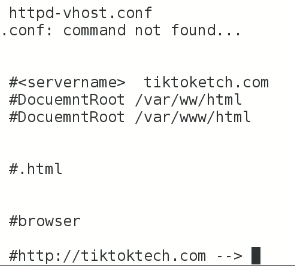
Lecture 19

**SAMBA**

Recap of webhosting



.



.

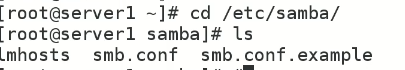
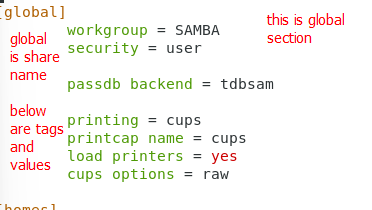
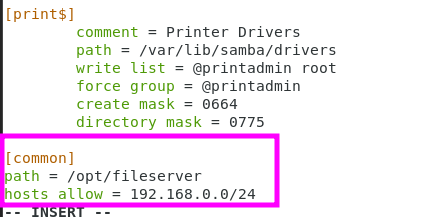
SAMBA Server

* Centralized file server
* Similar to NFS
* It is Linux to Linux & Linux to Windows
* Asks for username & password.
* NFS is less secure (NO username & Password)
* Samba is an open-source implementation of the SMB/CIFS networking protocol used by Windows-based computers to share files, printers, and other resources over a network. Samba allows Linux, Unix, and other operating systems to seamlessly integrate with Windows networks, allowing file and print services to be shared between different operating systems.
* Samba can be used to share files and printers between Windows and Linux/Unix systems, as well as between different Linux/Unix systems. It can also be used to provide Windows domain controller services, allowing Linux/Unix systems to participate in Windows-based domains. Samba can also act as an Active Directory domain controller or as a member server in an Active Directory domain.
* Samba is commonly used in enterprise environments where there is a mix of Windows and Linux/Unix systems. It is also used in home networks and small businesses that need to share resources between different operating systems. Samba is highly configurable and can be customized to suit the needs of different environments.

**Task**

* Create a directory and share it over the network 🡪 access it from Windows OS Client
* **$ rpm -qa | grep -I samba** 🡪 to check if Samba is already installed in system.
* *$ systemctl restart smb*
* *$ systemctl restart nmb*
* *$ systemctl enable smb: systemctl enable nmb*

🡪 root directory “/ect/samba/”

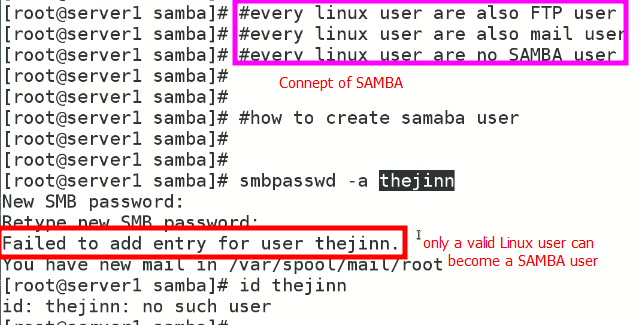
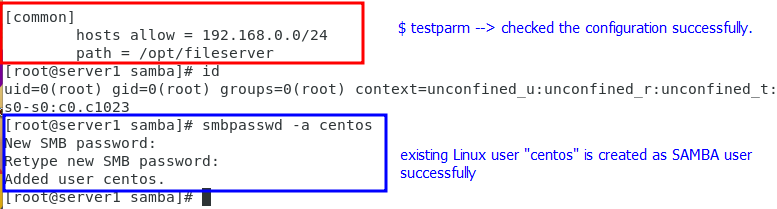
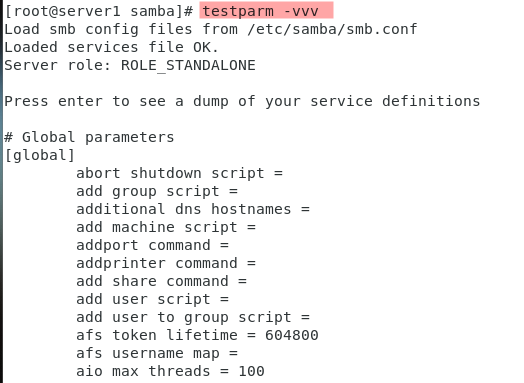
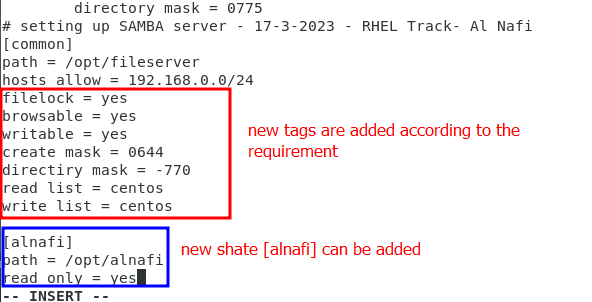
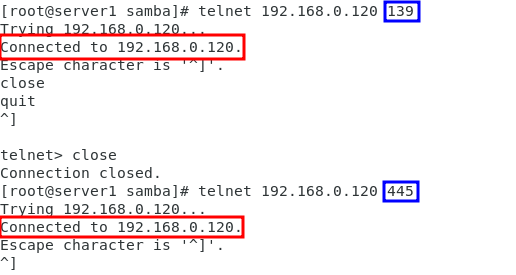
* 
* This conf file has two sections,
  + Global section
  + Share section.
* Edit it 🡪 $ vi smb.conf
* 
* ***[global], [homes], [printers] 🡪 these are share names and can be changed***
* For our task we are going to create a new “share”
*  IP address shows that all whole network in this range is allowd.
* Entry into “/etc/exports” 🡪 **/opt/fileserver, \* (sync,rw)**
* Test the configuration 🡪 **$ testparm** it will read all configuration and check for any syntax error. *(Press ENTER, and after the message on screen press ENTER again)*

**"testparm"** is a command that is commonly used in Samba, an open-source software suite that provides file and print services between different operating systems.

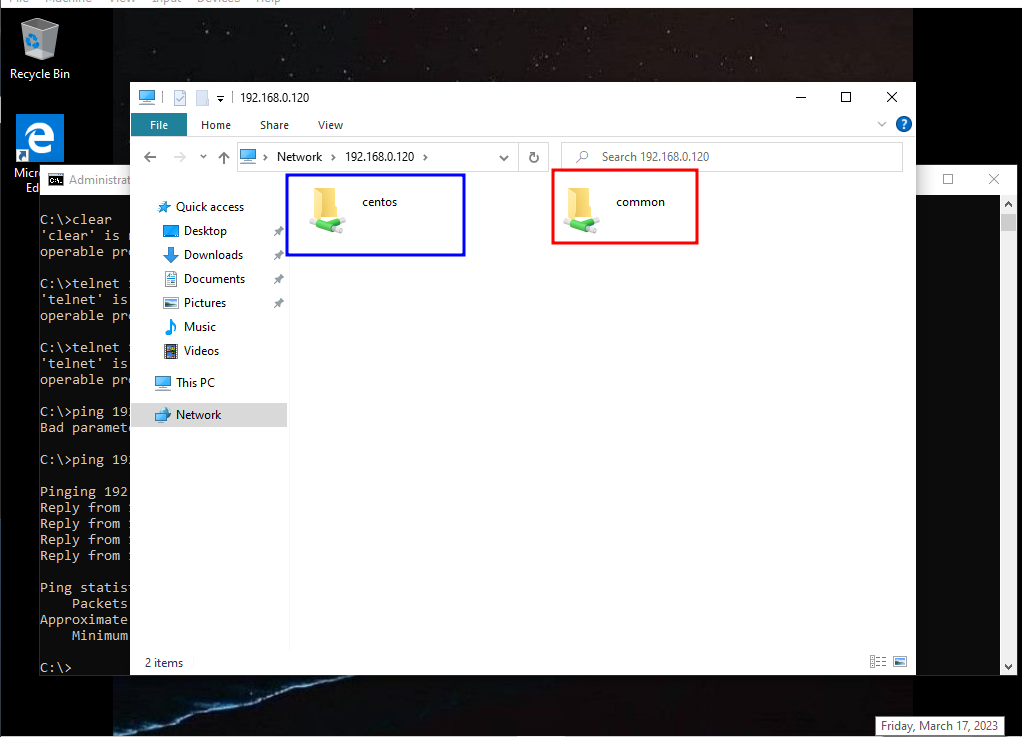
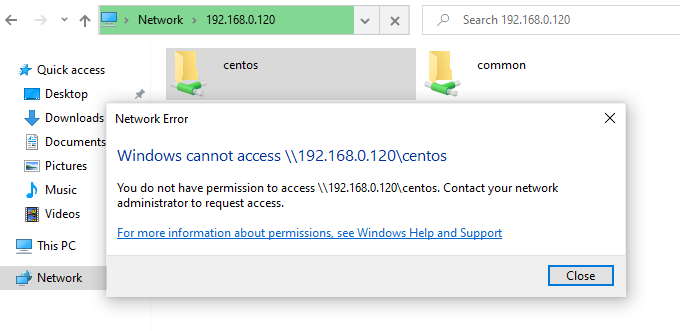
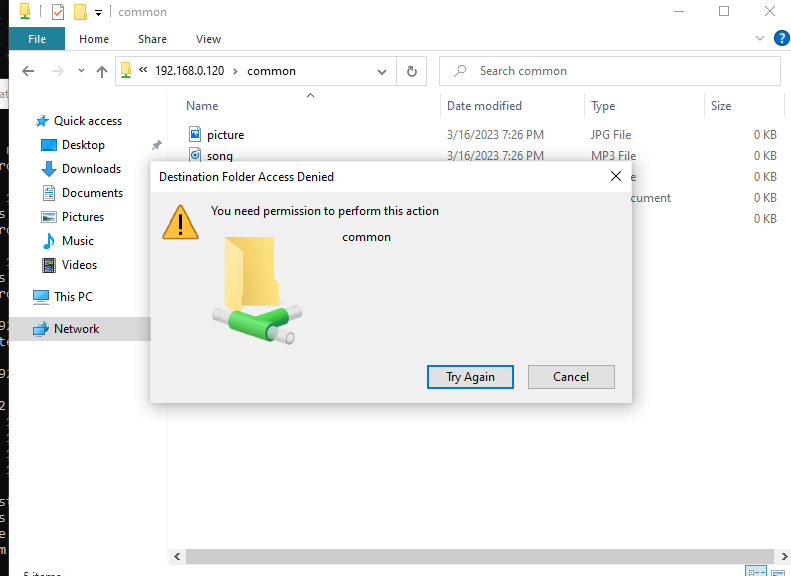
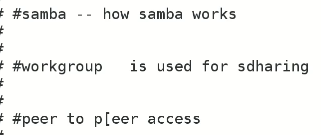
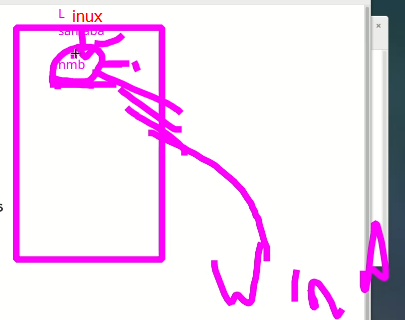
The "testparm" command is used to test the configuration file for Samba, usually named smb.conf, to ensure that there are no syntax errors or other problems that could prevent Samba from functioning properly. The command analyzes the configuration file and provides feedback on any issues found, allowing you to correct them before starting or restarting the Samba service.

If you are experiencing issues with the "testparm" command, make sure that you have Samba installed and that the command is being entered correctly. If you continue to experience issues, you may want to consult the documentation for Samba or seek support from the Samba community to troubleshoot the problem.

default port for samba is 137, 139 and 445

* **$ testparm → to test the script and configuration,**
* ports are explained as,
* 137 nmb
* 139 smb
* 445 for sharing
* .
* .
* 
* *Either add a new user by “useradd” command or create a valid user as Samba user*
* 
* If “tags” in configuration file are to be reviewed 🡪 **$ testparm -vvv** will list all available tags.
* 
* *.*
* 
* Check if port is up or not on server?
* **$ telnet (Server\_IP) <Port>**
* 
* Ports are up
* If connection is failed, 🡪 check ports if up or down in “”server”
* **$ systemctl restart smb**
* **$ systemctl restart nmb**
* 
* ***$ netstat -tulnp | grep -t*** <137 0r 139 0r 445>
* *Check if samba is added in firewall.*
* ***$ firewall-cmd --list-services***
* **$ firewall-cmd --permanent --add-service=samba** 🡪 add it to firewall

**After these steps to windows OS.**

* Open ***cmd*** and telnet <server\_IP> <Port>
* In run on windows machine \\<Server\_IP> e.g \\192.168.0.120
* Asking for username and password
* Files on CentOS 7 are opened on Windows 10
* 
* **Even it is accessible through my Host Machine (Windows 11 Pro) on my laptop.**
* But,
* Home directory is not accessible.
* 
* And
* Write permission in shared folder (common) is not granted.
* 
* .
* To grant **permissions** 🡪 on CentOS 7 (server) open **$ vi /etc/samba/smb.conf**
* There is a concept of “file lock” in file sharing.
  + It means if a file is accessed by multiple users 🡪 chances are high that it may be corrupted. Due to read and write permission.
  + So, if multiple users are accessing a single file 🡪 the 1st user with haver the read and write permission and all other users will have read only permission.
  + This is called **“file lock”.**
* The working of SAMB.
* Workgrop
* Domain controller DC
* 
* 
* 
* ***SAMBA can work across Linux and Windows platforms because of “nbm (NetBIOS)”***
* Same thing is not available in NFS that’s why I cant work across Linux and Windows platforms.
* Samba v4 🡪 *it is similar to Windows Active Directory.* (90% similar to AD)
* If Windows AD is controlling the network , and there is a Linux as client, it requires “winbind” to communicate with Linux machine.
* **Winbind** is a service that is provided by Samba, which is an open-source software suite that provides file and print services to Linux/Unix systems from Windows clients. Winbind allows Linux/Unix systems to integrate with Windows domains, providing a centralized authentication and authorization mechanism for users and groups in the Windows domain.
* When Winbind is installed and configured on a Linux/Unix system, it enables the system to authenticate users against the Windows domain controller and obtain user and group information from the domain. This allows users to log in to the Linux/Unix system using their Windows domain credentials, and for Linux/Unix systems to use Windows domain groups for access control and authorization purposes.
* Winbind can be used in conjunction with other services such as Samba, which provides file and print services, and the Pluggable Authentication Module (PAM), which provides a standardized interface for authentication services in Linux/Unix systems. Together, these services allow Linux/Unix systems to seamlessly integrate with Windows domains, providing a more cohesive and consistent experience for network users.
* ***Overall, Winbind is a powerful tool for integrating Linux/Unix systems with Windows domains, allowing users to take advantage of the benefits of both platforms in a single network environment.***

**windows active directory short definition**

* Windows Active Directory (AD) is a centralized database that stores information about users, computers, and other network resources in a Windows domain-based network. Active Directory provides authentication and authorization services, allowing network administrators to manage and control access to network resources based on user identity and group membership.
* With Active Directory, administrators can manage user accounts, group policies, security settings, and other network resources from a central location, providing a more efficient and consistent approach to network management. Active Directory also supports the use of trust relationships between domains, enabling organizations to integrate different parts of their network into a single, cohesive directory service.
* In addition, Active Directory provides support for other services such as domain name resolution, which translates human-readable domain names into IP addresses, and distributed file system, which enables network users to access and manage files stored across multiple servers as if they were stored on a single server.
* Overall, Windows Active Directory plays a critical role in managing user and computer accounts, network resources, and security in Windows-based networks.
* .
* In Microsoft Windows, "workgroup" and "domain controller" are terms used to describe different types of network configurations for managing resources such as files, printers, and user accounts.
* A workgroup is a basic peer-to-peer network model that allows multiple computers to connect and share resources without the need for a central server or authority. In a workgroup, each computer maintains its own list of user accounts, and resources are shared by granting permissions to specific user accounts or groups on a per-resource basis. Workgroups are typically used in small networks with fewer than 10 computers, and they are relatively simple to set up and manage.
* On the other hand, a domain controller is a central server that manages user accounts, authentication, and access control for a network of computers and resources. In a domain-based network, all user accounts and permissions are centrally managed by the domain controller, which is responsible for authenticating users and enforcing access control policies across the entire network. This allows for more centralized control and management of resources, and enables more advanced features such as Group Policy, which can be used to configure and enforce settings on multiple computers at once.
* In summary, a workgroup is a simple peer-to-peer network model that is suitable for small networks, while a domain-based network with a domain controller provides centralized management and control of resources and is suitable for larger networks with more complex management requirements.
* **how this phenomenon is different if we compare it to Linux**
* In Linux, the concepts of "workgroup" and "domain controller" are not as prominent as they are in Microsoft Windows. Instead, Linux systems typically use a combination of protocols and tools such as the Network File System (NFS), the Common Internet File System (CIFS), and the Lightweight Directory Access Protocol (LDAP) to manage network resources and user accounts.
* In a Linux-based network, file and print sharing can be achieved using the NFS or CIFS protocols, which allow for the sharing of files and directories between Linux and other systems. User authentication and access control can be managed using LDAP or other directory services, which provide centralized user account management and authentication across multiple systems.
* While there are some Linux-based solutions that provide similar functionality to Microsoft's domain controller, such as the Samba software suite, these are not as widely used or as tightly integrated into the operating system as the Windows domain controller. Additionally, Linux systems tend to be more flexible and customizable than Windows systems, which can make it easier to set up and manage networks with specific requirements.
* In summary, while Linux systems offer many similar capabilities for network resource sharing and user authentication as Windows, the specific tools and protocols used to achieve these goals may be different, and the concept of a domain controller is not as central to Linux-based network management as it is to Windows-based network management.
* ,
* **redefine it in the context of Samba in Linux**
* In the context of Samba in Linux, "workgroup" and "domain controller" are similar to their Windows counterparts in that they refer to different ways of managing network resources and user accounts.
* A workgroup in Samba is a collection of computers that share resources, such as files and printers, without the need for a central server or authority. In Samba, each computer in the workgroup maintains its own list of user accounts, and resources are shared by granting permissions to specific user accounts or groups on a per-resource basis. Samba workgroups are typically used in small networks with fewer than 10 computers, and they are relatively simple to set up and manage.
* A domain controller in Samba is a central server that manages user accounts, authentication, and access control for a network of computers and resources. In a domain-based network, all user accounts and permissions are centrally managed by the Samba domain controller, which is responsible for authenticating users and enforcing access control policies across the entire network. This allows for more centralized control and management of resources, and enables more advanced features such as Group Policy, which can be used to configure and enforce settings on multiple computers at once.
* Samba also provides the ability to integrate with existing Windows-based domains, allowing Linux systems to be managed using the same domain controller and user accounts as Windows systems. This can be useful for organizations that have a mix of Linux and Windows systems and want to manage them using a single set of user accounts and access control policies.
* In summary, in the context of Samba in Linux, workgroups and domain controllers are similar to their Windows counterparts in that they provide different ways of managing network resources and user accounts, but they use different tools and protocols to achieve these goals. Samba provides the flexibility to use either approach or integrate with existing Windows domains as needed.
* .

**example of centralized authentication with AD in windows and Linux**

Here's an example of centralized authentication with Active Directory (AD) in both Windows and Linux:

1. Windows: In a Windows environment, you would set up AD as a domain controller, which would store user accounts and authentication information centrally. Users would be able to log in to any Windows system on the network using their domain credentials, and access to resources such as files and printers would be controlled based on their permissions in the AD domain.
2. Linux: In a Linux environment, you would install the Winbind service, which enables the Linux system to authenticate against the AD domain controller and obtain user and group information. You would configure the Linux system to use Winbind for authentication, and set up access control based on AD groups.

To provide a specific example, let's say you have a network with a Windows Server domain controller running AD, and several Linux servers running Ubuntu. You want users to be able to log in to any Linux server using their Windows domain credentials.

To achieve this, you would:

1. Install Winbind on each Linux server: You would install the winbind package using the package manager (e.g. apt-get install winbind).
2. Join the Linux servers to the AD domain: You would use the net join command to join each Linux server to the AD domain. This would involve providing the domain name, administrator credentials, and other relevant information.
3. Configure Winbind: You would configure the /etc/nsswitch.conf file to use winbind for authentication, and set up the /etc/samba/smb.conf file to specify the domain controller and other relevant configuration details.
4. Test authentication: You would test authentication by attempting to log in to a Linux server using a Windows domain account. If successful, the user would be able to log in to the Linux server and access resources based on their permissions in the AD domain.

By setting up centralized authentication using AD and Winbind, you can provide a seamless experience for users across both Windows and Linux platforms, and simplify the management of user accounts and access control.

**what is a domain controller ?**

A domain controller is a server that manages a centralized database of user accounts, passwords, and other security-related information for a Windows domain. It is a key component of the Windows Active Directory infrastructure and is responsible for authenticating users, granting access to network resources, and enforcing security policies.

When a user attempts to log in to a Windows-based network, the domain controller is responsible for verifying the user's identity and credentials, and granting access to the appropriate resources based on their permissions in the domain. The domain controller also maintains a record of user activity and manages security policies, such as password complexity and account lockout settings.

In addition to authentication and access control, a domain controller also provides other services such as domain name resolution, which translates human-readable domain names into IP addresses, and replication, which ensures that domain data is consistent across multiple domain controllers.

Overall, a domain controller plays a critical role in managing user accounts and security in a Windows-based network, and is a key component of the Active Directory infrastructure.

**why its is called domain, why there is not other term used ?**

The term "domain" is used in Windows Active Directory to refer to a logical grouping of resources, including users, computers, and network resources, that are managed as a single entity. The term "domain" was chosen because it reflects the idea of a group of objects that are related to each other and are under a single administrative authority.

In the context of Windows Active Directory, a domain represents a security boundary, with each domain having its own unique security policies and user accounts. Users can log in to any computer in the domain and access resources based on their permissions and group memberships, regardless of the physical location of the computer or user.

The term "domain" was chosen as an alternative to other terms such as "realm" or "directory," which were also considered. However, "domain" was chosen because it was felt to be a more descriptive and intuitive term that conveyed the idea of a logical grouping of related objects.

In summary, the term "domain" is used in Windows Active Directory to represent a logical grouping of resources that are managed as a single entity, with each domain having its own unique security policies and user accounts. The term was chosen for its descriptive and intuitive qualities.

* .

**if i am a computer software engineer and I am creating such method what alternative name I can give instead of "domain" ?**

As a computer software engineer, if you were creating a method similar to Windows Active Directory, but wanted to use an alternative name instead of "domain," there are a few options you could consider:

1. Realm: This term is commonly used in other authentication systems, such as Kerberos, and refers to a logical grouping of resources and users that share a common security policy.
2. Organization: This term could be used to describe a logical grouping of resources and users within an organization, such as a company or institution.
3. Cluster: This term could be used to describe a grouping of resources and users that are clustered together based on their function or purpose.
4. Group: This term could be used to describe a logical grouping of users and resources based on their permissions or access level.

Ultimately, the choice of name would depend on the specific requirements and context of the system being developed, as well as the preferences of the developer and stakeholders involved.