 5060. The priority given is 0 with 5th weight in case of multiple 0 priorities. [9]

3) **What is the difference between a forward and reverse lookup DNS query? What special kind of DNS record is required to make this work? (5 points)**
   Forward DNS lookup is using Internet domain name (google.com) to find an IP address (172.217.14.238 (Seattle server)). Reverse lookup is the opposite, using IP address to find a domain name. A **routing table** in the DNS server or router looks up the IP address of the address (URL) entered in the browser by the user. [10]

4) **Instead of using .local at the end of a domain name, like we've done in our reference server (cs312domain.local), the recommendation is that a true domain name be used, instead, with a real top-level-domain name. (5 points)**

In order to run a domain, you need a server that can stores all the data of the domain and the server should be mapped to a static IP address so that it could be assigned a domain name. The advantage of that would be that you are not borrowing a server from some 3rd party server storage and can avoid fees. However, with that money you're saving, you're also paying with the electricity and service. If your website gets a DDoS or (just really popular like facebook), you it would limit the connection to number of wires running to the server x amount of Gbps it could handle per wire.

Sources:

[1] https://azure.microsoft.com/en-us/pricing/details/active-directory/
[2] https://stackoverflow.com/questions/997424/active-directory-vs-openldap
[3] https://www.wikiwand.com/en/Kerberos_(protocol)
[4] https://www.wikiwand.com/en/Distributed_Access_Control_System
[5] https://dacs.dss.ca/exec-overview.html
[6] https://jumpcloud.com/blog/cheaper-alternative-active-directory/
[7] https://jumpcloud.com/pricing/
[8] https://my.bluehost.com/hosting/help/whats-an-a-record
[9] https://www.wikiwand.com/en/SRV_record
[10] https://searchnetworking.techtarget.com/definition/Forward-DNS-lookup