***Module: 14 Identity with Windows Server***

***Active directory domain services***

1. ***What is a domain controller?***

***Ans.*** *A domain controller is the server responsible for managing network and identity security requests. It acts as a gatekeeper and authenticates whether the user is authorized to access the IT resources in the domain. The Microsoft Windows Active Directory Server hierarchically organizes and protects user information, business-critical data, and IT devices operating on the network.*

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

***Ans.*** *A* ***forest*** *is a collection of one or more domain trees. The* ***domains*** *in the movie.edu domain tree and the example.com domain tree could be part of the same forest. A domain tree is based on a common namespace, but a forest is not. A forest is named after the first domain created in the forest.*

*A* ***schema*** *is the definition of attributes and classes that are part of a distributed directory and is similar to fields and tables in a database. Schemas include a set of rules which determine the type and format of data that can be added or included in the database.*

*An* ***organizational unit*** *(OU) is a container within a Microsoft Active Directory domain which can hold users, groups and computers.*

*A* ***container*** *is a unit of software that packages code and its dependencies so the application runs quickly and reliably across computing environments.*

*A site is made up of one or more Internet Protocol (IP) subnets that are linked by high-speed and reliable connections. Sites represent the physical structure or topology of your network, and a domain represents the logical structure where all the domain controllers are logically linked.*

1. ***partition, trust relationship***

***Ans.*** *Directory partitions are also known as naming contexts. A directory partition is a contiguous portion of the overall directory that has independent replication scope and scheduling data.*

*Trust relationships are an administration and communication link between two domains. A trust relationship between two domains enables user accounts and global groups to be used in a domain other than the domain where the accounts are defined.*

1. ***What is active directory?***

***Ans.*** *Active Directory (AD) is a* [*directory service*](https://en.wikipedia.org/wiki/Directory_service) *developed by* [*Microsoft*](https://en.wikipedia.org/wiki/Microsoft) *for* [*Windows domain*](https://en.wikipedia.org/wiki/Windows_domain) *networks. It is included in most* [*Windows Server*](https://en.wikipedia.org/wiki/Windows_Server)[*operating systems*](https://en.wikipedia.org/wiki/Operating_system) *as a set of* [*processes*](https://en.wikipedia.org/wiki/Process_(computing)) *and* [*services.*](https://en.wikipedia.org/wiki/Windows_service) *Initially, Active Directory was used only for centralized domain management. However, Active Directory eventually became an umbrella title for a broad range of directory-based identity-related services.*

*A server running the Active Directory Domain Service (AD DS) role is called a* [*domain controller*](https://en.wikipedia.org/wiki/Domain_controller)*. It* [*authenticates*](https://en.wikipedia.org/wiki/Authentication) *and* [*authorizes*](https://en.wikipedia.org/wiki/Authorization) *all users and computers in a* [*Windows*](https://en.wikipedia.org/wiki/Microsoft_Windows) *domain type network, assigning and enforcing security policies for all computers, and installing or updating software. For example, when a user* [*logs into*](https://en.wikipedia.org/wiki/Login) *a computer that is part of a Windows domain, Active Directory checks the submitted username and password and determines whether the user is a* [*system administrator*](https://en.wikipedia.org/wiki/System_administrator) *or normal user Also, it allows management and storage of information, provides authentication and authorization mechanisms and establishes a framework to deploy other related services: Certificate Services,* [*Active Directory Federation Services*](https://en.wikipedia.org/wiki/Active_Directory_Federation_Services)*, Lightweight Directory Services, and* [*Rights Management Services*](https://en.wikipedia.org/wiki/Active_Directory_Rights_Management_Services)

*Active Directory uses* [*Lightweight Directory Access Protocol*](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) *(LDAP) versions 2 and 3, Microsoft's version of* [*Kerberos*](https://en.wikipedia.org/wiki/Kerberos_(protocol)) *and* [*DNS*](https://en.wikipedia.org/wiki/Domain_Name_System)*.*

*Robert R. King defined it in the following way*

*"A domain represents a database. That database holds records about network services-things like computers, users, groups and other things that use, support, or exist on a network. The domain database is, in effect, Active Directory."*

1. ***What is a global catalog server?***

***Ans.*** *The global catalog is a feature of* [*Active Directory*](https://www.netwrix.com/what_is_active_directory_e-book.html?cID=70170000000kgEZ) *(AD) that allows a domain controller (DC) to provide information on any object in the forest, regardless of whether the object is a member of its domain. Domain controllers with the global catalog feature enabled are referred to as global catalog servers.*

1. ***What is ADC AND RODC?***

***Ans.*** *Checking the FSMO roles to the ADC server after role transfer. Read-only domain controller (RODC) RODC 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.*

1. ***What is the operation master role?***

***Ans.*** *Operations master role holders are assigned automatically when the first domain controller in a given domain is created. The two forest-level roles (schema master and domain naming master) are assigned to the first domain controller created in a forest.*

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

***Ans.*** *An operations master server is also known as the Flexible Single Master Operations (FSMO) server. There are five different operations master roles: Schema, Domain Naming, Primary Domain Controller (PDC) emulator, Relative Identifier (RID), and Infrastructure. Only domain controllers can hold these roles.*

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

***Ans.*** *Transferring makes the old DC know that it does not own the role(s) any more. If the DC is broken (e. g. hardware defect) and will never come back again, then you can seize the role on a remaining DC.*

1. ***password policy***

***Ans.*** *A password policy defines the password strength rules that are used to determine whether a new password is valid. A password strength rule is a rule to which a password must conform.*

1. ***what id profile and type of profile?***

***Ans.*** *A profile-type defines a set of properties, also referred to as a schema, that are inherent to all profiles of that type. This set of properties is used internally to group objects and enforce overall system constraints. Examples of common profile-types are customer , employee , and contractor .*

1. ***group nesting and scope, type of group***

***Ans.* *Group nesting-*** *Adding a group as a member of another group is called nesting.*

***Scope-*** *The scope of an AD group determines both where the group can be applied in the forest or domain and who can be a member of a group. Because Active Directory has few limitations on how groups can be nested within each other, group nesting can present massive security and operational risks to an organization.*

*Active Directory defines the following three group scopes: Universal. Global.*

* ***Practical***

1. ***install ADDS and create a new forest***

***Ans.*** *Done in lab.*

1. ***give membership of pc to domain***

***Ans.*** *Done in lab.*

1. ***create a ADC***

***Ans.*** *Done in lab.*

1. ***create RODC and password replication***

***Ans.*** *Done in lab.*

1. ***create a new site***

***Ans.*** *Done in lab.*

1. ***create a new child domain***

***Ans.*** *Done in lab.*

1. ***create a new tree***

***Ans.*** *Done in lab.*

1. ***create a new user with GUI and CLI***

***Ans.*** *Done in lab.*

1. ***create roaming profile***

***Ans.*** *Done in lab.*

1. ***create OU and give delegation***

***Ans.*** *Done in lab.*

1. ***create a group***

***Ans.*** *Done in lab.*

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

***Ans.*** *Done in lab.*

1. ***Doamin name master—***

***Ans.*** *Done in lab.*

1. ***GUI and ntdsutil***

***Ans.*** *Done in lab.*

1. ***IFM***

***Ans.*** *Done in lab.*

***Advance feature***

1. ***describe account policy***

***Ans.*** *A user account policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, typically within an organization. It is very important for large sites where users typically have accounts on many systems.*

1. ***describe account lockout policy***

***Ans.*** *The 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 can't be used until you reset it or until the number of minutes specified by the Account lockout duration policy setting expires.*

1. ***what is trust relationship***

***Ans.*** *Trust relationships are an administration and communication link between two domains. A trust relationship between two domains enables user accounts and global groups to be used in a domain other than the domain where the accounts are defined.*

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

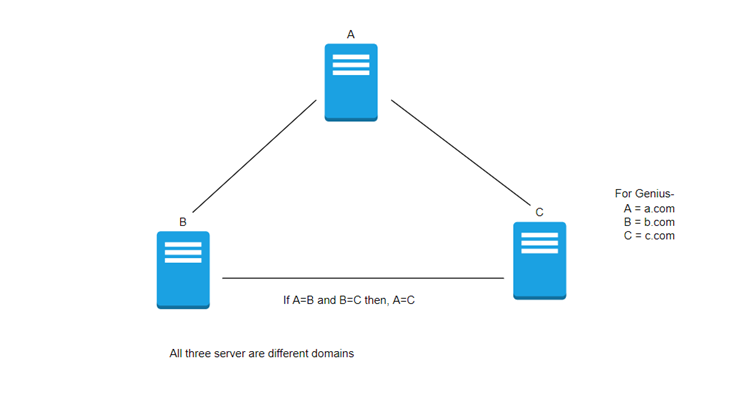
### ***Ans.* *AD Trust types***

* *Transitive Trust*
* *Non-Transitive trust*

#### ***Transitive Trust***

*Basically, Transitive trust is a two-way relationship automatically created between parent and child domains in Microsoft Active Directory Forest. When a domain is created, it shares the resource with its parent domain by default, enabling an authenticated users to access a resource in both the child and parent.*

***For example****, In an Active Directory transitive trust relationship, if domain A (a.com) trusts domain B (b.com), and domain B has a transitive trust with domain C (c.com), therefore domain A automatically trusts domain C.*



#### ***Non-Transitive Trust***

*Inside Non-Transitive trust, if domain A trusts domain B, and domain B has a non-transitive trust with domain C. In this case, even though domain A has an indirect link to domain C through domain B, domain A does not trust domain C because the trust is non-transitive.*

*Active Directory is classified into two categories; they are as follows –*

* *One way Trust*
* *Two-way Trust*

### ***One-way Trust***

*It means that when a domain trusts another domain, that trust does not replicate visa versa. Hence, the trust flows only one way.*

*For example, if domain A has a one-way trust with domain B, then domain A trusts domain B and can access a resource from domain B. However, domain B does not trust domain A and cannot access a resource from domain A.*

### ***Two-way Trust***

*In two-way trust, when one domain trusts another domain, the other way is also trust. So, both domains can access the resource of the other.*

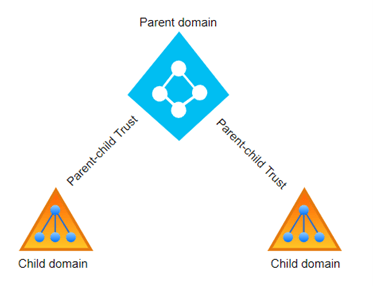
*For example, if domain A has two-way trust with domain B, it automatically means that domain B also trusts domain A, and both domains can share resources between themselves.*

*There are Five types of Trust in Active Directory –*

* *Parent-child Trust.*
* *Tree-Root Trust.*
* *Forest Trust.*
* *Shortcut Trust.*
* *Realm Trust.*
* *External Trust.*

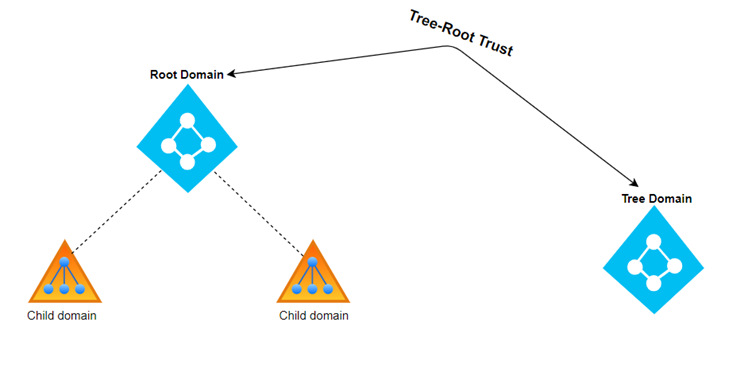
### ***Parent-child Trust***

*Parent-child trust is implicitly established. It is a two-way transitive trust. Parent-child trust is automatically generated when a child domain is added to a parent domain. When a new child domain is added, the trust path flows upward through the domain hierarchy.*



### ***Tree-Root Trust***

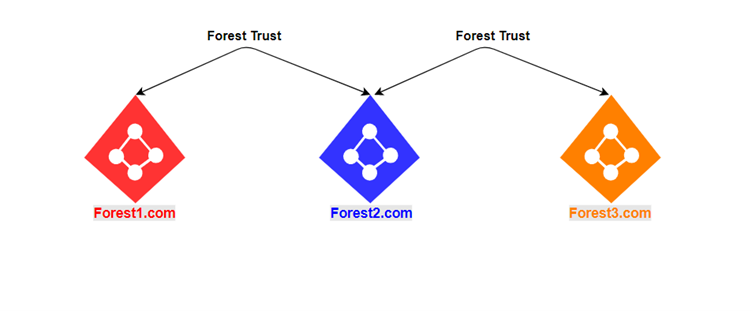
*Tree-root trust is also a two-way transitive trust similar to parent-child trust. When a new domain tree is created within a forest, a tree-root trust is automatically created between the new domain tree and all exiting tree domains.*



### ***Forest Trust***

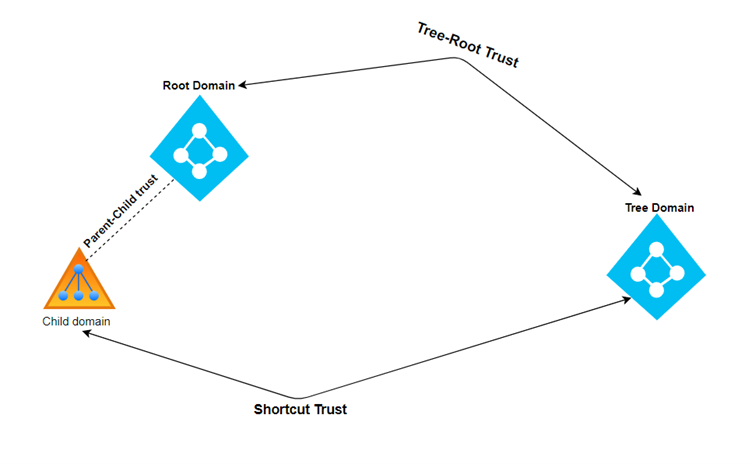
*Forest trust are transitive trust, and they can either one-way or two-way trust. It is explicitly transitive (between two forest) created trust between two forest root domains. Forest trust are manually created, one-way transitive or two-way transitive trust that allows you to provide access to the resource between multiple forest. It required DNS resolution to be established between forests.*

*Forest trust cannot be extended to other forests, for example, if* ***Forest1.com*** *trusts* ***Forest2.com****, and another forest* ***Forest3.com*** *trust is created between* ***Forest2.com*** *and* ***Forest3.com****,* ***Forest1.com*** *does not have an implied trust. If a trust is required, one must be manually created.*



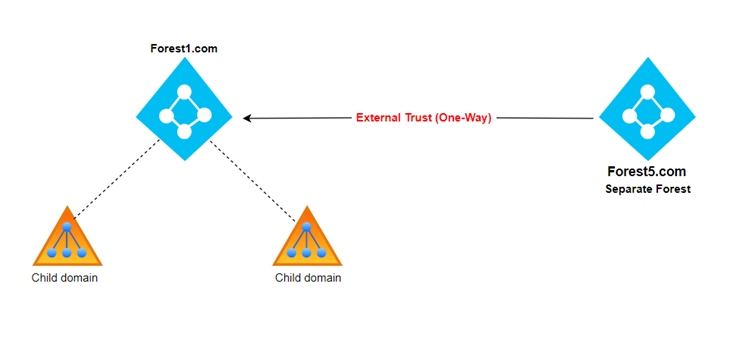
### ***Shortcut Trust***

*Shortcut trust are manually created one-way, transitive trusts. They can only exist within a forest. They are created to optimize the authentication process shortening the trust path. These trusts are created when one domain needs to trust another domain by bypassing the hierarchy of trusts such as parent-child trust and Tree-root trusts.*



### ***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.*



### ***Realm Trust***

*These kinds of trust between a domain or a forest with another domain and a forest that is not based on Windows Active Directory. A Realm Trust can be established to provide resource access and cross-platform inter-operability between an AD DS Domain and non-windows Kerberos v5 Realm.*

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

***Ans.*** *A site is made up of one or more Internet Protocol (IP) subnets that are linked by high-speed and reliable connections. Sites represent the physical structure or topology of your network, and a domain represents the logical structure where all the domain controllers are logically linked.*

* ***Practical***

1. ***manage active directory offline***

***Ans.*** *Done in lab.*

1. ***restore object of active directory from AD Recycle bin***

***Ans.*** *Done in lab.*

1. ***backup active directory***

***Ans.*** *Done in lab.*

1. ***manage active directory replication---repadmin DcDiag***

***Ans.*** *Done in lab.*

1. ***create multiplae UPN suffix multidomain enviourment***

***Ans.*** *Done in lab.*

1. ***configure trust between forest check with login***

***Ans.*** *Done in lab.*

1. ***configure ADDS sites and subnet***

***Ans.*** *Done in lab.*

***Group Policy***

1. ***what is group policy?***

***Ans.*** *Group Policy is a feature of the Microsoft* [*Windows NT*](https://en.wikipedia.org/wiki/Windows_NT) *family of* [*operating systems*](https://en.wikipedia.org/wiki/Operating_system) *(including Windows 7, Windows 8.1, Windows 10, Windows 11, and Windows Server 2003+) that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an* [*Active Directory*](https://en.wikipedia.org/wiki/Active_Directory) *environment. A set of Group Policy configurations is called a Group Policy Object (GPO). A version of Group Policy called Local Group Policy (LGPO or Local GPO) allows Group Policy Object management without Active Directory on standalone computers.*

*Active Directory servers disseminate group policies by listing them in their* [*LDAP*](https://en.wikipedia.org/wiki/LDAP) *directory under objects of class group Policy Container. These refer to fileserver paths (attribute gPCFileSysPath) that store the actual group policy objects, typically in a* [*SMB*](https://en.wikipedia.org/wiki/Server_Message_Block) *share \\domain.com\*[*SYSVOL*](https://en.wikipedia.org/wiki/File_Replication_Service) *shared by the Active Directory server. If a group policy has registry settings, the associated file share will have a file registry. Pol with the registry settings that the client needs to apply.*

1. ***what is default policy? Default Domain and domain controller***

***Ans.*** ***Default Domain Policy****: A default GPO that is automatically created and linked to the domain whenever a server is promoted to a domain controller. It has the highest precedence of all GPOs linked to the domain, and it applies to all users and computers in the domain.*

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

***Ans.*** ***Computer Configuration:*** *These policies apply to the local computer, and do not change per user.* ***User Configuration:*** *These policies apply to users on the local machine, and will apply to any new users in the future, on this local computer.*

1. ***what is GPO?***

***Ans.*** *A local Group Policy Objectrefers to the collection of group policy settings that only apply to the local computer and to the users who log on to that computer.*

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

***Ans.*** *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.*

1. ***link GPO***

***Ans.*** *To link the GPO to the domain container in Active Directory. Open the Group Policy Management console. In the navigation pane, expand Forest: YourForestName, expand Domains, and then expand YourDomainName. Right-click YourDomainName, and then click Link an Existing GPO.*

1. ***delegation GPO management***

***Ans.*** *A Group Policy Object (GPO) is a collection of Group Policy settings that determine how a system appears and behaves for a certain group of users. GPO delegation in AD allows you to offer end-users permission to execute certain Group Policy management activities that are typically performed by administrators.*

1. ***inheritance policy***

***Ans.*** *This is called GPO inheritance. It enables administrators to specify a common set of policies at the domain or site level while configuring specific policies at the OU level. Group policy inheritance is useful in many cases. For example, assume you need to make some changes to your finance department.*

1. ***filtering***

***Ans.*** Security filtering of a GPO allows you to limit what users or computers are hit by the GPO settings and allows you to delegate the administration of the GPO. To target a user or computer you must assign Read and Apply permissions to the user/computer or a group of which they are member.

1. ***script, templates***

***Ans.*** *GPO logon* ***scripts*** *allow you to run a BAT or PowerShell script at computer startup or user logon/logoff. In some cases, an administrator wants a particular script (command/program) to be run for each user or computer only once and not run at the next logons.****A template*** *is an uneditable, static version of a GPO for use as a starting point for creating new, editable GPOs. A user account with the Editor or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure.*

* ***Practical***

1. ***backup restore import and copy GPO***

***Ans.*** *Done in lab.*

1. ***force group policy command***

***Ans.*** *Done in lab.*

1. ***check group policy settings***

***Ans.*** *Done in lab.*

1. ***configure folder redirection***

***Ans.*** *Done in lab.*

1. ***software installation ---assign and publish***

***Ans.*** *Done in lab.*

***drive map through policy***

1. ***Certification services***

***Ans.*** *Certification Services means assessment of a product, process or service in accordance with Certification Procedures. Certification Services includes assessment and verification services, gap analysis and second party audits, whether or not a certificate is issued; Sample 1.*

1. ***purpose of certification***

***Ans.*** *The purpose of certification is to demonstrate that specified requirements are met. The requirements are usually based on international standards. For example, SFS-EN ISO 9001 is a generic quality management standard that is used as a requirement in the certification of organisations' quality management systems.*

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

***Ans.*** *A certificate service is basically an organization of services surrounding a CA that allows it to issue, renew, and revoke certificates. Certificates are what are used to pass a public key to computers, which need to communicate securely using the PKI system.*

*Active Directory Certificate Services or AD CS is used to establish an on-premises Public Key Infrastructure (PKI). It has the ability to create, validate and revoke public key certificates. These certificates have various uses such as encrypting files, emails, network traffic.*

*A certificate authority (CA) is a trusted entity that issues Secure Sockets Layer (SSL) certificates. These digital certificates are data files used to cryptographically link an entity with a public key. Web browsers use them to authenticate content sent from web servers, ensuring trust in content delivered online.*

*The Certificate Enrollment Web Service is an Active Directory Certificate Services (AD CS) role service that enables users and computers to perform certificate enrollment by using the HTTPS protocol.*

1. ***standalone v/s enterprise CA***

***Ans.*** *At the most basic level, the basic different between a standalone CA and an Enterprise CA is that an Enterprise CA needs to be a member of the domain while a standalone CA does not. If you decide to, you can install a standalone CA on a server that is a member of the domain.*

1. ***root CA and subordinate CA***

***Ans.*** *A CA certified by another is called a subordinate CA. A CA that is not certified by any other, but relies solely on its own reputation, is called a root CA.*

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

***Ans.*** *Certificate templates define the format and content of certificates issued by enterprise certificate authorities. A template determines which user or computer accounts can enroll for a certificate, and it defines the enrollment process (automatic, manual, or enrollment with authorized certificates).*

* ***Practical***

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

***Ans.*** *Done in lab.*

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

***Ans.*** *Done in lab.*

1. ***self-signed certificate***

***Ans.*** *Done in lab.*

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

***Ans.*** *Done in lab.*

1. ***backup CA***

***Ans.*** *Done in lab.*

***ADFS***

1. ***what is federation services***

***Ans.*** *ADFS is Microsoft’s on-prem SSO solution that authenticates users into applications that are incompatible with Active Directory (AD) and Integrated Windows Authentication (IWA). Microsoft released ADFS as an opportunity for many organizations that were taking advantage of the software-as-a-service (SaaS) boom of the 2000s.*

*At the time, Microsoft was dominating the IT industry, and nearly all applications that organizations used were on-premise and Windows-based. This created authentication challenges for applications that were outside the Windows ecosystem and the organization’s perimeter. However, ADFS allows identity information to be securely shared outside of a company’s network, in order to access web-facing resources like web apps that were hosted by organizations they had established relationships with.*

*In essence, it allows organizations to create a “trust relationship” between one another across the internet, complementing AD by extending identities in on-prem setups to cloud-based environments. It operates much like any web application-based SSO service that uses the* [*Secure Assertion Markup Language (SAML)*](https://jumpcloud.com/blog/what-is-saml) *protocol. ADFS can also use cookies and other token standards such as* [*JSON web tokens (JWT)*](https://dzone.com/articles/what-is-jwt-token) *to provide authentication services; however, it’s leveraged in on-prem setups rather than in the cloud.*

1. ***ADFS service component***

***Ans.*** *What are the components of ADFS? Active Directory: The Identity Information which is to be used by ADFS is stored on the Active Directory. Federation Server: It contains the tools needed to manage federated trusts between business partners.*

1. ***ADFS requirement***

***Ans.*** *All AD FS servers must be a joined to an AD DS domain. All AD FS servers within a farm must be deployed in a single domain. The domain that the AD FS servers are joined to must trust every user account domain that contains users authenticating to the AD FS service.*

1. ***multifactor authentication***

***Ans.*** *Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email, answer a secret question, or scan a fingerprint.*

1. ***web application proxy***

***Ans.*** *Web Application Proxy works in two main ways. It makes organizations capable of giving end users outside of an organization selective access to applications that run on servers in the organization. It also serves as a barricade between corporate applications and the Internet.*

* ***Practical***

1. ***Install ADFS service and configure between two trusted organizations (relay party trust)***

***Ans.*** *Done in lab.*

1. ***multifactor authentication***

***Ans.*** *Done in lab.*

***ADRMS***

1. ***what is ADRMS***

***Ans.*** *AD RMS is a server role in the Windows Active Directory. It helps augment the organizational security strategy by protecting your documents and emails using Information Right Management (IRM). AD RMS uses policy templates that are customizable to suit the specific needs of an organization. It not only takes care of what rights the user can have to access specific documents but also the validity period or expiry date for which a user can access it, no matter where the user is located. Further, AD RMS features are completely integrated with Microsoft Office Suite and can be further extended to work with other AD RMS-enabled servers in the domain or third-party applications using appropriate AD RMS Software Development Kits (SDKs).*

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

***Ans.*** 1. Understand data technologies and databases.

2. Identify and classify sensitive data.

3.Create a data usage policy.

4.Control access to sensitive data.

5.Implement change management and database auditing.

6.Use data encryption.

7.Back up your data.

8.Use RAID on your servers.

1. ***what is service account***

***Ans.*** *A service account is a user account that's created explicitly to provide a security context for services that are running on Windows Server operating systems. The security context determines the service's ability to access local and network resources. Windows operating systems rely on services to run various features.*

* ***Practical***

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

***Ans.*** *Done in lab.*