### Module: 14 Identity with Windows Server

# Topic : Active directory Domain Services

**1. what is domain controller?**

A domain controller is a server that responds to authentication requests and verifies users on computer networks. Domains are a hierarchical way of organizing users and computers that work together on the same network. The domain controller keeps all of that data organized and secured.

It provides security by authentication and policies and centralised management. It prevents from attacks of Active Directory that stores all the database, and information of different types of objects, objects class and resources.

**2. describe forest, domain, tree, schema, OU, container, site, subnet.**

A domain tree is simply a collection of one or more domains that share a common namespace. Domains within the AD tree structure have a [transitive trust](https://www.techtarget.com/searchwindowsserver/definition/transitive-trust) relationship, meaning that if a domain joins a tree, it automatically trusts all the other domains in that tree. The tree typically begins with a single parent or root, and branches out into multiple peripheral child domains. The domains in the AD tree share the same namespace, and also share a boundary with each other. Two different trees cannot share one namespace.

**A forest** : is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible. A forest is a collection of one or more domains which may have one or more trees. What makes a forest unique is that it shares the same schema. The schema defines what and how Active Directory objects are stored. A forest is a group of trees that do not share a contiguous namespace.

**Domain :** A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database. When you add a domain to an existing tree, the new domain is a child domain of an existing parent domain.

**Tree :** A tree is a collection of one or more domains and domain trees in a contiguous namespace, and is linked in a transitive trust hierarchy. When you have multiple domains in the same namespace (e.g., techdirect.local, zone.techdirect.local), they are considered to be in the same tree. The tree also supports multiple levels of domains. A tree is a hierarchical arrangement of Windows domains that share a contiguous namespace.

**Schema** **:**  is a blueprint that describes the rules about the type of objects that can be stored in the AD as well as the attributes related to these objects. The schema thus defines the content, and the structure of the object classes, and the object attributes used to create an object. While creating a new object, the AD references the classes defined in the schema and utilizes the retrieved information to create the object.

**Organizational units (OU) :** are containers that hold other Active Directory objects like users, computers, printers, shared folders, and even other organizational Units. The advantage of OU is that it can be used to set security policies and delegate administrative control.

**AD Sites :** These are the objects that represent the physical locations of DCs and/or client machines. Typically, every defined site should have at least one DC, and the sites should match the physical locations the servers are in. Specifically, servers that are on the same LAN should be in the same site, and servers that are separated by a WAN should be in separate sites.

**A subnet :** or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments. Subnets are the IP ranges that are associated with specific AD sites. DCs and clients use the subnets you define to determine what site they are in.

Forest root domain

Root tree trust

Trust relationship

Dc adc

Parent -child trust

Organization

Root.com unit

Child domain

Surat.com baroda .com ou

site

Ou

Varacha.surat .Root .com

**3. partition, trust relationship**

AD Partitions basically arrange and segregate the data as per their use and working. There are mainly four partitions, out of which three are are core and one has introduced later. All the partitions are replicated with every Domain Controllers within the Forest/Domain.

1. **Schema Partition:** Active Directory Schema is blueprint of AD, which is combination of Class and Attribute. The same Schema related objects (classSchema, attributeSchema) are stored in Schema Partition. This partition is replicated to every Domain Controller in the entire forest.

1. **Configuration Partition:** This partition stores all configuration related data for Active Directory, such as Replication, Topologies, Sites and other settings. This partition is also replicated to every DC in the entire forest.

1. **Domain Partition:** This partition contains the actual objects, such as Users, Groups, Computers etc. Whatever objects available in Active Directory Users and Computers, everything is stored in this partition. This partition replicates with every partition within the local domain, but not in the other domains in the forest.

**(iv)Application Partition:** This partition was introduced with Windows Server 2003. This stores data related to various Services, such as DNS, LDAP etc. If your DNS is Active Directory Integrated, there will be two logical sub-partitions inside that: DomainDNSZones and ForestDNSZones.

Apart from these partitions, there are one special Active Directory Partition called Global Catalog Partition. This stores all the information about available Global Catalogs (DCs) within the forest.

**Trust relationship :**

Active Directory Domain Services (AD DS) provides security across multiple domains or forests through domain and forest trust relationships. To check for this trust relationship, the Windows security system computes a trust path between the domain controller (DC) for the server that receives the request and a DC in the domain of the requesting account.

The access control mechanisms provided by AD DS and the Windows distributed security model provide an environment for the operation of domain and forest trusts. For these trusts to work properly, every resource or computer must have a direct trust path to a DC in the domain in which it is located.

Different types of trust areTree-root trust, Parent-child trust, External trust, Forest trust, Realm trust.

The flow of communication over trusts is determined by the direction of the trust. Trusts can be one-way or two-way, and can be transitive or non-transitive.

**4. what is active directory?**

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

**5. what is global catalog server?**

A global catalog is a distributed data storage that is stored in domain controllers, known as global catalog server and is used for faster searching. It provides a searchable catalog of all objects in every domain in a multi-domain Active Directory Domain Services (AD DS). A global catalog provides a partial representation of the objects and is distributed using multi-master replication.

A global catalog is a multi-domain catalog that allows for faster searching of objects without the need for a domain name. It helps in locating an object from any domain by using its partial, read-only replica stored in a domain controller. As it uses only partial information and a set of attributes that are most commonly used for searching, the objects from all domains, even in a large forest, can be represented by a single database of a global catalog server. A global catalog is created and maintained by the AD DS replication system. Users are allowed to add or delete the attributes stored in a global catalog and thus change the database schema.

**6. what is ADC AND RODC?**

**ADC :** It is the clone of the main/root domain controller. The primary objective of the ADC is disaster recovery. It acts as a backup in case of the failure of root DC. Secondarily, ADC is used when the main DC is physically apart at longer distances with client machines.

**RODC :** It is very similar to ADC in terms of roles and features. For instance, like ADC, it can be used on branch office, acts as a DNS, and has a Global Catalogue feature. However, the crucial difference between ADC and RODC is, the RODC can’t be used as a backup DC in case of DC failure. So, if for some reason, the DC server goes down, the migration of RODC roles to DC roles is impossible. It can be used for a branch office where physical security isn’t guaranteed, then read-only DC’s are preferred. Another reason could be that if there is a lack of IT staffing who can handle infrastructure, then RODC could be a better option than adding a DC server.

**7. what is operation master role?**

Operations master roles (also known as flexible single master operations, or FSMO) are special roles assigned to one or more domain controllers in an Active Directory domain. Active Directory Domain Services (AD DS) supports multimaster replication of directory data, which means any domain controller can accept directory changes and replicate the changes to all other domain controllers.

However, certain changes, such as schema modifications, are impractical to perform in a multimaster fashion. For these reasons certain domain controllers, known as operations masters, hold roles responsible for accepting requests for certain specific changes.

**8. type of operation master role and describe all role.**

Active Directory supports multi-master replication of the directory data store between all domain controllers in the domain. Hence all domain controllers in a domain are considered essentially peers.

There are five Operation Master Roles and two of them are Forest level roles and three of them are Domain Level roles. Following table lists the Operation Master Roles and their scope.

|  |  |
| --- | --- |
| **Operations Master** | **Scope** |
| Schema Master | Forest wide |
| Domain Naming Master | Forest wide |
| Primary Domain Controller (PDC) Emulator | Domain wide |
| Relative Identifier (RID) Master | Domain wide |
| Infrastructure Master | Domain wide |

**(i) Schema Master Role :**

 Active Directory schema defines what can exist within the directory. Managing the process of updating it with new objects and attributes should be a closely monitored process. The domain controller assigned the schema master role controls all updates and modifications to the schema. To update the schema of a forest, must have access to the schema master. There only a single Schema Master in the entire forest at any time.

**(ii) Domain Naming Master :**

 All objects within AD must be unique. It cannot be created two objects in a container with the same name, and the distinguished names all of all objects must be unique. Domain Naming Master ensures that new domains added to windows server forest have unique names. There only a single Domain Naming Master in the entire forest at any time.

**(iii) PDC (Primary Domain Controller) Emulator :**

* The PDC emulator services network clients that do not have Active Directory client software installed, and it replicates directory changes to any Microsoft Windows NT backup domain controllers (BDCs) in the domain. The PDC emulator receives preferential replication of password changes performed by other domain controllers in the domain.
* If a password was recently changed, that change takes time to replicate to every domain controller in the domain. If a logon authentication fails at another domain controller due to a bad password, that domain controller forwards the authentication request to the PDC emulator before rejecting the logon attempt. There is only a single PDC Emulator per domain.

**(iv) Relative ID (RID) Master :**

* A Security Principal is an Active Directory object that can be assigned permissions within a Windows Server 2003 network. Examples for Security Principal objects are users, groups, and computers. Each Security Principal is assigned a Security Identifier (SID) so it can be identified.
* A Security Identifier (SID) is made up of two components. The first component, the domain SID, is common to all security principals in a domain. The uniqueness in SID comes from the addition of a second number, the Relative Identifier (RID). The RID is assigned from a pool of RIDs stored at each Domain Controller. The RIDs in this pool are assigned to each Domain Controller by the RID Master.
* RIDs are assigned to each DC in blocks of 500 RIDs. When the block of RIDs is exhausted, the DC requests another block from the RID Master. To ensure uniqueness, the RID Master keeps track of which RID blocks have been assigned.
* If the RID pool on a DC is exhausted and the RID Master is not available, it will not allow to create Security Principals (Example: a user) on that server. There is only a single RID Master per domain.

**(v) Infrastructure Master :**

 The domain controller assigned the infrastructure master role is responsible for updating the group-to-user references whenever the members of groups are renamed or changed. There is a single Infrastructure Master per domain.

**9. difference between transferring and seizing role**

In transfer, both the source and destination DCs must be connected, that is one can transfer the role first to destination server and then transferred it back to source server in case of data corruption While seize is designed for disaster recovery where lost the connectivity is already there and neither chance to recover the source server in near future. Seizing role is basically forcefully moving the role, without having any connectivity between source and destination DCs.

So, the main difference isTransfer needs source and destination to be connected but Seize doesn’t need the connection.

**10. password policy**

A password policy defines the password strength rules. Windows supports fine-grained password policies. This feature provides organizations with a way to define different password and account lockout policies for different sets of users in a domain. Finegrained password policies apply only to user objects and global security groups.

Fine-grained password policies include attributes for all the settings that can be defined in the default domain policy, in addition to account lockout settings. While specifying a fine-grained password policy, must need to specify all of these settings. By default, only members of the Domain Admins group can set fine-grained password policies.

**11. what is profile and type of profile?**

All account policies settings applied by using Group Policy are applied at the domain level. Default values are present in the built-in default domain controller policy for Password Policy settings, Account Lockout Policy settings, and Kerberos Policy settings. The domain account policy becomes the default local account policy of any device that is a member of the domain.

If these policies are set at any level below the domain level in Active Directory Domain Services (AD DS), they affect only local accounts on member servers. The only exception is when another account policy is defined for an organizational unit (OU). The account policy settings for the OU affect the local policy on any computers that are contained in the OU.

**Types of User Profiles :**

1. **Local User Profiles:** A local user profile is created the first time that a user logs on to a computer. The profile is stored on the computer's local hard disk. Changes made to the local user profile are specific to the user and to the computer on which the changes are made.

1. **Roaming User Profile :** A roaming user profile is a copy of the local profile that is copied to, and stored on, a server share. This profile is downloaded to any computer that a user logs onto on a network. Changes made to a roaming user profile are synchronized with the server copy of the profile when the user logs off. The advantage of roaming user profiles is that users do not need to create a profile on each computer they use on a network.
2. **Mandatory User Profile :** A mandatory user profile is a type of profile that administrators can use to specify settings for users. Only system administrators can make changes to mandatory user profiles. Changes made by users to desktop settings are lost when the user logs off.

1. **Temporary User Profile :** A temporary profile is issued each time that an error condition prevents the user's profile from loading. Temporary profiles are deleted at the end of each session, and changes made by the user to desktop settings and files are lost when the user logs off. Temporary profiles are only available on computers running Windows 2000 and later.

**12. group nesting and scope, type of group**  **Group nesting :**

Adding a group as a member of another group is called nesting*.* For distribution groups, nesting is supported in both mixed mode and native mode. For security groups, nesting is supported only for domains running in native mode. To nest a group in another group, use the same techniques described in Adding members to group in domain. Be aware that depending on the scope of the group, the group can contain only specific types and scopes of other groups. The nesting options also depend on whether the domain is in mixed mode or native mode.

**Group scope :**

Groups are characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest. The scope of the group defines where the group can be granted permissions. The following three group scopes are defined by Active Directory:

* Universal
* Global
* Domain Local

 Practical

1. install ADDS and create a new forest

DONE

1. give membership of pc to domain

DONE

1. create a ADC

DONE

1. create RODC and password replication

DONE

1. create a new site

DONE

1. create a new child domain

DONE

1. create a new tree

DONE

1. create a new user with GUI and CLI

DONE

1. create roaming profile

DONE

1. create OU and give delegation

DONE

1. create a group

DONE

1. transfer roles—PDC, RID , schema master ,

DONE

1. Doamin name master— 14. GUI and ntdsutil

DONE

15. IFM

DONE

# Topic : Advance feature

**1. describe account policy**

All account policies settings applied by using Group Policy are applied at the domain level. Default values are present in the built-in default domain controller policy for Password Policy settings, Account Lockout Policy settings, and Kerberos Policy settings. The domain account policy becomes the default local account policy of any device that is a member of the domain. If these policies are set at any level below the domain level in Active Directory Domain Services (AD DS), they affect only local accounts on member servers.

The only exception is when another account policy is defined for an organizational unit (OU). The account policy settings for the OU affect the local policy on any computers that are contained in the OU.

**2. describe account lockout policy**

Someone who attempts to use more than a few unsuccessful passwords while trying to log on to system might be a malicious user who is attempting to determine an account password by trial and error. Windows domain controllers keep track of logon attempts, and domain controllers can be configured to respond to this type of potential attack by disabling the account for a present period of time. Account Lockout Policy settings control the threshold for this response and the actions to be taken after the threshold is reached.

1. **Account lockout threshold policy** setting determines the number of failed sign-in attempts that will cause a user account to be locked. A locked account cannot be used until administrator reset it or until the number of minutes specified by the account lockout duration policy setting expires.

1. **Account lockout duration policy** setting determines the number of minutes that a locked-out account remains locked out before automatically becoming unlocked.

1. **Reset account lockout counter after** policy setting determines the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0. If Account lockout thresholdis set to a number greater than zero, this reset time must be less than or equal to the value of account lockout duration.

**3. what is trust relationship**

Active Directory Domain Services (AD DS) provides security across multiple domains or forests through domain and forest trust relationships. To check for this trust relationship, the Windows security system computes a trust path between the domain controller (DC) for the server that receives the request and a DC in the domain of the requesting account. An access control mechanisms provided by AD DS and the Windows distributed security model provide an environment for the operation of domain and forest trusts. For these trusts to work properly, every resource or computer must have a direct trust path to a DC in the domain in which it is located.

Different types of trust areTree-root trust, Parent-child trust, External trust, Forest trust, Realm trust. The flow of communication over trusts is determined by the direction of the trust. Trusts can be one-way or two-way, and can be transitive or non-transitive.

**4. type of trust relationship describe all trust**

Different types of trust areTree-root trust, Parent-child trust, External trust, Forest trust, Realm trust.

1. **Tree-root trust :**

Tree-root trusts are also two-way transitive trusts similar to parent-child trusts. When a new domain tree is created within a forest, a tree-root trust is automatically created between the new domain tree and all existing domain trees. For example, domain A is an existing domain with child domains B and C within a forest X. When a new domain D with child domains E and F are created since they come under the same forest X, domains D, E, and F will automatically be trusted by domains A, B, and C.

1. **Parent-child trust :**

A parent-child trust is a two-way transitive trust. A parent-child trust is automatically established when a child domain is added to a parent domain. When new child domains are added, the trust path flows upward through the domain hierarchy.

**(iii) External trust :**

An external trust is a one-way non-transitive trust. These trusts are manually established. An external trust is established with an external domain outside the forest of the trusting domain.

**(iv)Forest trust :**

Forest trusts are transitive, and they can either be one-way or two-way trusts. Forest trusts are ones that occur between forests, and these trusts are manually created. When one forest trusts another forest, all the domains within the two forests will automatically trust each other.

1. **Realm trust :**

Real trust is trust between a domain or a forest with another domain or a forest that is not based on Windows Active Directory. Realm-trusts allow for cross-platform communication between domains. This trust is one-way by default. To create a two-way trust, one must create trust in the other way.

1. **Shortcut trust :**

Shortcut trusts are one-way transitive trusts. These trusts are created manually. These trusts are created when one domain needs to trust another domain by bypassing the hierarchy of trusts such as parent-child trusts or forest-root trusts. A shortcut trust is usually established to shorten what is called a trust path. A trust path is a path that an authentication process must take if two domains do not directly trust each other. So, direct trust is established. Hence, shortcut trust is used to make the authentication process between two domains simpler.

**5. what is site and subnet ?**

**AD Sites :** These are the objects that represent the physical locations of DCs and/or client machines. Typically, every defined site should have at least one DC, and the sites should match the physical locations the servers are in. Specifically, servers that are on the same LAN should be in the same site, and servers that are separated by a WAN should be in separate sites.

**A subnet :** or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments. Subnets are the IP ranges that are associated with specific AD sites. DCs and clients use the subnets you define to determine what site they are in.

 Practical

1. manage active directory offline

DONE

1. restore object of active directory from AD Recycle bin

DONE

1. backup active directory

DONE

1. manage active directory replication---repadmin DcDiag

DONE

1. create multiplae UPN suffix multidomain enviourment

DONE

1. configure trust between forest check with login

DONE

1. configure ADDS sites and subnet

DONE

#### **Group Policy**

**1. what is group policy?**

Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers.

Group Policy is primarily a security tool, and can be used to apply security settings to users and computers. Group Policy allows administrators to define security policies for users and for computers. These policies, which are collectively referred to as Group Policy Objects GPOs, are based on a collection of individual Group Policy settings. Group Policy objects are administered from a central interface. Group Policy can also be managed with command line interface tools such as gpresult and gpupdate.

**2. what is default policy? Default Domain and domain controller**  **Default policy** :

Policies are being used to determine how and when Internet requests are handled for users and devices. Each policy includes information about which websites and Internet communication protocols are blocked or permitted, and the days and times to enforce those rules. The Default policy is in effect 24 hours a day, 7 days a week. This policy is used to handle requests whenever no other policy applies. Initially, the Default policy monitors requests without blocking.

**Default Domain Policy :**

Windows Server creates a Default Domain Policy GPO for every domain in the forest. This domain is the primary method used to set some security-related policies such as password expiration and account lockout. You can use fine-grain password and account lockout policy to apply custom password and account lockout policy settings to individual users and global security groups within a domain.

**Default Domain Controllers Policy:**

A default GPO that is automatically created and linked to the domain whenever a server is promoted to a domain controller. This GPO represents the default policy that is applied to all domain controllers in the Domain Controllers container.

**3. what is user configuration and computer configuration**

**Computer Configuration** : In Group Policy is applied to computers, regardless of who logs on to the computers. The Computer Configuration section is used for computerwide settings. Many of these settings are applied when the system first boots up.

**User Configuration** : It controls the user’s log-on session. Settings configured for a computer are processed first when the computer starts, followed by the user configuration settings when the user logs on. User Configuration in Group Policy is applied to users, regardless of which computer they log on to.

**4. what is GPO?**

GPO stands for Group Policy Object, It is a virtual collection of policy settings. A GPO has a unique name, such as a GUID. Group Policy settings are contained in a GPO. A GPO can represent policy settings in the file system and in the Active Directory. GPO settings are evaluated by clients using the hierarchical nature of Active Directory.

**5. define software setting, windows setting, and administrative templates**

**Software Setting**

Software installation and upgrades are configured here. Two options are available for installing software.

1. **Assign :**

When a software package is assigned to a computer, it is automatically installed on that computer and is available for use to all the users who log on to that computer. When a software package is assigned to a user, it is automatically installed when the user logs on to a computer and is available only for that user. The software assigned to a user will be available on all the machines the user logs on to.

1. **Publish :**

The software can be published only to users and not computers. Published software is made available to the users in the Add/Remove Programs of the Control Panel. Users can install the software whenever the need arises.

**Windows Settings**

The following are some of the important Windows Settings that can be configured using Group Policies.

1. **Scripts :**

Scripts are programming codes that perform some action when executed.

Startup/Shutdown scripts can be configured for the computer and Logon/Logoff scripts can be configured for the user.

1. **Security Settings :**

Both the Computer and User configuration sections have many important security settings that can be configured here. Some of the most important settings are :

* + Account Policies
  + Local Policies
  + Audit policy
  + User Rights Assignment
  + Security Options
  + Software Restriction Policies
  + Internet Explorer Maintenance
  + Folder Redirection

 **Administrative Templates**

It contains a number of settings that can be used to customize the user/computer environment.

**(i) Computer Configuration :**

Some of the important settings available under Computer Configuration are as follows:

* **Windows Components:** Contains settings related to NetMeeting, Task Scheduler, Windows Installer, etc.
* **System:** Contains settings related to Disk Quotas, Group Policy, Logon, Shutdown Options and much more.
* **Network:** Contains settings related to Network Connections, Offline Files, etc.

**(ii) User Configuration :**

Some of the important settings available under User Configuration are as follows:

* **Control Panel:** Contains settings related to the management of Control Panel such as Remove Add/Remove Programs.
* **Desktop:** Contains settings related to the management of the User’s Desktop such as Wallpaper settings, Show/Hide desktop icons, etc.
* **Start Menu and Taskbar:** Contains settings related to the configuration of the start menu and taskbar such as lock taskbar, classic start menu, etc.

**6. link GPO**

To complete this procedure, user must be a member of the Domain Admins groupTo link the GPO to the domain container in Active Directory :

* Open the Group Policy Management console.
* In the navigation pane, expand **Forest:** forestname, expand **Domains**, and then expand domainname.
* Right-click domainname and then click **Link an Existing GPO**.
* In the **Select GPO** dialog box, select the GPO to deploy, and then click **OK**.
* The GPO appears in the **Linked Group Policy Objects** tab in the details pane and as a linked item under the domain container in the navigation pane.
* The order of the linked GPOs can be adjust to ensure that the higher priority GPOs are processed last. Select a GPO and click the up or down arrows to move it. The GPOs are processed by the client device from the highest link order number to the lowest.

**7. delegation GPO management**

The management of group policies can be fully delegated to dedicated administrators without the need to add them as members of domain admins Active Directory groups.

This could be done by following this approach:

* Open the Group Policy Management Console. Expand the **Starter GPOs** node.
* Click the Starter GPO you want to delegate.
* In the results pane, click the **Delegation** tab.
* Click **Add**.
* In the **Select User, Computer, or Group** dialog box, click **Object Types**, select the types of objects to add Starter GPO permissions, and then click **OK**.
* Click **Locations**, select either **Entire Directory** or the domain or organizational unit containing the object to add Starter GPO permissions, and then click **OK**.
* In the **Enter the object name to select** box, type the name of the object to add Starter GPO permissions by performing one of the following actions.
* To search for the name, click **Advanced**, type the search criteria, click **Find Now**, select the name in the list box, click **OK**, and then click **OK** again.
* In the **Permissions** box of the **Add Group or User** dialog box, select the appropriate permissions from the drop-down list, and then click **OK**.

**8. inheritance policy**

A policy is specified for an administration group. Policy settings can be inherited, that is, received in the subgroups (child groups) of the administration group for which they were set. Hereinafter, a policy for a parent group is also referred to as a parent policy.

It can be enable or disable two options of inheritance: Inherit settings from parent policy and Force inheritance of settings in child policies. By default, the Inherit settings from parent policy option is enabled for a new policy. If a policy has profiles, all the child policies inherit these profiles.

**9. filtering**

Group Policy can map to Sites, Domain and OUs. If group policy is mapped to OU, by default it will apply to any object under it. But within a OU, Domain or Site there are lots of objects.

The security, system or application settings requirements covers by group policies not always applies to boarder target groups. Group Policy filtering capabilities allows to further narrow down the group policy target to security groups or individual objects. There are few different ways we can do the filtering in group policy :

* + Security Filtering
  + WMI Filtering

**10. script, templates**  **Script** :

* Microsoft offers various options for integrating scripts into Group Policy, which makes the administration of computers extremely flexible. Group Policy allows to associate one or more scripting files to four triggered events:
* Computer startup
* Computer shutdown
* User logon
* User logoff

* Windows PowerShell scripts can be used, or author scripts in any other language supported by the client computer. Windows Script Host (WSH) supported languages and command files are also used, including VBScript and Jscript.

**Templates :**

* Policy settings that appear in the Administrative Templates node of the GPO Editor contain Registry settings to achieve each of the settings contained in the hierarchy. It contains a number of settings that can be used to customize the user/computer environment.
* Administrative templates contain settings for Windows components such as

NetMeeting, Internet Explorer, Terminal Services, Windows Media Player, and Windows update, to name a few. Other components common to both user and computer configurations include settings for user profiles, script execution, and group policy.

* While the different policy settings between user and computer configurations are too numerous to list here, there are some key components available for the user configuration. These include the Start Menu, Taskbar, Desktop, Control Panel, and Shared folder settings.

 Practical

1. backup restore import and copy GPO

DONE

1. force group policy command

DONE

1. check group policy settings

DONE

1. configure folder redirection

DONE

1. software installation ---assign and publish

DONE

1. drive map through policy

DONE

# Certification services

**1. purpose of certification**

Certificate Services allows an organization to manage the issuing, renewal and revocation of certificates. It has a number of features which make it valuable to organizations that do not choose to rely upon external certification authorities and who need a flexible tool that can be adapted to the needs of the organization.

**2. certificate service and its role service –certificate authority, certificate enrolment policy web service**

**Certificate Service :** a service running on a Windows server operating system, receives requests for new digital certificates over transports such as RPC or HTTP. It checks each request against custom or site-specific policies, sets optional properties for a certificate to be issued, and issues the certificate.

 Certificate Services allows administrators to add elements to a Certificate Revocation List (CRL), and to publish signed CRLs on a regular basis. Certificate services include programmable interfaces for creating support for additional transports, policies, and certificate properties and formats.

**Certificate Authority :** Certificate Services is a development platform for building Certification Authorities for enterprises or secure Internet applications. A configured and operational certification authority will allow a site to issue, track, manage, and revoke certificates with minimal administration overhead and maximal security.

**Certificate Enrolment Web Service :** The Certificate Enrolment Web Service is an Active Directory Certificate Services (AD CS) role service that enables users and computers to perform certificate enrolment by using the HTTPS protocol. Together with the Certificate Enrolment Policy Web Service, this enables policy-based certificate enrolment when the client computer is not a member of a domain or when a domain member is not connected to the domain.

 The Certificate Enrolment Web Service uses the HTTPS protocol to accept certificate requests from and return issued certificates to network client computers. The Certificate Enrolment Web Service uses the DCOM protocol to connect to the certification authority (CA) and complete certificate enrolment on behalf of the requester.

**3. standalone v/s enterprise CA**  **Enterprise CA :**

* It is integrated with Active Directory. The server will use domain services for certificate management, integrates with the directory for naming and authentication, and provides a ton of other integration points that simplify the user experience.
* It should be use an Enterprise CA for issuing end-entity, or user and computer, certificates. It is fantastic in that role. A root CA should never be an Enterprise CA because that would expose the root CA to increased risk of attack or misconfiguration. It is considered an extremely bad practice in all cases. Never, ever create an Enterprise Root CA.

**Standalone CA :**

* It is one that doesn’t integrate with AD. This is a great implementation choice for many scenarios including non-AD clients, offline servers, or simply in case of not want to use Active Directory to manage certificates.
* The main drawback with a Standalone CA is that it needs to be backed up on its own instead of relying on Active Directory replication. Another possible drawback is that users may need to authenticate using separate credentials if the Standalone CA is not part of a domain.

**4. root CA and subordinate CA**  **Root CA** :

The root CA is the highest level of the hierarchy and serves as the trust anchor. In order for an end entity certificate to be trusted, the root CA it chains up to must be embedded in the operating system, browser, device, or whatever is validating the certificate. Root CAs are heavily secured and kept offline.

**Subordinate CAs** :

These live between the root and end entity certificates and their main purpose is to define and authorize the types of certificates that can be requested from the root CA.

**5. describe certificate templates and how to use it**

**Certificate Template** : It defines some predefined structure and policies associated with the certificate. The certificate templates and their permissions are defined in Active Directory, and are valid within the forest. This is because Certificate Templates are stored in AD Configuration partition, which is replicated to the entire forest. When a certificate template is created in one CA, it should be available to all other CAs within that forest, which is accomplished through AD Replication. Some of which are as follows:

* Format and Content of Certificate suitable for specific need.
* To specify which users and computers can request for what type of certificates though well defined permission settings.
* To specify the enrolment process, manual or Auto enrolment.
* To specify whether the private key would be exportable or not.

**How to use Certificate Template :**

* Open the Certificate Authority Console in the CA server.
* It will show a section called “Certificate Template”. This section shows all the templates which are enabled for this CA.
* Now, right click on “Certificate Template” and click “Manage”.
* It shows all the default templates.
* One can use to copy the default template, and to customize the duplicate template rather than customizing the default template itself.

 Practical

1. install certiface services ---certifacte authority and web enrolment

DONE

1. issue certificate through web enrolment and make secure web site

DONE

1. self-signed certificate

DONE

1. mange certificate---using template and issue certificate for computer

DONE

1. backup CA

DONE

# ADFS

**1. what is federation services**

Active Directory Federation Service (AD FS) enables Federated Identity and Access Management by securely sharing digital identity and entitlements rights across security and enterprise boundaries. AD FS extends the ability to use single sign-on functionality that is available within a single security or enterprise boundary to Internet-facing applications to enable customers, partners, and suppliers a streamlined user experience while accessing the web-based applications of an organization.

**2. ADFS service component**

 Active Directory Federation Services consists of four major components:

**(i) Active Directory:**

This is where all the identity information is stored to be used by ADFS.

**(ii)Federation server:** Contains the tools needed to manage federated trusts between business partners, and hosts the “Federation Service” role service of ADFS. It routes requests that come in from external users and also hosts a security token service that issues tokens for claims based on verification of credentials from AD.

**(iii)Federation server proxy:** Hosts the Federation Service Proxy role service of ADFS. External clients connect to this proxy server when requesting the security token. It’s deployed in your organization’s perimeter network (DMZ or extranet). This is done because the federation server is not exposed directly to the internet as it is heavily dependent on the AD doing so would be a major security risk. So the proxy server forwards the requests from the outside world to the federation server.

**(iv)ADFS web server:** Hosts either the claims-aware or the Windows token-based ADFS Web Agent role service. This web agent manages security tokens and authentication cookies that are sent to the web server for authenticating external users.

**3. ADFS requirement**

The following are the requirements for deploying AD FS:

* + Certificates requirements
  + Hardware requirements
  + Proxy requirements
  + ADDS requirements
  + Configuration requirement database
  + Browser requirements
  + Network requirements
  + Permissions requirements

It requires services and features such as :

* + Active Directory Certificate Services
  + Active Directory Domain Services
  + Active Directory Federation Services
  + DNS Server
  + File and Storage Services
  + Web Server (IIS)
  + .NET Framework 3.5 Features
  + .NET Framework 4.5 Features
  + Group Policy Management
  + Remote Server Administration Tools
  + SMB 1.0/CIFS File Sharing Support  User Interfaces and Infrastructure
  + Windows Internal Database
  + Windows PowerShell
  + Windows Process Activation Service
  + WoW64 Support

**4. multifactor authentication**

AD FS is an identity access solution that provides client computers (internal or external to network) with seamless SSO access to protected Internet-facing applications or services, even when the user accounts and applications are located in completely different networks or organizations.

In order to enable multi-factor authentication (MFA), must have to select at least one extra authentication method. By default, in Active Directory Federation Services (AD FS) in Windows Server, it can be selected Certificate Authentication an extra authentication method.

**5. web application proxy**

In Active Directory Federation Services (AD FS), the role of a federation server proxy is handled by a new Remote Access role service called Web Application Proxy. To enable AD FS for accessibility from outside the corporate network, which was the purpose of deploying a federation server proxy in legacy versions of AD FS, such as AD FS 2.0 and AD FS.

In the context of AD FS, Web Application Proxy functions as an AD FS federation server proxy. In addition to this, Web Application Proxy provides reverse proxy functionality for web applications inside any corporate network to enable users on any device to access them from outside the corporate network.

 Practical

1. Install ADFS service and configure between two trusted

DONE

1. organizations (relay party trust)

DONE

1. multifactor authentication

DONE

# ADRMS

**1. what is ADRMS**

AD RMS is the server Microsoft Windows security tool that provides with management and development tools that work with industry security technologies including encryption, certificates, and authentication to help organizations create reliable information protection solutions.

Active Directory Rights Management Services (AD RMS) is a that provides persistent data protection by enforcing data access policies. For documents to be protected with AD RMS, the application the document is associated with must be RMS-aware. Originally known as Windows RMS, the name was changed AD RMS in Windows server 2008.

AD RMS has server and client components. The server component is made up of multiple web services that run on a Microsoft server. The client component, which can either be run on a client or server operating system, contains functions that enable an application to encrypt and decrypt content, acquire licenses and certificates from a server and perform many other security-related tasks.

**2. how to secure data and type of security**

Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers hardware, software, storage devices, and user devices; access and administrative controls; and organizations’ policies and procedures.

* These tools can protect data through processes like data masking, encryption, and redaction of sensitive information. The process also helps organizations streamline their auditing procedures and comply with increasingly stringent data protection regulations.

* Active Directory Rights Management Services (AD RMS) is an information protection platform that enables documents to be shared with protection so that only authorized users are allowed to perform specific actions on them. In order to ensure that content remains protected, AD RMS utilizes cryptographic technologies that require the generation and storage of public and private keys.

**Type of security** : Organizations can use a wide range of data security types to safeguard their data, devices, networks, systems, and users. Some of the most common types of data security, which organizations should look to combine to ensure they have the best possible strategy, include:

1. **Encryption :**

Data encryption is the use of algorithms to scramble data and hide its true meaning. Encrypting data ensures messages can only be read by recipients with the appropriate decryption key. This is crucial, especially in the event of a data breach, because even if an attacker manages to gain access to the data, they will not be able to read it without the decryption key. Data encryption also involves the use of solutions like tokenization, which protects data as it moves through an organization’s entire IT infrastructure.

1. **Data Erasure :**

There will be occasions in which organizations no longer require data and need it permanently removed from their systems. Data erasure is an effective data security management technique that removes liability and the chance of a data breach occurring.

1. **Data Masking :**

Data masking enables an organization to hide data by obscuring and replacing specific letters or numbers. This process is a form of encryption that renders the data useless should a hacker intercept it. The original message can only be uncovered by someone who has the code to decrypt or replace the masked characters.

1. **Data Resiliency :**

Organizations can mitigate the risk of accidental destruction or loss of data by creating backups or copies of their data. Data backups are vital to protecting information and ensuring it is always available. This is particularly important during a data breach or ransomware attack, ensuring the organization can restore a previous backup.

**3. what is service account**

A service account is a user account that is created explicitly to provide a security context for services running on Windows Server operating systems. The security context determines the service's ability to access local and network resources. The Windows operating systems rely on services to run various features. These services can be configured through the applications, the Services snap-in, or Task Manager, or by using Windows PowerShell. Different service accounts are as follow :

**(i) Standalone managed service accounts :**

A managed service account is designed to isolate domain accounts in crucial applications, such as Internet Information Services (IIS), and eliminate the need for an administrator to manually administer the service principal name (SPN) and credentials for the accounts.

1. **Group-managed service accounts:**

Group-managed service accounts are an extension of the standalone-managed service accounts, which were introduced in Windows Server 2008 R2. These accounts are managed domain accounts that provide automatic password management and simplified service principal name (SPN) management, including delegation of management to other administrators.

1. **Virtual accounts :**

Virtual accounts were introduced in Windows Server 2008 R2 and Windows 7, and are managed local accounts that provide the following features to simplify service administration:

* + The virtual account is automatically managed.
  + The virtual account can access the network in a domain environment.
  + No password management is required.

 Practical

1. install ADRMS and secure data (different security apply)

DONE