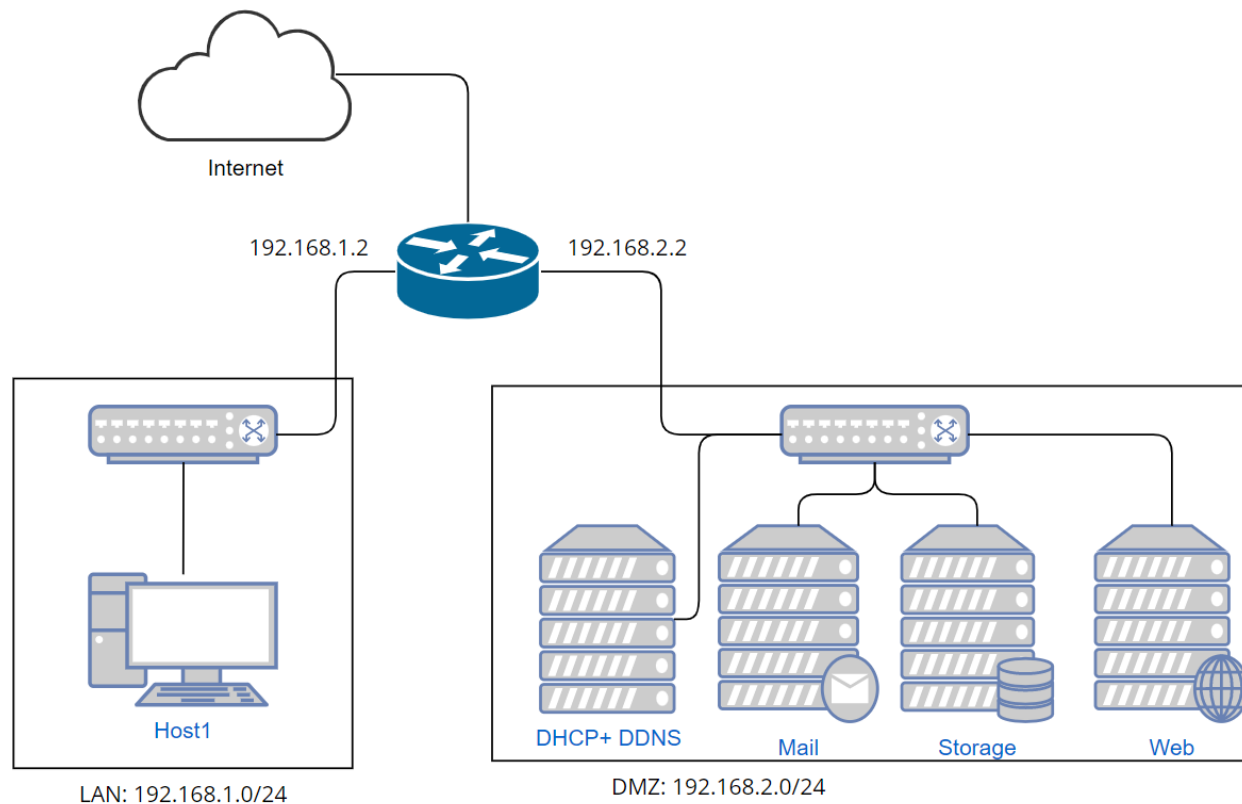


Reminder of the previous session

Problematic

- Enterprise Network Architecture



Web Servers

Prof. Dr. Soufiane Hourri



Introduction to Web Servers

What is a web server ?

- A software program that handles requests from clients and serves web pages, files, or other resources
- Receives requests from web browsers or other client applications via HTTP or HTTPS
- Processes requests and returns responses in the form of web pages or other content
- Can handle other tasks such as running web applications, databases, or managing user access and authentication
- Some common web servers include Apache, Nginx, and Microsoft IIS.



Apache

- An open-source web server software that is widely used on Unix-based systems
- Provides support for multiple programming languages, such as PHP, Python, and Perl
- Offers a modular architecture that allows users to add or remove functionality as needed
- Has a large and active community that provides support, documentation, and plugins
- Is often used in combination with other open-source software such as MySQL or PostgreSQL for database management



Nginx

- A high-performance, open-source web server software that is designed to handle large traffic volumes
- Can be used as a reverse proxy or load balancer to distribute traffic across multiple servers
- Offers support for multiple protocols, such as HTTP, HTTPS, and WebSocket
- Has a low memory footprint and is optimized for serving static files and handling concurrent connections
- Is often used in combination with other software such as PHP-FPM or Node.js for dynamic content generation.



Microsoft IIS

- A web server software that is designed for Windows-based systems
- Offers support for ASP.NET web applications and other Microsoft technologies such as SharePoint or Exchange
- Provides features such as integrated Windows authentication, SSL/TLS encryption, and dynamic content caching
- Has a graphical user interface that makes it easy to configure and manage web applications
- Is often used in combination with other Microsoft software such as SQL Server or Visual Studio for application development and deployment.



Lighttpd

- A lightweight and fast web server software that is designed for serving static files and handling high traffic volumes
- Has a low memory footprint and is optimized for serving large numbers of concurrent connections
- Provides features such as URL rewriting, custom error pages, and HTTP compression
- Is often used in combination with other open-source software such as MySQL or PostgreSQL for database management.



Caddy

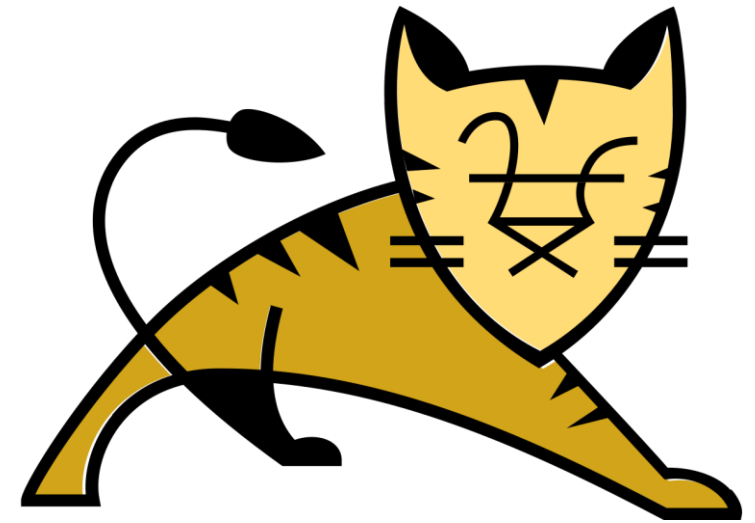
- A modern, open-source web server software that provides automatic HTTPS encryption, HTTP/3 support, and easy configuration
- Offers support for multiple programming languages and application protocols, such as PHP, Python, and Node.js
- Has a simple and intuitive configuration file format that allows users to easily customize their server setup
- Provides features such as virtual hosting, reverse proxying, and rate limiting
- Is often used in combination with other open-source software such as Let's Encrypt for automated SSL/TLS certificate management.



Caddy[®]
THE ULTIMATE SERVER

Tomcat

- A Java-based web server software that is designed for serving dynamic Java-based web applications
- Has a built-in servlet container that provides support for Java Server Pages (JSP) and Java Servlets
- Offers support for multiple programming languages and application protocols, such as PHP and Ruby
- Provides features such as session management, clustering, and load balancing
- Is often used in combination with other Java-based technologies such as Spring Framework or Hibernate for application development and deployment.



Web Server Software in Fedora 37

- Fedora 37 includes several popular web server software packages, such as Apache HTTP Server, Nginx, Lighttpd, and Caddy.
- These web servers are available in the official Fedora repositories and can be easily installed and configured using the command-line interface or graphical user interface.
- Fedora 37 also includes other software packages that are commonly used with web servers, such as PHP, MySQL, and PostgreSQL.
- These packages can be installed and configured to work together with the web servers to provide a complete web development and hosting environment.
- Fedora 37 offers regular updates and security patches for its software packages, ensuring that users have access to the latest features and bug fixes.





Installing and Configuring Apache Web Server



Installing and Configuring Apache Web Server

Install Apache HTTPD Server by running the following command in the terminal:

```
$ sudo dnf install httpd
```



Installing and Configuring Apache Web Server

Once installed, start the Apache server by running:

```
$ sudo systemctl start httpd.service
```



Installing and Configuring Apache Web Server

To ensure that Apache starts automatically at boot time, run:

```
$ sudo systemctl enable httpd.service
```




Installing and Configuring Apache Web Server

Next, create a directory to store your website files by running:

```
$ sudo mkdir -p /var/www/html/est.intra
```



Installing and Configuring Apache Web Server

Change the ownership of the `/var/www/html` directory to the Apache user by running:

```
$ sudo chown -R apache:apache /var/www/html/
```

Installing and Configuring Apache Web Server

Create an index.html file in the /var/www/html/est.intra directory with the following command:

```
$ sudo nano /var/www/html/est.intra/index.html
```

This will open a text editor where you can add the content for your website. Once done, save and exit the editor.



Installing and Configuring Apache Web Server

To configure Apache to serve the website files from the est.intra directory, create a new virtual host configuration file by running:

```
$ sudo nano /etc/httpd/conf.d/est.intra.conf
```

Installing and Configuring Apache Web Server

Add the following content to the configuration file:

```
<VirtualHost *:80>  
    ServerName www.est.intra  
    DocumentRoot /var/www/html/est.intra  
    ErrorLog /var/log/httpd/est.intra-error.log  
    CustomLog /var/log/httpd/est.intra-access.log combined  
</VirtualHost>
```

This configuration sets up the virtual host for the `www.est.intra` domain, specifies the document root as `/var/www/html/est.intra`, and sets up error and access logs for the site.



Installing and Configuring Apache Web Server

Finally, restart the Apache server to apply the changes:

```
$ sudo systemctl restart httpd.service
```

Your website should now be accessible by visiting <http://www.est.intra> in your web browser.



Installing and Configuring PHP

Installing and Configuring PHP

Install the PHP package and its dependencies by running the following command in the terminal:

```
$ sudo dnf install php php-mysqlnd
```


Installing and Configuring PHP

Once installed, restart the Apache server to load the PHP module:

```
$ sudo systemctl restart httpd.service
```

Installing and Configuring PHP

This will open a text editor where you can add the PHP code to print "Hello, World!". Add the following content:

```
<?php  
echo "Hello, World!";  
?>
```

Installing and Configuring PHP

To configure Apache to serve index.php as the default file for the est.intra site, edit the /etc/httpd/conf/httpd.conf file by running:

```
$ sudo nano /etc/httpd/conf/httpd.conf
```

Installing and Configuring PHP

Look for the following line in the file:

```
$ DirectoryIndex index.html
```

Change it to:

```
$ DirectoryIndex index.php index.html
```

This tells Apache to serve index.php as the default file if it exists in the directory.

Finally, restart the Apache server to apply the changes:

```
sudo systemctl restart httpd.service
```

Your website should now be accessible by visiting `http://www.est.intra` in your web browser, and it should display the "Hello, World!" message.



Installing and Configuring MySQL

Installing and Configuring MySQL

Install the MySQL community release package repository by running the following command in the terminal:

```
$ sudo dnf install  
https://dev.mysql.com/get/mysql80-community-release-  
fc37-4.noarch.rpm
```

Installing and Configuring MySQL

Once installed, run the following command to enable the MySQL module:

```
$ sudo dnf module enable mysql:8.0
```

Installing and Configuring MySQL

Install the MySQL server package by running the following command:

```
$ sudo dnf install mysql-server
```


Installing and Configuring MySQL

Once installed, start the MySQL service by running:

```
$ sudo systemctl start mysqld
```

Installing and Configuring MySQL

Run the following command to secure the MySQL installation:

```
$ sudo mysql_secure_installation
```

This command will prompt you to set a root password for the MySQL server, and ask you some security-related questions. Follow the prompts to complete the process.

Installing and Configuring MySQL

Once you've secured the MySQL installation, you can log in to the MySQL server with the following command:

```
$ sudo mysql -u root -p
```

You'll be prompted to enter the root password you set in the previous step.

Installing and Configuring MySQL

Now you can create a new database and user for your website. For example, to create a database called "estdb" and a user called "estuser" with a password "password", run the following commands:

```
CREATE DATABASE estdb;  
GRANT ALL ON estdb.* TO 'estuser'@'localhost'  
IDENTIFIED BY 'password';
```

Installing and Configuring MySQL

Finally, restart the MySQL service to apply the changes:

```
sudo systemctl restart mysqld
```

MySQL is now installed and ready to be used by your website. You can use the "estuser" account with the password "password" to access the "estdb" database from your PHP code.



Installing and Configuring PhpMyAdmin

Installing and Configuring PhpMyAdmin

Install phpMyAdmin and its dependencies by running the following command in the terminal:

```
$ sudo dnf install phpMyAdmin
```

Installing and Configuring PhpMyAdmin

Once installed, edit the `/etc/httpd/conf.d/phpMyAdmin.conf` file to allow access to phpMyAdmin from your web browser. You can do this by running the following command:

```
$ sudo nano /etc/httpd/conf.d/phpMyAdmin.conf
```


Installing and Configuring PhpMyAdmin

Look for the following lines in the file:

```
# Require ip 127.0.0.1
```

```
# Require ip ::1
```

Uncomment these lines by removing the "#" at the beginning of each line. This will allow access to phpMyAdmin from any IP address.

Installing and Configuring PhpMyAdmin

Restart the Apache server to apply the changes:

```
$ sudo systemctl restart httpd.service
```

You should now be able to access phpMyAdmin by visiting <http://localhost/phpMyAdmin/> in your web browser. Log in with your MySQL username and password to manage your databases.



Installing and Configuring PhpMyAdmin

- If you want to access phpMyAdmin on the same machine where MySQL and Apache are installed, you can access it by visiting **`http://localhost/phpMyAdmin/`** in your web browser.
- However, if you want to access phpMyAdmin from another machine on the network, you can use the IP address or hostname of the machine where MySQL and Apache are installed instead of "localhost". For example, if the IP address of the machine is 192.168.1.1, you can access phpMyAdmin by visiting **`http://192.168.1.1/phpMyAdmin/`** in your web browser.
- In the case of the est.intra domain, you would need to set up the DNS or hosts file on the machine you're trying to access phpMyAdmin from to resolve the est.intra domain to the IP address of the machine where MySQL and Apache are installed. Once that's set up, you should be able to access phpMyAdmin by visiting **`http://est.intra/phpMyAdmin/`** in your web browser.

Active Directory

Prof. Dr. Soufiane Hourri



Problematic

Problematic


- Company has multiple departments and locations with different user accounts, groups, and resources
- Manual management is time-consuming and error-prone
- Some employees have incorrect or unnecessary access to resources, while others are locked out
- Employees who transfer between departments or locations have trouble accessing necessary resources



Solutions

- ✓ **Active Directory** can streamline user account and resource management
- ✓ Standardized approach can save time and reduce errors
- ✓ **Active Directory** can ensure that employees have access to necessary resources while keeping unauthorized users out

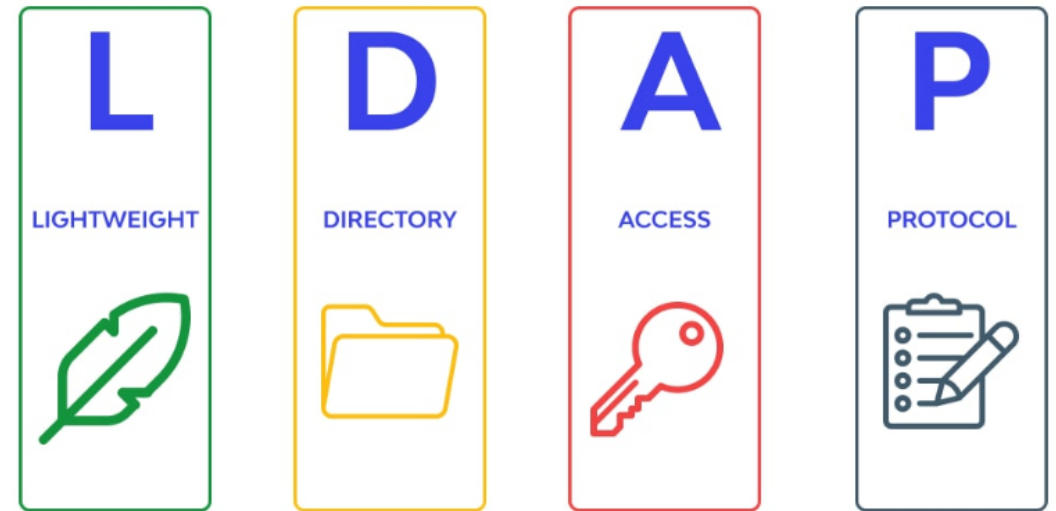




Introduction to Lightweight Directory Access Protocol (LDAP)

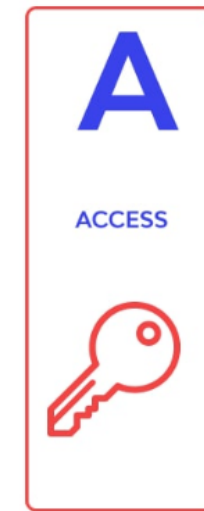
Features of LDAP

- LDAP has two main goals:
 - Store data in the LDAP directory
 - Authenticate users to access the directory
- LDAP provides the communication language that applications require to send and receive information from directory services
- LDAP functions as an Identity and Access Management (IAM) solution targeting user authentication, including support for Kerberos and single sign-on (SSO), Simple Authentication Security Layer (SASL), and Secure Sockets Layer (SSL)



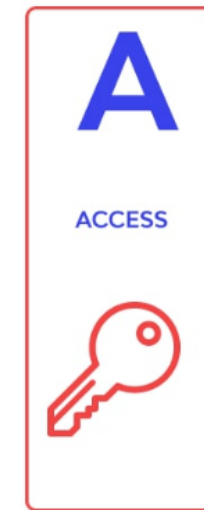
LDAP Directory Services

- A directory service provides access to information on organizations, individuals, and other data within a network
- LDAP enables organizations to store, manage, and secure information about the organization, its users, and assets
- Hierarchical structure of information simplifies storage access
- The most common LDAP use case is providing a central location for accessing and managing directory services



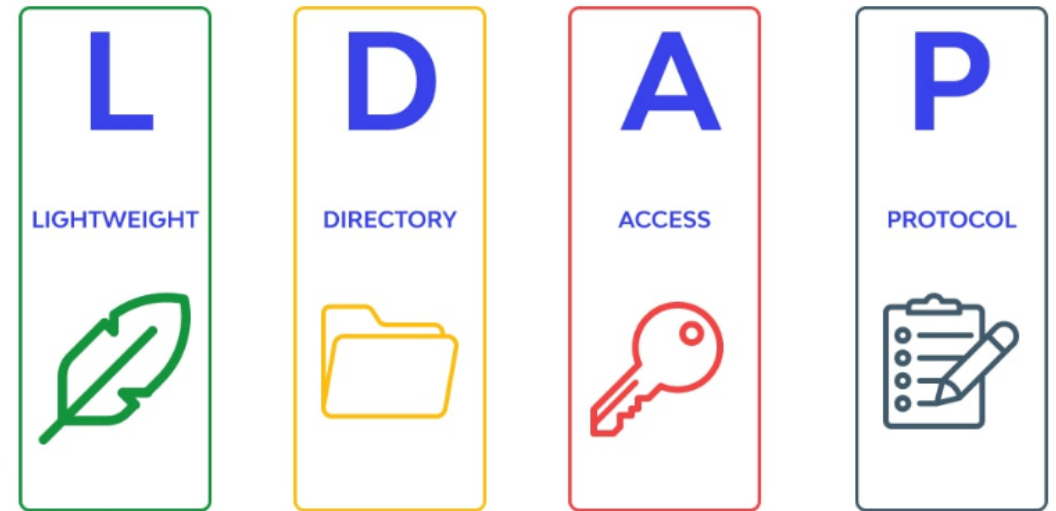
LDAP and DNS

- LDAP is used to locate data about organizations, individuals, files, and devices in a network
- DNS relates a domain name to a specific network address, but LDAP allows a user to search for an individual without knowing where they are located
- LDAP provides a way to search for data in a network, even without knowing the domain name



Advantages of LDAP

- LDAP provides a standardized way to manage and access data stored in a directory
- It simplifies storage access by providing a hierarchical structure of information
- LDAP enables secure authentication of users to access the directory, providing an IAM solution for organizations
- It is efficient for network communication due to its lightweight design and smaller code
- LDAP is widely used in enterprise and internet applications for directory services and authentication purposes





What is Active Directory ?

Definition of Active Directory

- **Active Directory** is a **Microsoft directory service** that provides a **centralized** and **hierarchical** database for managing network resources, storing information about objects on a network, and making this information available to users and administrators.
- Active Directory is a service that enables administrators to **define settings** for computers and users in an Active Directory environment and **control access to resources** based on user roles and permissions.
- Active Directory allows users to **authenticate** and access resources on the network and provides a framework for **assigning policies, deploying software, and distributing updates** to networked computers.



Functions of Active Directory

- Active Directory serves as a **single sign-on (SSO)** mechanism that allows users to log in to the network once and have access to all resources for which they are authorized.
- Active Directory provides a **domain-based architecture** that enables centralized administration and delegation of administrative responsibilities, allowing for easier management of network resources.
- Active Directory serves as a **framework for assigning policies**, deploying software, and distributing updates to networked computers, allowing administrators to define and manage settings for computers and users in an Active Directory environment.



Services provided by Active Directory

- Active Directory provides a range of services, including Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Lightweight Directory Access Protocol (LDAP), that allow for integration with other network services and protocols.
- It provides Group Policy, which enables administrators to define and manage settings for computers and users in an Active Directory environment, allowing for easier management of network resources and more consistent user experiences.



Benefits of using Active Directory

- Active Directory simplifies network administration by providing a central location for managing network resources, making it easier for administrators to manage users, computers, and groups in a hierarchical structure.
- It improves security by allowing administrators to control access to resources based on user roles and permissions, ensuring that users only have access to the resources they need to perform their work.
- Active Directory enhances user productivity by providing a single sign-on mechanism and enabling easy access to network resources, which saves time and reduces the burden on users to remember multiple login credentials.



Limitations of Active Directory

- Active Directory requires dedicated hardware and software to run, which can be costly to implement and maintain.
- It can be complex to set up and administer, requiring a significant level of technical expertise and training for administrators.
- Active Directory may not be suitable for small or simple networks, as its complexity may outweigh its benefits in these scenarios.

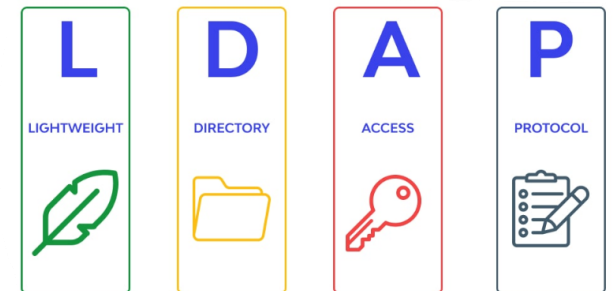




Active Directory and LDAP

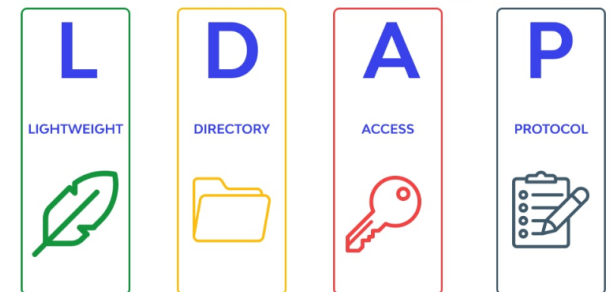
Introduction to LDAP and Active Directory

- LDAP is a protocol used for accessing and managing directory services running on TCP/IP.
- Active Directory is a large directory service database that contains information spanning every user account in a network.
- LDAP is the core protocol used in Active Directory, but it is not exclusive to it.
- The most recent version is LDAPv3.



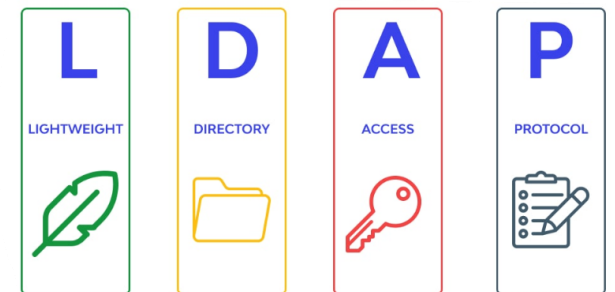
LDAP's Role in Active Directory

- LDAP provides a central location for accessing and managing directory services running on TCP/IP.
- LDAP is used to communicate with, store, and extract objects (i.e. domains, users, groups, etc.) from Active Directory into a usable format for its own directory, located on the LDAP server.
- LDAP enables applications to access and manage Active Directory objects in a standardized manner.
- LDAP is responsible for querying Active Directory and providing information to other applications or services.



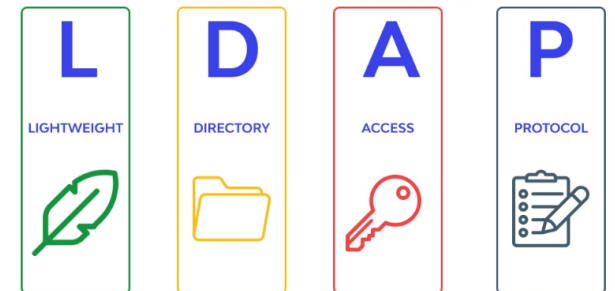
LDAP vs. Active Directory Database

- LDAP is a protocol used for accessing and managing directory services running on TCP/IP.
- Active Directory is a database that contains user account information, and it uses LDAP for querying.
- LDAP specializes in finding a directory object with little information, so it doesn't need to extract all of its attributes from Active Directory, or whichever directory service it is pulling from.
- Active Directory contains more attributes than what is pulled into LDAP.



The Importance of LDAP in Active Directory

- LDAP plays a vital role in the functionality of Active Directory.
- It enables applications to access and manage Active Directory objects in a standardized manner.
- LDAP provides a central location for accessing and managing directory services running on TCP/IP.
- LDAP is responsible for querying Active Directory and providing information to other applications or services.
- Without LDAP, Active Directory would not be able to function properly.

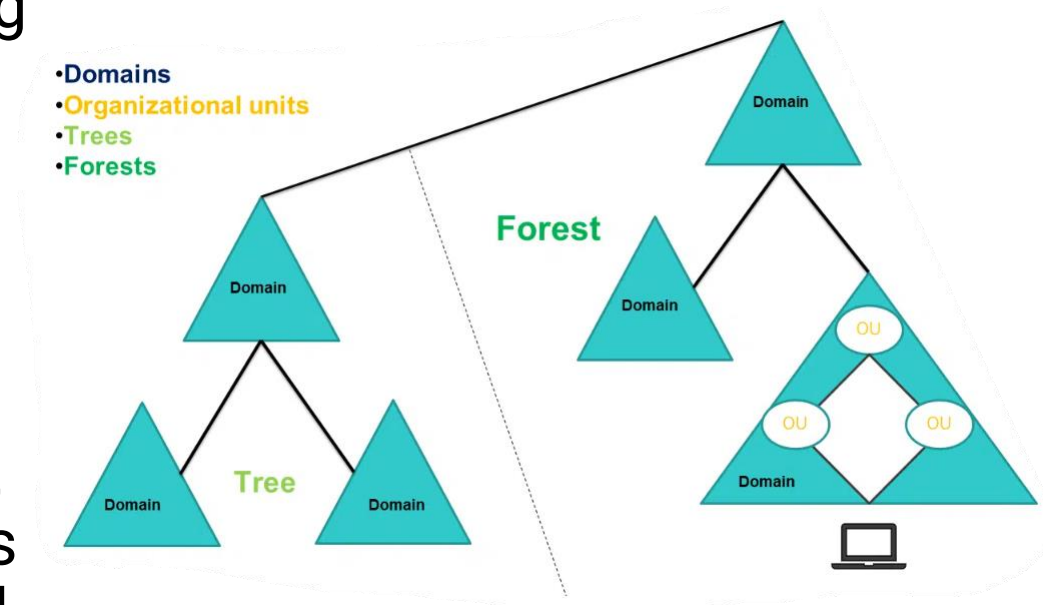




Active Directory Architecture and Design

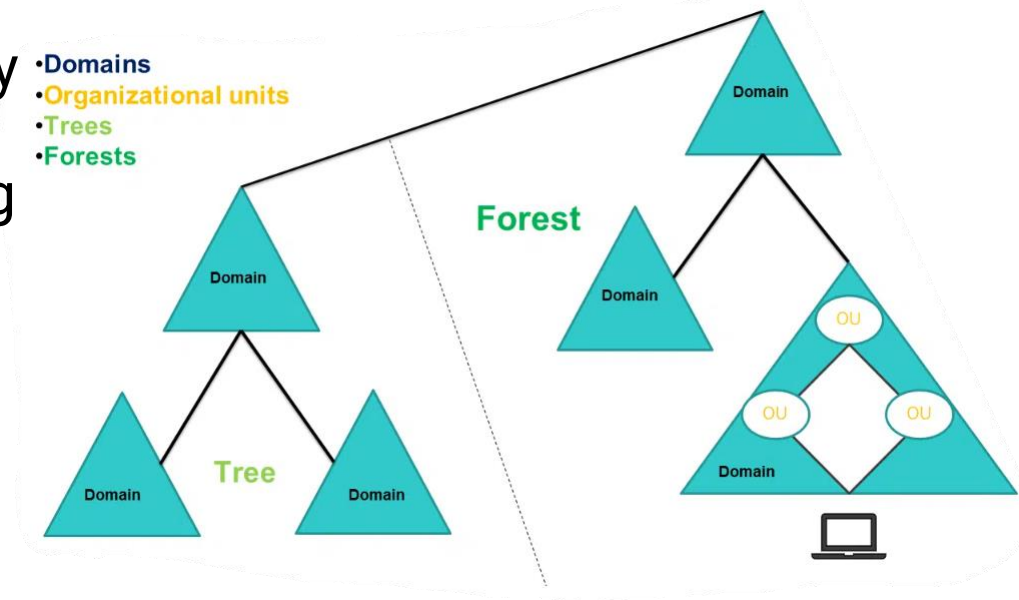
Overview of Active Directory architecture

- Active Directory is based on a domain-based architecture, where a **domain** is a logical grouping of computers, users, and resources that share a common security policy and database.
- **Domains** are organized into **trees**, which are collections of one or more domains that share a contiguous namespace and a common schema.
- Multiple trees can be connected to form a **forest**, which is a collection of one or more domain trees that share a common schema, configuration, and global catalog.



Active Directory components

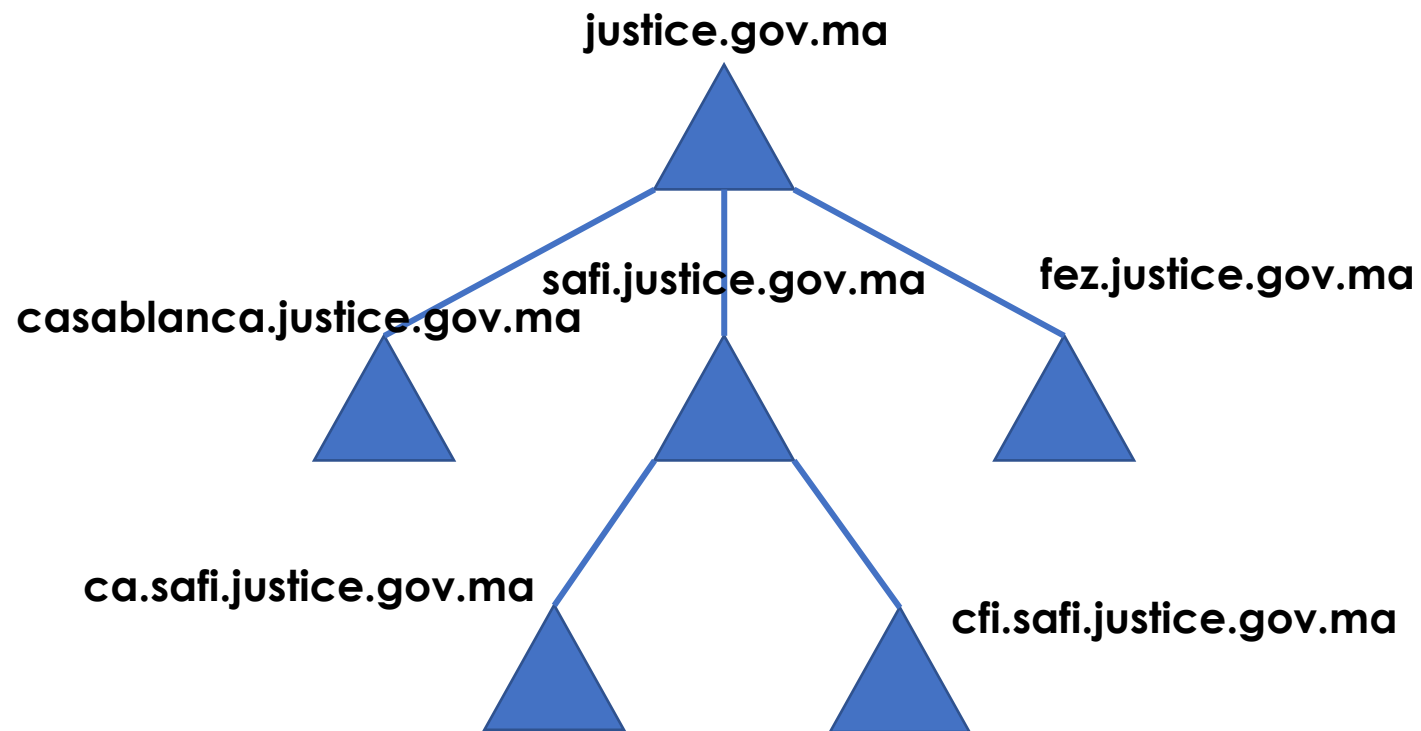
- Active Directory is composed of several components, including **domain controllers**, **sites**, and **trusts**.
- **Domain controllers** are servers that run Active Directory and contain a copy of the Active Directory database. They are responsible for authenticating users, providing directory information, and replicating changes to other domain controllers.
- **Sites** are collections of IP subnets that represent physical locations in the network. They are used to manage replication traffic and optimize network performance.
- **Trusts** are relationships between domains that allow users in one domain to access resources in another domain.



Active Directory design considerations

- When designing an Active Directory environment, several factors need to be considered, including **scalability**, **availability**, **security**, and **performance**.
- **Scalability** considerations include the number of users and resources that need to be managed and the expected growth of the network.
- **Availability** considerations include the need for redundancy and fault tolerance to ensure that Active Directory services are available when needed.
- **Security** considerations include the need to protect sensitive data and control access to resources based on user roles and permissions.
- **Performance** considerations include the need to optimize network traffic and minimize the impact of replication on network resources.

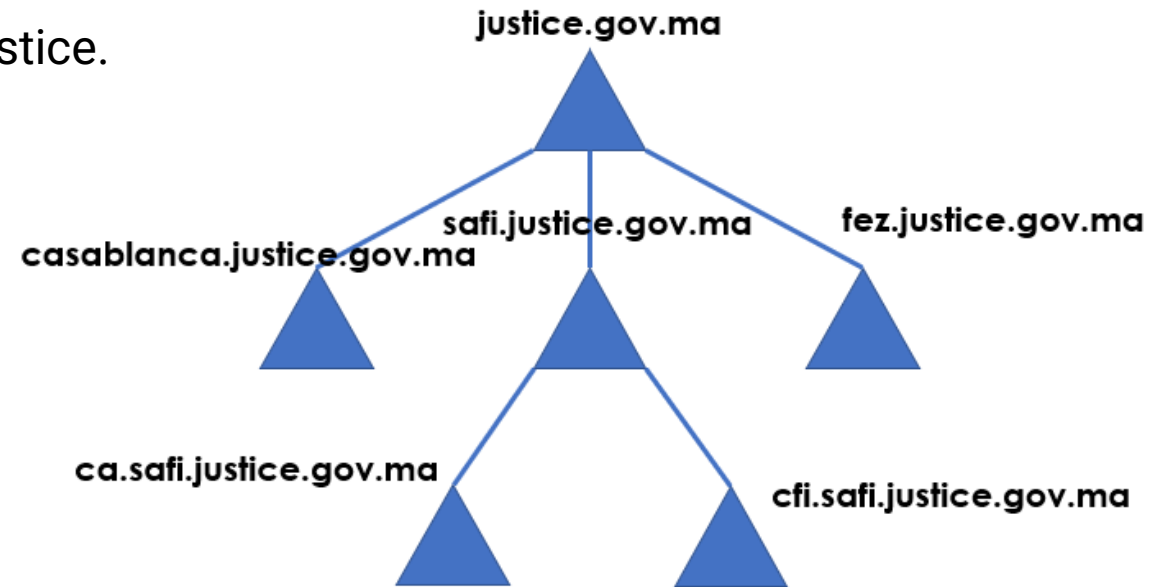
Example of *justice.gov.ma*



Example of *justice.gov.ma*

Domains

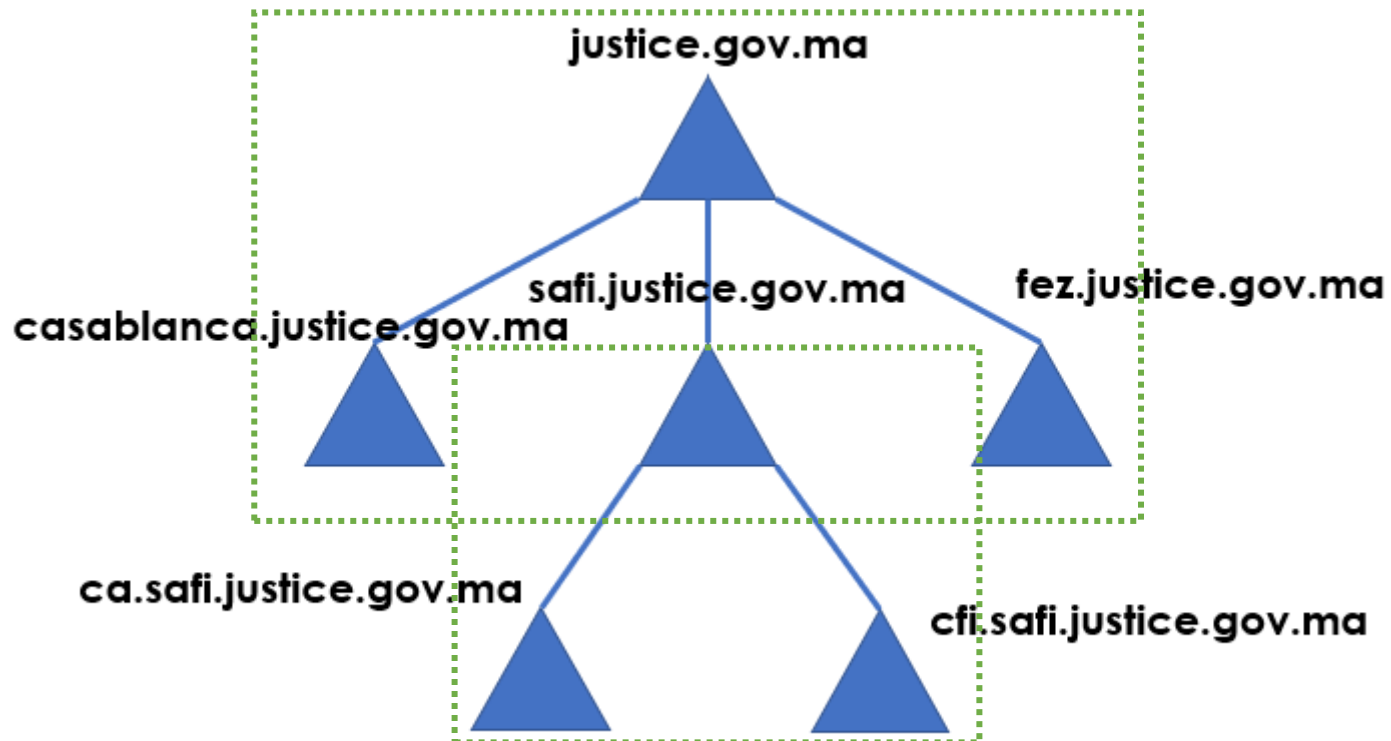
- **justice.gov.ma**
 - This is the top-level domain for the Ministry of Justice.
- **casablanca.justice.gov.ma**
 - This is the domain for the Casablanca courts.
- **fez.justice.gov.ma**
 - This is the domain for the Fez courts.
- **marrakech.justice.gov.ma**
 - This is the domain for the Marrakech courts.
- **safi.justice.gov.ma**
 - This is the domain for the Safi courts.



Example of *justice.gov.ma*

Tree

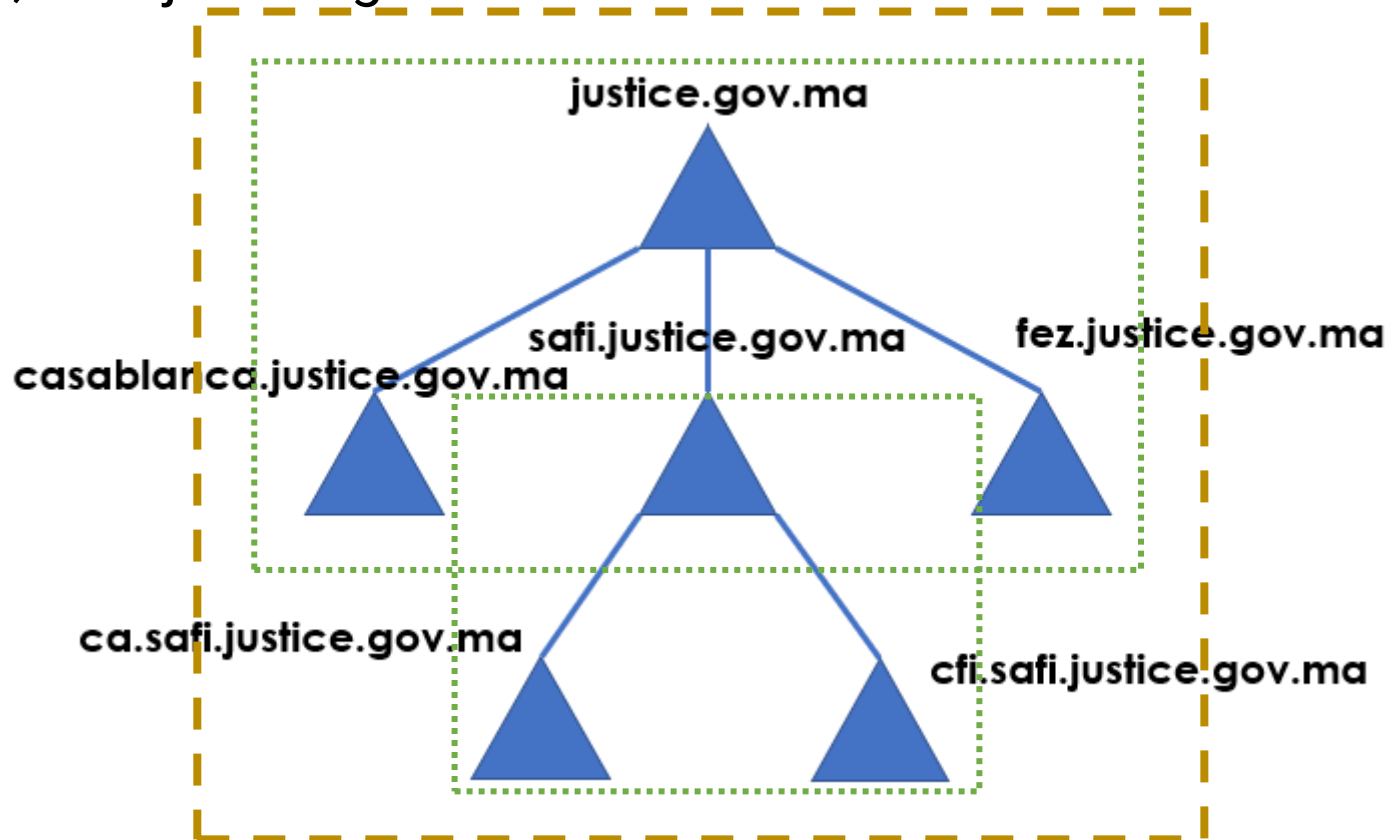
The domains for each region would be part of an Active Directory tree, with *justice.gov.ma* as the root domain.



Example of *justice.gov.ma*

Forest

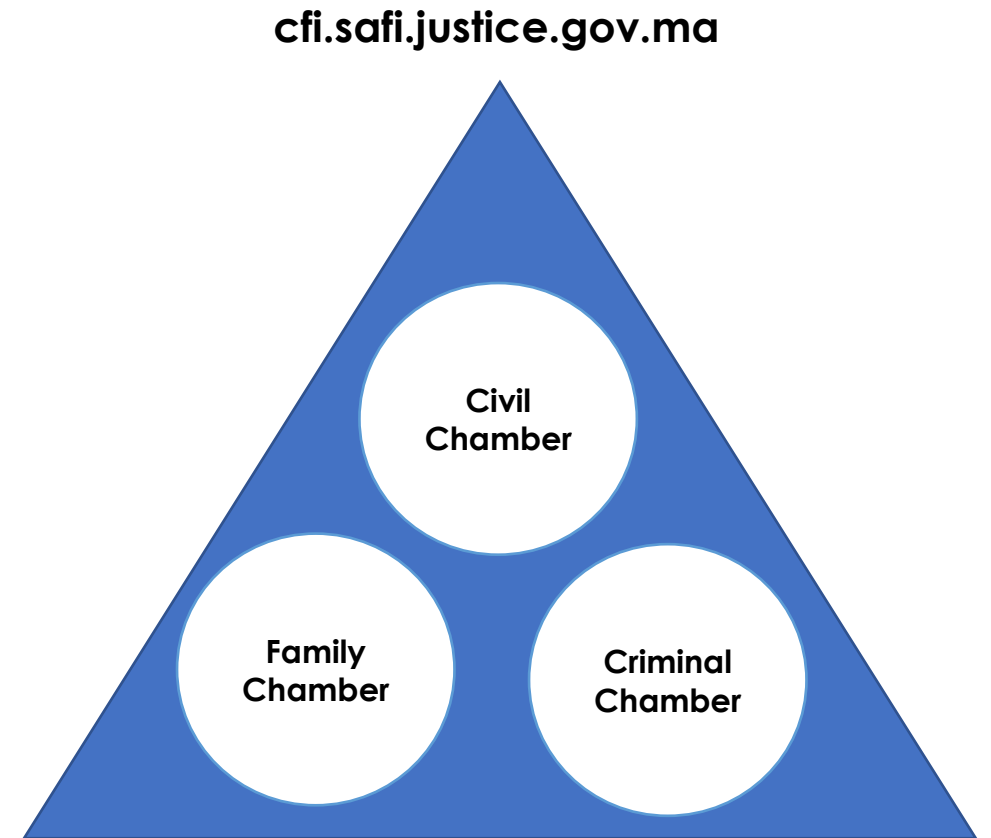
The forest would be the set of all Active Directory trees for each region, with *justice.gov.ma* as the root domain.



Example of *justice.gov.ma*

Organizational Units (OUs)

- OUs can be used to organize resources within each domain.
- Example of OUs within the justice.gov.ma domain:
 - Central Office
 - This OU could contain users, groups, and resources that are managed centrally by the Ministry of Justice.
- Example of OUs within the safi.justice.gov.ma domain:
 - Civil Chamber
 - This OU could contain users and groups related to the civil chamber of the first court of instance in Safi.
 - Family Chamber
 - This OU could contain users and groups related to the family chamber of the first court of instance in Safi
 - Criminal Chamber
 - This OU could contain users and groups related to the criminal chamber of the first court of instance in Safi.



Example of *justice.gov.ma*

Sites

- Active Directory uses "sites" to represent one or more physical network locations.
- A site is associated with one or more domain controllers, which authenticate users and computers in the domain.
- Sites help to optimize network traffic and authentication requests, as well as to ensure that users and computers connect to the nearest and most available domain controller.



Example of *justice.gov.ma*

Sites

- In the context of a court system, a site would represent a physical location that includes one or more courts.
- For example, the first court of instance and the court of appeal in Safi could be associated with a single site named "Safi Site."
- This site would include one or more subnets that cover the physical location of the courts, and it would be associated with one or more domain controllers that service the safi.justice.gov.ma domain.



Example of *justice.gov.ma*

Sites

- By using sites to organize and optimize network traffic, administrators can improve authentication performance and ensure that users and computers can connect to the nearest and most available domain controller.
- Sites can also be used to control when and how data is replicated between domain controllers in different physical locations, improving data availability and resilience.





Overview of Active Directory features and capabilities

Authentication and authorization

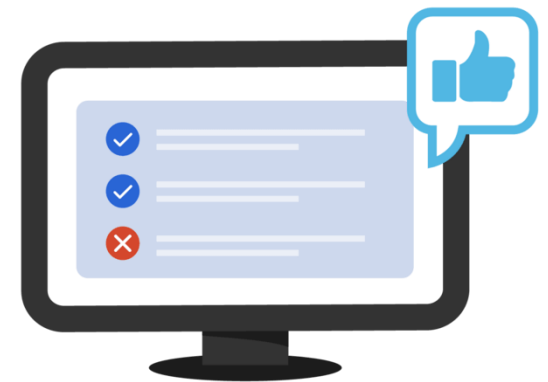
- Active Directory provides centralized **authentication** and **authorization** services for users, computers, and resources on the network.
- **Authentication** is the process of verifying the identity of a user or computer attempting to access a resource, while **authorization** determines what level of access the user or computer should have to that resource.
- Active Directory uses a combination of user accounts, passwords, and group policies to manage authentication and authorization.

Authentication



Confirms users are who they say they are.

Authorization



Gives users permission to access a resource.

Group Policy

- **Group Policy** is a feature of Active Directory that allows administrators to manage and configure user and computer settings on the network.
- Group Policy settings can be used to enforce security policies, control access to resources, configure software settings, and more.
- Group Policy is managed through the Group Policy Management Console (GPMC) and can be applied at the domain, site, or organizational unit (OU) level.



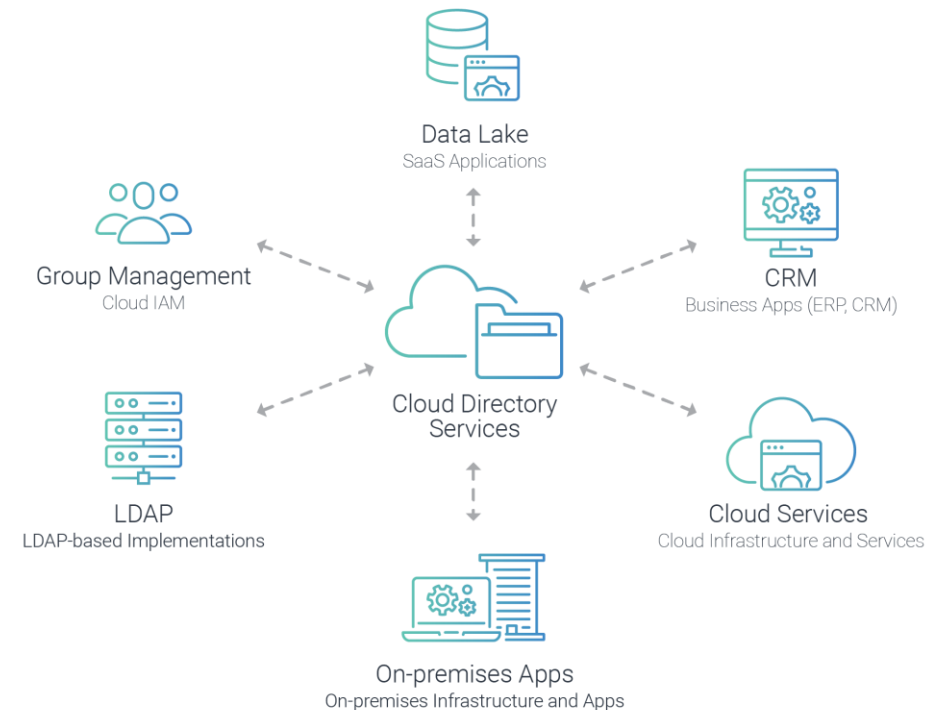
DNS Integration

- Active Directory integrates with the Domain Name System (DNS) to provide name resolution services for resources on the network.
- DNS is used to resolve domain names to IP addresses, allowing users and computers to locate resources on the network.
- Active Directory requires a properly configured DNS infrastructure to function properly.



Directory Services

- Active Directory provides a hierarchical, object-oriented database of directory services that can be used to store and manage information about users, computers, and resources on the network.
- Directory services can be accessed using LDAP (Lightweight Directory Access Protocol) and other protocols.
- Active Directory also provides a global catalog that contains information about all objects in the forest and can be used for searching and locating resources on the network.



Replication and scalability

- Active Directory uses a multi-master replication model to ensure that changes made to the directory database are replicated to all domain controllers in the domain or forest.
- Replication ensures that all domain controllers have a consistent view of the directory and can provide authentication and directory services to users and computers on the network.
- Active Directory is designed to be highly scalable and can support thousands or even millions of objects in the directory database.





Overview of Active Directory Components and Services



Active Directory Domain Services (AD DS)

- AD DS is the core service of Active Directory and provides centralized authentication and authorization for network resources.
- AD DS stores information about users, computers, and other objects in a hierarchical structure of domains and forests.
- AD DS uses the LDAP to provide access to directory data.
- AD DS also provides services such as Group Policy, which enables administrators to manage computer and user settings across the network.
- AD DS uses the Kerberos authentication protocol to provide secure authentication between clients and servers.
- AD DS can also integrate with other services such as DNS and DHCP to provide a comprehensive solution for managing network resources.

Active Directory Federation Services (AD FS)

- AD FS is a service that enables single sign-on (SSO) across different organizations or web applications.
- AD FS uses standard protocols such as Security Assertion Markup Language (SAML) and OAuth to establish trust relationships between organizations.
- AD FS provides a secure way to authenticate users across different organizations without the need for separate usernames and passwords.

Active Directory Certificate Services (AD CS)

- AD CS is a service that enables the issuance and management of digital certificates for secure communication.
- AD CS can be used to issue certificates for users, computers, and services such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates.
- AD CS can also be used to revoke and renew certificates and manage certificate templates.



Active Directory Lightweight Directory Services (AD LDS)

- AD LDS is a service that provides a lightweight directory for applications that require directory services but do not need the full functionality of AD DS.
- AD LDS can store information about users, groups, and other objects in a directory structure that is separate from the AD DS domain hierarchy.
- AD LDS uses the same LDAP protocol as AD DS to provide access to directory data.



Active Directory Rights Management Services (AD RMS)

- AD RMS is a service that provides information protection and control for documents and email messages.
- AD RMS enables users to define and enforce policies for accessing, editing, and distributing sensitive information.
- AD RMS uses encryption and digital signatures to protect data and can be integrated with other Microsoft applications such as SharePoint and Outlook.

Active Directory Administrative Center

- The Active Directory Administrative Center is a management console that provides a unified interface for managing Active Directory components and services.
- The Active Directory Administrative Center can be used to perform common administrative tasks such as creating users, groups, and other objects.
- The Active Directory Administrative Center can also be used to manage AD DS, AD LDS, AD CS, and AD RMS services from a single console.



Logical and physical design considerations for Active Directory

Logical Design Considerations

- The logical design of Active Directory refers to the way that directory objects are organized and arranged in a hierarchical structure of domains and forests.
- Logical design considerations include defining the number of domains and forests needed, the naming convention for domains and forests, and the placement of domain controllers.
- A well-designed logical structure can improve management efficiency and security by limiting access to resources and reducing administrative overhead.

Physical Design Considerations

- The physical design of Active Directory refers to the hardware and network infrastructure that support directory services, including the placement and configuration of domain controllers, sites, and subnets.
- Physical design considerations include the number and location of domain controllers, the type and configuration of hardware, the network topology, and the placement of global catalog servers.
- A well-designed physical infrastructure can improve performance, reliability, and availability of directory services.

Domain Design

- Domain design considerations include the number and size of domains needed to support the organization's structure and security requirements.
- A single-domain model can simplify management and reduce administrative overhead, but may not provide enough isolation between resources or support complex security policies.
- A multi-domain model can provide better isolation and support more complex security policies, but can increase management complexity and administrative overhead.

Forest Design

- Forest design considerations include the need for multiple forests to support business requirements such as mergers, acquisitions, or partnerships.
- A single-forest model can simplify management and reduce administrative overhead, but may not provide enough isolation between resources or support complex security policies.
- A multi-forest model can provide better isolation and support more complex security policies, but can increase management complexity and administrative overhead.

Site Design

- Site design considerations include the physical locations of domain controllers and clients, the network topology, and the placement of global catalog servers.
- Sites can be used to manage network traffic and replication between domain controllers, and to ensure that clients authenticate with a domain controller that is physically close to them.
- A well-designed site topology can improve performance, reliability, and availability of directory services.

Capacity Planning

- Capacity planning considerations include the number of objects in the directory, the rate of change, and the size of the database.
- Capacity planning can help ensure that directory services can scale to meet the needs of the organization and that hardware and network resources are adequate.
- Capacity planning should take into account future growth and business requirements.



Authentication protocols used by Active Directory

Introduction to Authentication Protocols

- Authentication is the process of verifying the identity of a user, computer, or service.
- Active Directory uses several authentication protocols to provide secure access to network resources.
- Understanding these protocols is important for securing the network and troubleshooting authentication issues.



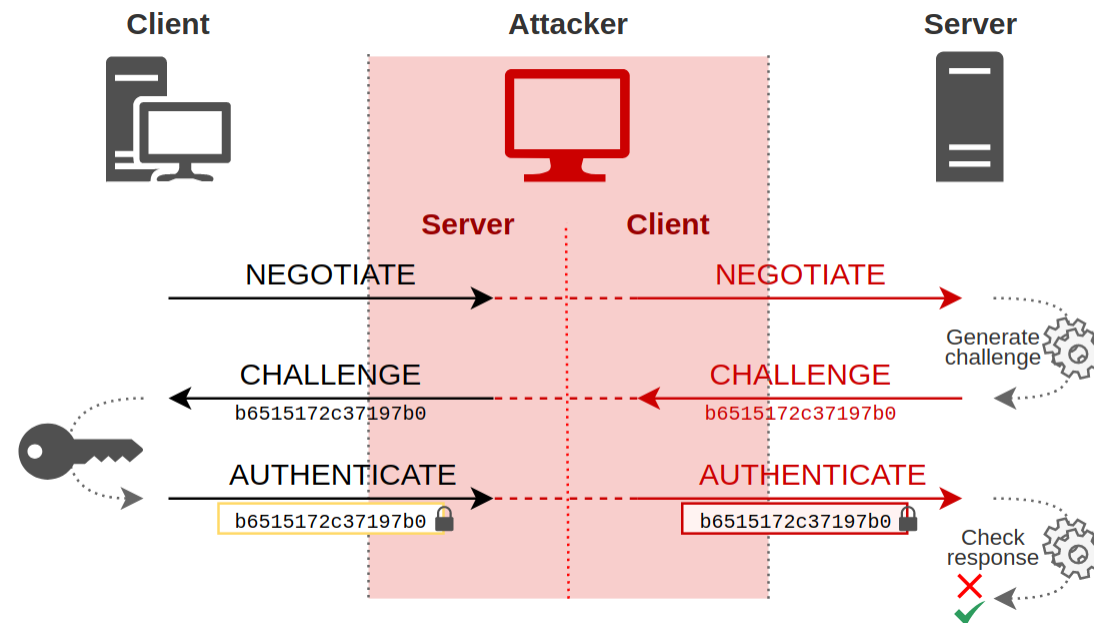
Kerberos Authentication

- Kerberos is the default authentication protocol used by Active Directory.
- Kerberos uses a ticket-granting service (TGS) and a key distribution center (KDC) to authenticate users and computers.
- Kerberos is a mutual authentication protocol that requires both the client and the server to verify each other's identity.



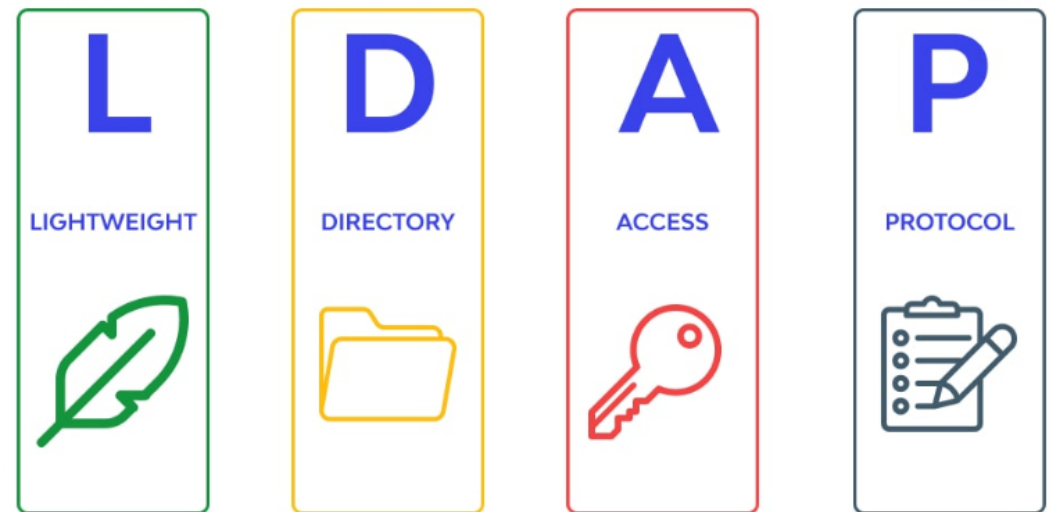
NTLM Authentication

- NTLM is an older authentication protocol that is still supported by Active Directory for backward compatibility.
- NTLM uses a challenge-response mechanism to authenticate users and computers.
- NTLM is less secure than Kerberos and should be avoided when possible.



LDAP Authentication

- LDAP is a directory service protocol used by Active Directory to access and search the directory.
- LDAP can also be used for authentication by binding to the directory with a user's credentials.
- LDAP authentication can be used with SSL/TLS encryption to provide secure authentication over the network.



Smart Card Authentication

- Smart card authentication uses a smart card and a personal identification number (PIN) to authenticate users.
- Smart card authentication provides strong two-factor authentication and is often used in high-security environments.
- Smart card authentication requires additional hardware and software to be installed and configured.



Certificate Authentication

- Certificate authentication uses digital certificates to authenticate users and computers.
- Certificate authentication can be used with SSL/TLS encryption to provide secure authentication over the network.
- Certificate authentication requires a public key infrastructure (PKI) to issue and manage digital certificates.



Security Features and Mechanisms in Active Directory



Security Features and Mechanisms in Active Directory

- Security is a critical aspect of any network infrastructure, and Active Directory provides several features and mechanisms to secure the directory.
- Understanding these security features is important for protecting sensitive information and ensuring the integrity of the network.



Domain Controllers

- Domain controllers are the backbone of Active Directory and play a crucial role in securing the directory.
- Domain controllers store the Active Directory database, handle authentication requests, and enforce security policies.
- Domain controllers can be secured using techniques such as physical security, hardening, and regular patching and updates.

Active Directory Users and Groups

- Active Directory provides a centralized mechanism for managing users and groups, which is essential for controlling access to network resources.
- User accounts and groups can be secured using techniques such as strong password policies, account lockout policies, and group nesting.



Group Policy

- Group Policy is a powerful feature of Active Directory that allows administrators to configure security settings, software installation, and other system-level settings.
- Group Policy can be used to enforce security policies such as password complexity, account lockout, and software restriction policies.


Audit and Monitoring

- Active Directory provides extensive auditing and monitoring capabilities to track changes to the directory and detect potential security threats.
- Audit and monitoring can be configured to track events such as user logon/logoff, changes to group membership, and changes to directory objects.



Domain Name System Security Extensions (DNSSEC)

- DNSSEC is a security extension to DNS that provides authentication and data integrity for DNS queries.
- DNSSEC can be used to protect against DNS cache poisoning attacks, which can redirect users to malicious websites.
- DNSSEC can be configured in Active Directory to provide additional security for DNS queries.



Overview of Group Policy Objects (GPOs) and How They are Used to Manage User and Computer Settings

Introduction

- Group Policy Objects (GPOs) are a key feature of Active Directory that allow administrators to manage user and computer settings across the network.
- GPOs can be used to enforce security policies, configure software settings, and customize the user environment.
- Understanding how to create, edit, and apply GPOs is essential for managing a secure and efficient network.



GPO Basics

- A GPO is a container object that holds a collection of policy settings that can be applied to user and computer objects in Active Directory.
- Each GPO can contain multiple policy settings, and a single policy setting can be defined in multiple GPOs.
- GPOs are linked to Active Directory sites, domains, or organizational units (OUs) to define the scope of their application.



Creating and Editing GPOs

- GPOs can be created and edited using the Group Policy Management Console (GPMC) or the Active Directory Users and Computers console.
- GPO settings can be defined using administrative templates, security settings, software settings, and script settings.
- GPOs can be filtered using security group filtering, WMI filtering, and loopback processing.



GPO

Group policy Objects

Applying GPOs

- GPOs are applied to user and computer objects based on the scope of their linkage and the order in which they are applied.
- The order of GPO application can be modified using link order, enforced link, and block inheritance.
- GPOs can be forced to update immediately using the GPUpdate command or scheduled to update at regular intervals using Group Policy refresh settings.



User Settings

- GPOs can be used to manage a variety of user settings, such as logon scripts, folder redirection, and desktop settings.
- User settings can be defined in the User Configuration section of a GPO, and can be applied to individual users or groups of users based on their membership in security groups.



Computer Settings

- GPOs can also be used to manage a variety of computer settings, such as security settings, software installation, and network settings.
- Computer settings can be defined in the Computer Configuration section of a GPO, and can be applied to individual computers or groups of computers based on their membership in security groups.



Security Policies

- GPOs can be used to enforce a variety of security policies, such as password policies, account lockout policies, and auditing policies.
- Security policies can be defined in the Security Settings section of a GPO, and can be applied to users or computers based on their membership in security groups.



GPO

Group policy Objects

Customizing the User Environment

- GPOs can be used to customize the user environment by defining settings such as desktop backgrounds, screensavers, and Start menu options.
- Customization settings can be defined in the User Configuration section of a GPO, and can be applied to individual users or groups of users based on their membership in security groups.



Software Installation and Maintenance

- GPOs can be used to deploy and manage software installation and maintenance across the network.
- Software installation and maintenance settings can be defined in the Computer Configuration section of a GPO, and can be applied to individual computers or groups of computers based on their membership in security groups.



Group Policy Preferences

- Group Policy Preferences is a feature of GPOs that allows administrators to configure a variety of user and computer settings in a more flexible and targeted way.
- Group Policy Preferences can be used to set registry settings, map drives and printers, and manage power settings.
- Group Policy Preferences can be defined in the Preferences section of a GPO, and can be applied to individual users or groups of users based on their membership in security groups.



Troubleshooting GPOs

- GPOs can fail to apply due to various reasons such as permission issues, network connectivity problems, and configuration errors.
- GPO troubleshooting can be performed using tools such as Group Policy Results, Group Policy Modeling, and Group Policy Event Logs.
- Common GPO troubleshooting techniques include checking for GPO replication errors, reviewing GPO permissions, and verifying network connectivity.





Active Directory Configuration on Windows Server 2008

Active Directory Configuration on Windows Server 2008

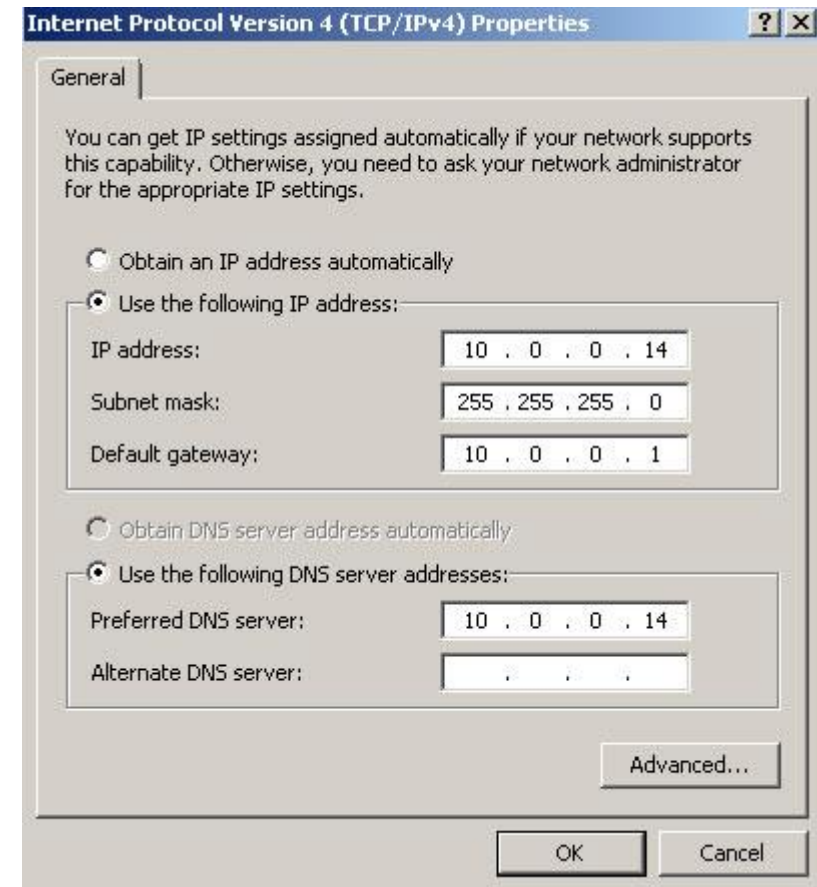
This tutorial will explain how to install AD on server 2008.

Requirement

- Minimum: Single processor with 1.4 GHz (x64 processor) or 1.3GHz (Dual Core)
- Minimum: 512 MB RAM
- Minimum: 32 GB or greater

Active Directory Configuration on Windows Server 2008

Assign an IP Address to the AD Server.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 0 . 0 . 14

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 0 . 14

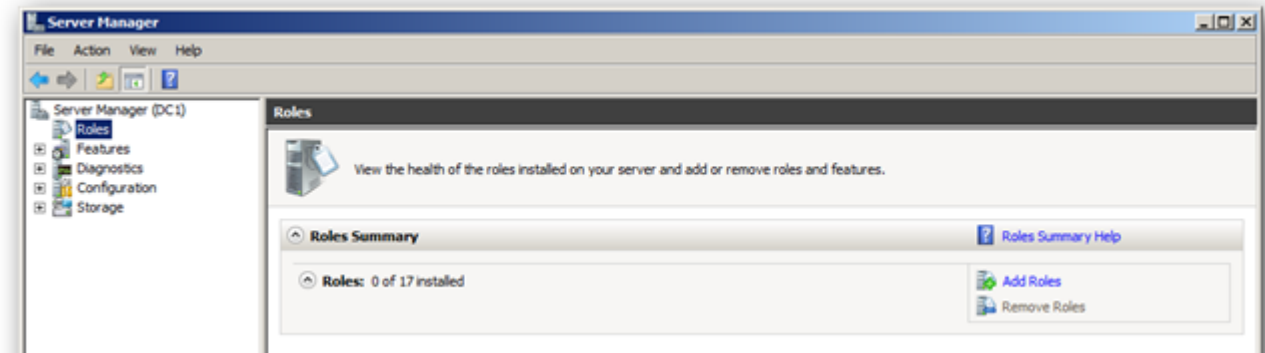
Alternate DNS server: . . .

Advanced...

OK Cancel

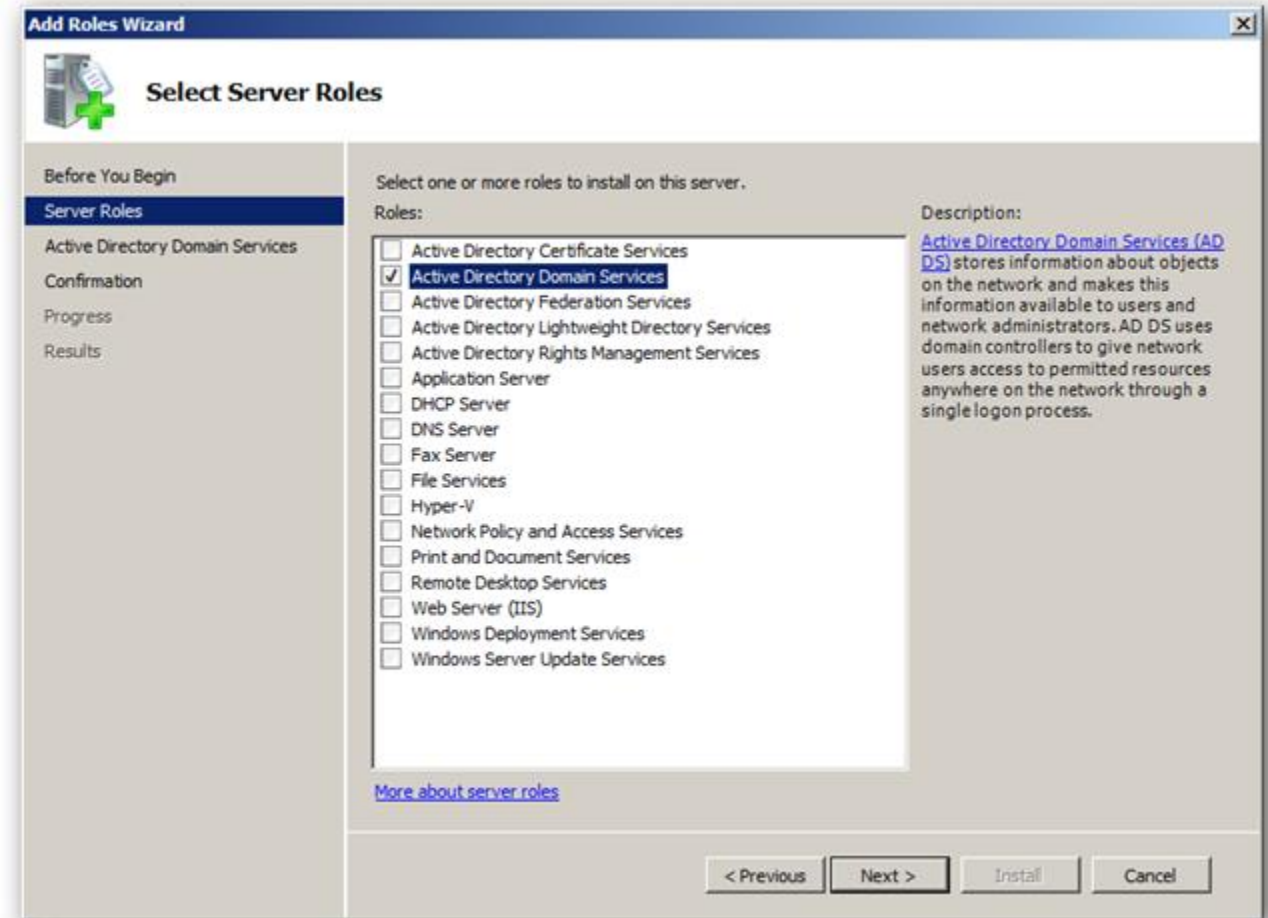
➤ Active Directory Configuration on Windows Server 2008

Open Server Manager → Roles, this will bring up the Roles Summary on the right hand side where you can click on the Add Roles link.



Active Directory Configuration on Windows Server 2008

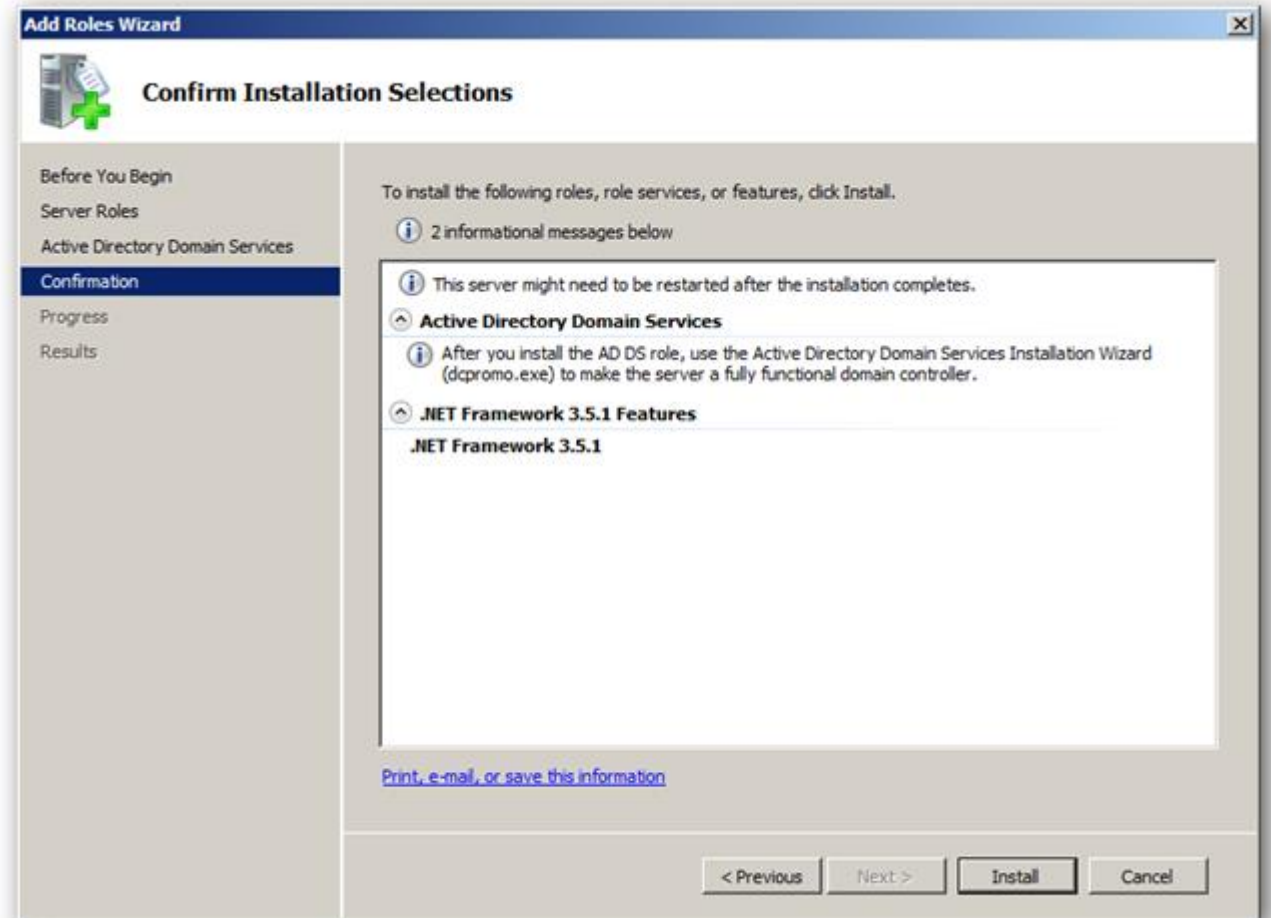
Select Active Directory Domain Services from the list, you will be told that you need to add some features, click on the Add Required Features button and click next to move on.



Active Directory Configuration on Windows Server 2008

A brief introduction about Active Directory, and links to additional resources will be displayed.

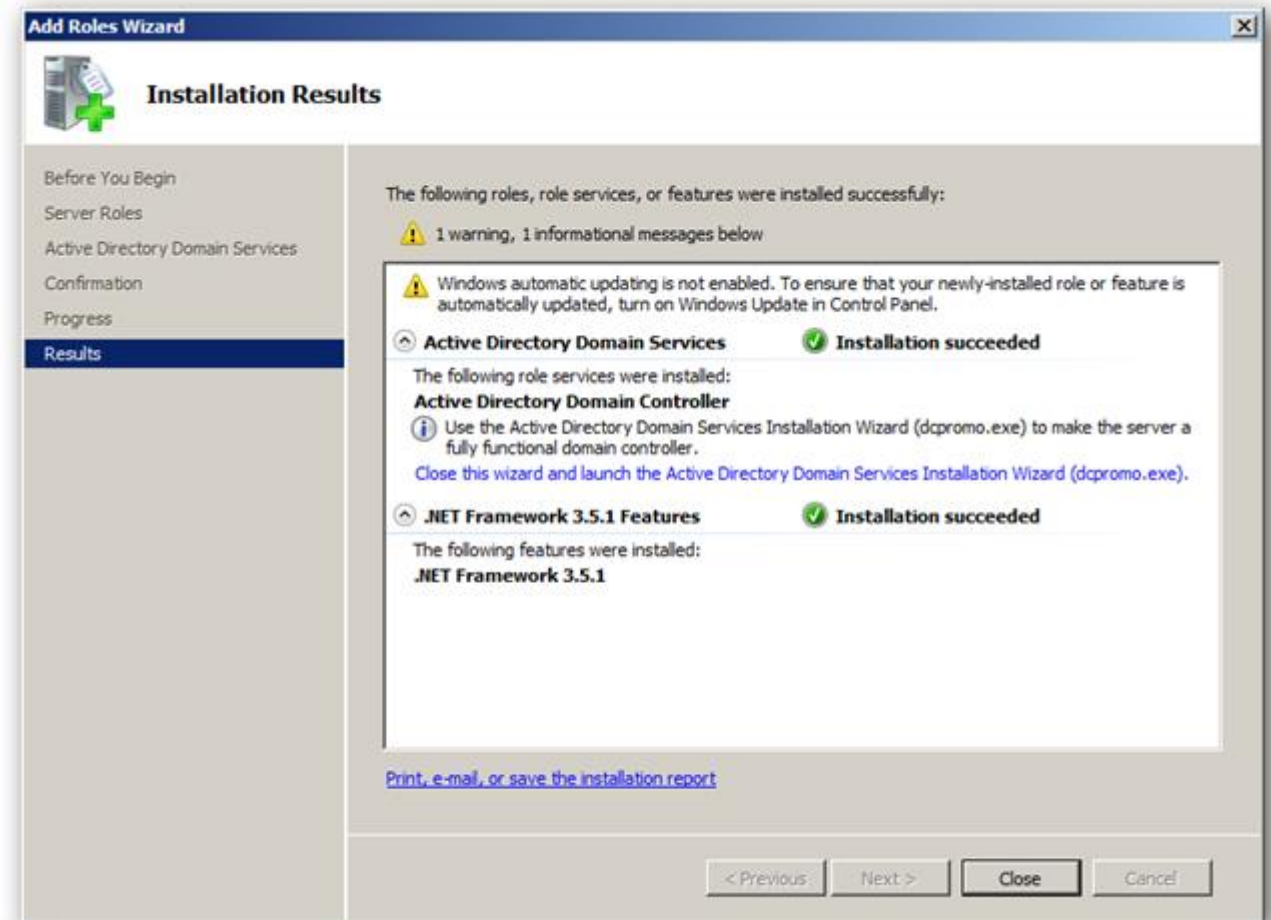
Click next, and then click Install to start installing the binaries for Active Directory.



Active Directory Configuration on Windows Server 2008

When the installation is finished you will be shown a success message.

Just click Close.



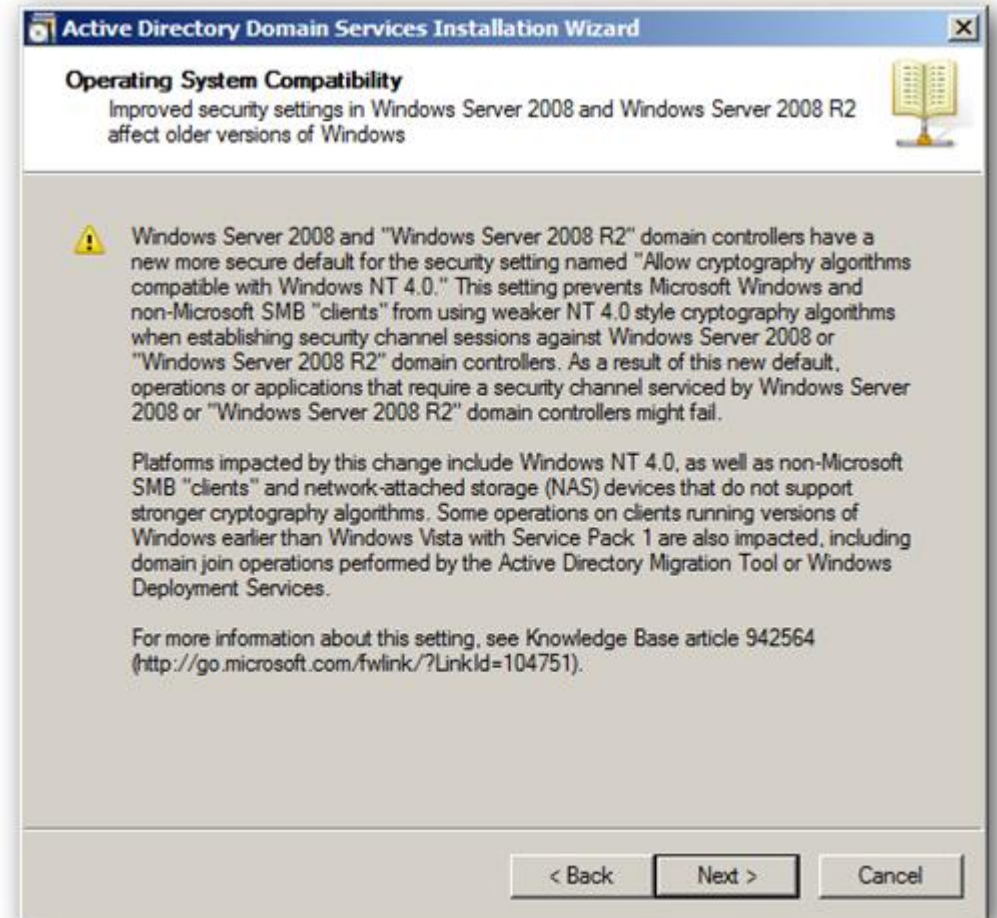
Active Directory Configuration on Windows Server 2008

Start → Run → Type dcpromo
to run the ADDS wizard.



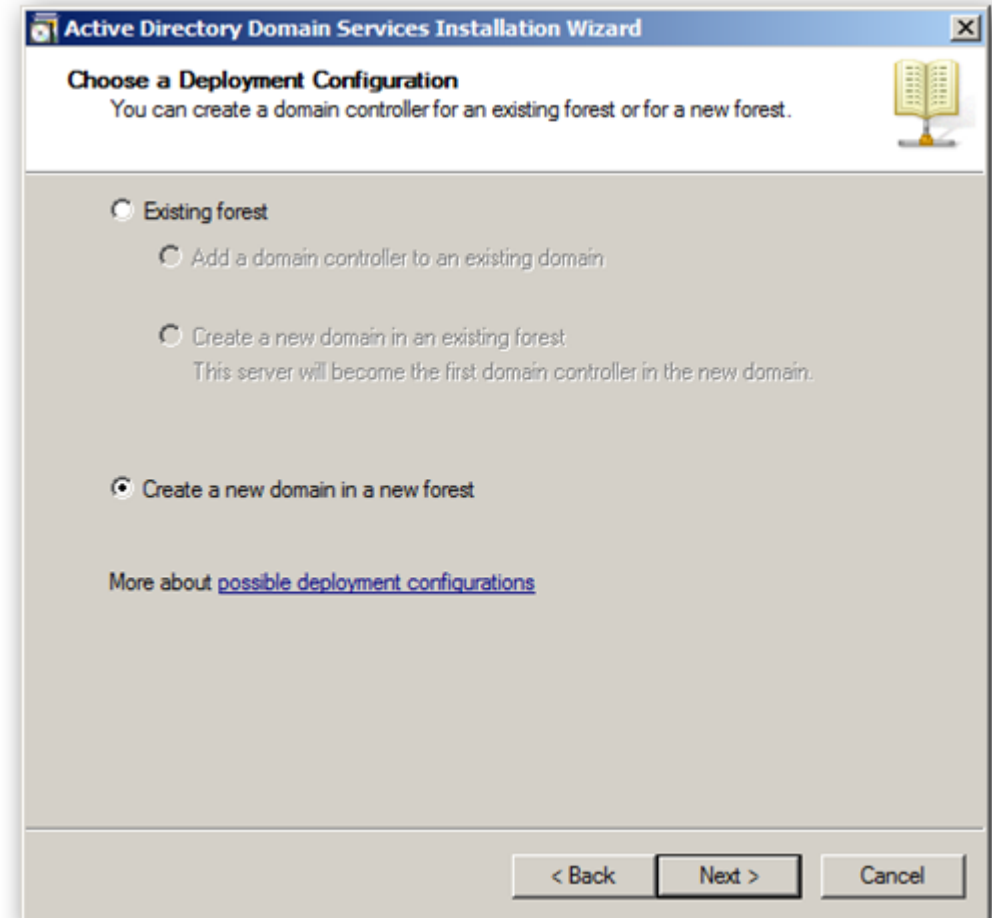
Active Directory Configuration on Windows Server 2008

The message that is shown now relates to older clients that do not support the new cryptographic algorithms supported by Server 2008 R2. Click Next to move on.



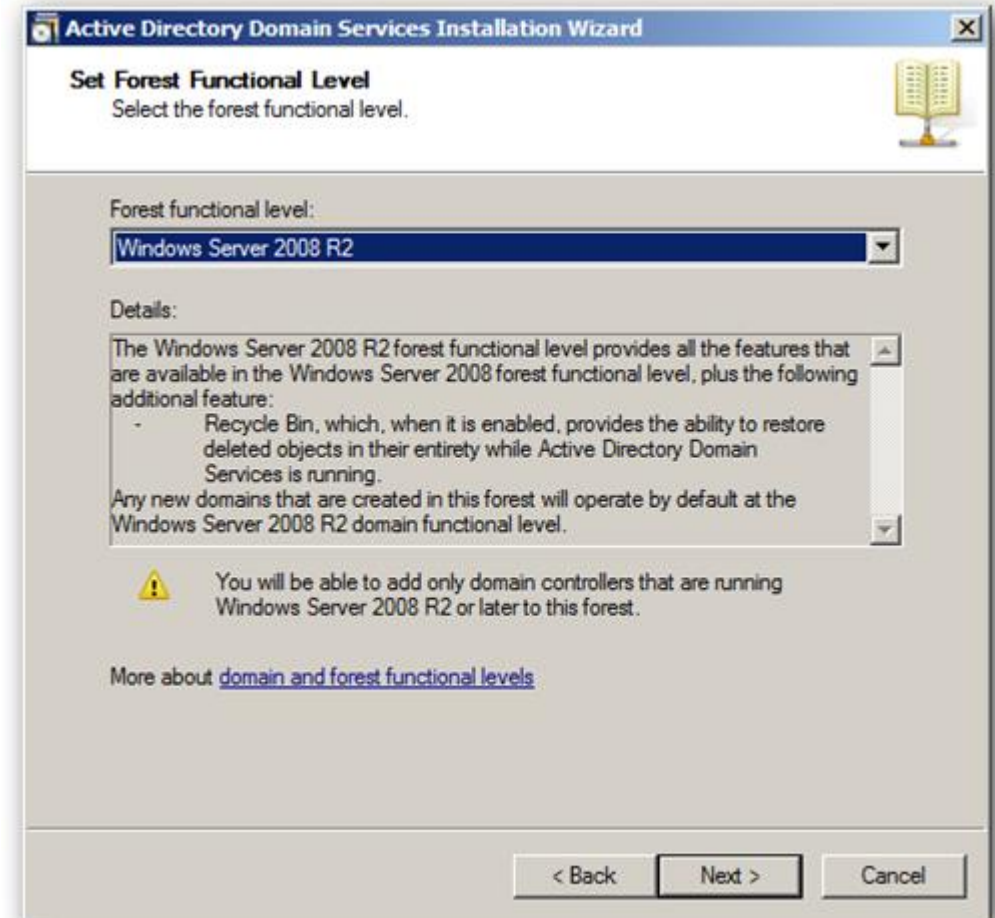
Active Directory Configuration on Windows Server 2008

If this is the first forest in your Active Directory environment, select the option "Create a new domain in a new forest".



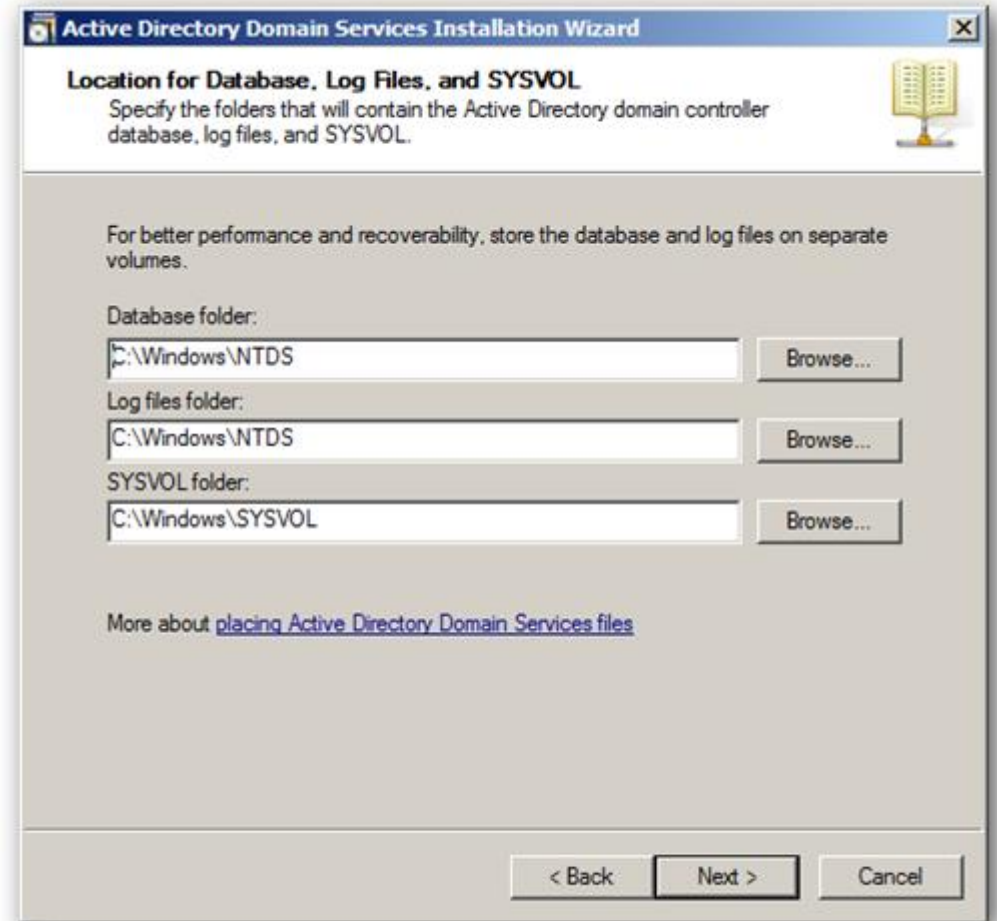
Active Directory Configuration on Windows Server 2008

Since this is the first DC in our domain we can change our forest functional level to Server 2008 R2.



Active Directory Configuration on Windows Server 2008

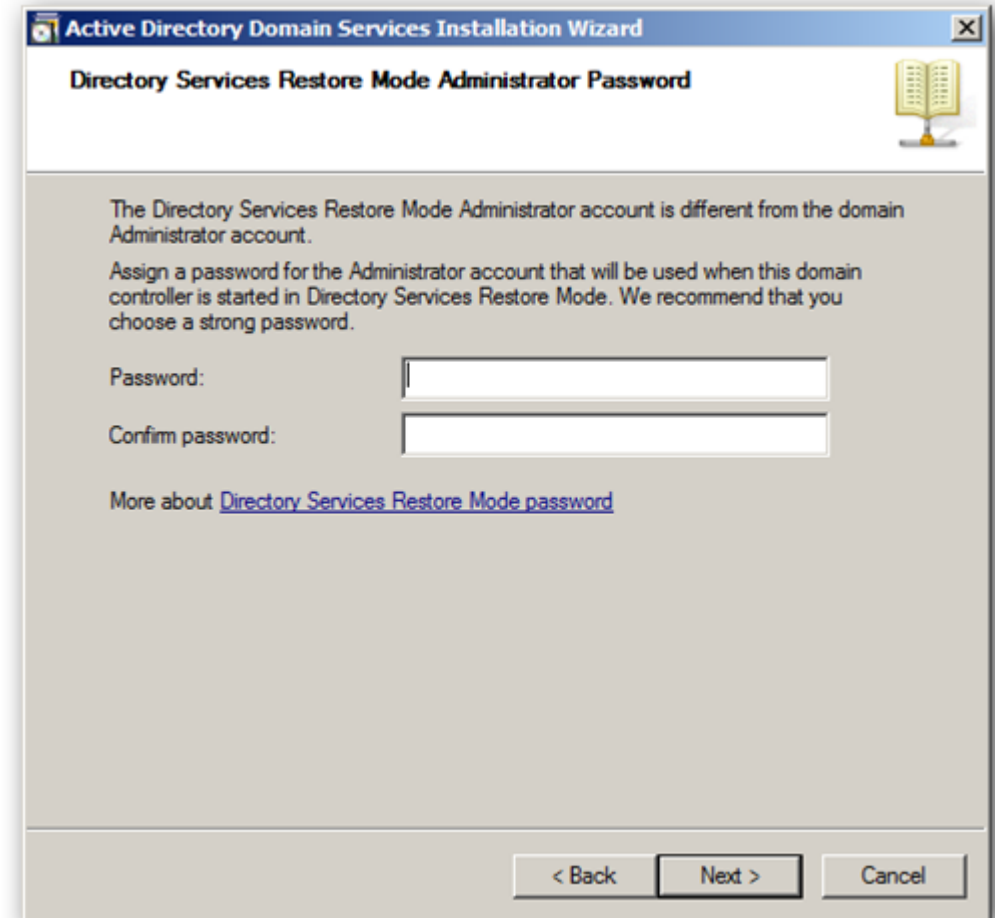
Select the folder where your database, log files and SYSVOL will be stored. It is recommended to stick to the default settings.



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Location for Database, Log Files, and SYSVOL'. Below this, it says 'Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.' There is a small icon of a book on the right. The main area contains a note: 'For better performance and recoverability, store the database and log files on separate volumes.' Below this are three rows of input fields with 'Browse...' buttons: 'Database folder:' with 'C:\Windows\NTDS', 'Log files folder:' with 'C:\Windows\NTDS', and 'SYSVOL folder:' with 'C:\Windows\SYSVOL'. At the bottom, there is a link: 'More about [placing Active Directory Domain Services files](#)'. The bottom of the window has three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Configuration on Windows Server 2008

Enter a unique Active Directory Restore Mode password that will be used during recovery.



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Directory Services Restore Mode Administrator Password'. Below the heading, there is an icon of an open book. The text explains that the Directory Services Restore Mode Administrator account is different from the domain Administrator account and that a password must be assigned for use when the domain controller is started in Directory Services Restore Mode. It recommends a strong password. There are two input fields: 'Password:' and 'Confirm password:'. At the bottom, there is a link 'More about [Directory Services Restore Mode password](#)'. The bottom of the window has three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password:

Confirm password:

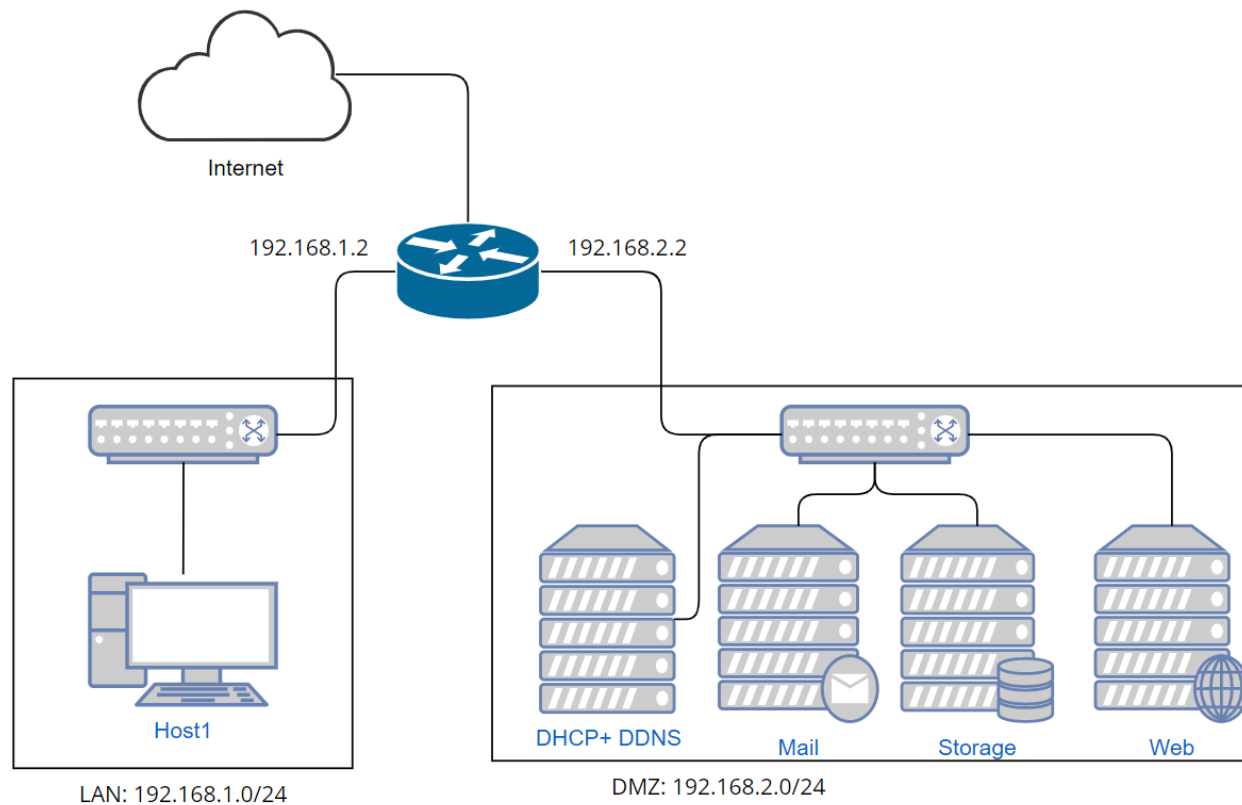
More about [Directory Services Restore Mode password](#)

< Back Next > Cancel



Practice

Practice Network Design





Practice outline


1. **Week 1** : Install a Fedora Server on a Virtual Machine
2. **Week 2** : Configure DHCP on Fedora Server
3. **Week 3** : Configure DHCP + Relay Agent (LAN + DMZ)
4. **Week 4** : Configure DHCP + DNS
5. **Week 5** : Configure DDNS
6. **Week 6** : Web Server
7. **Week 7** : Active Directory
8. **Week 8** : Presentations

Week 4 : Configure DHCP + DNS

1. **Goal** : Install DHCP + DNS in one server. The client needs to get IP address and DNS configuration from the server.

Week 5 : Configure DDNS

1. **Goal:** The client needs to get IP address and DNS configuration from the server + The zone files should be updated dynamically.



Week 6 : Web Server

1. **Goal** : Configure Web Server, PHP, MySQL, PhPMyAdmin.



Week 7: Active Directory

1. **Goal** : Replace DHCP+DDNS+Web Server by a Windows Server 2008.
Install Active Directory (DHCP+ DNS+Web Server).



Week 8: Presentation

1. **Goal:** Configure Mail Server.