**Chapter-4: Active Directory Certificate Services**

**Lesson-1:**

**1. Certificate authorities (Digital certificates):**  
Certificates play an increasingly important part on Windows networks. A Certificate Authority (CA), also known as a certificate server, is a Windows Server 2012 role service responsible for issuing, revoking, verifying, and managing digital certificates.

**2. Certification Authority:** The core component responsible for issuing certificates to computers, users, and services. You can deploy four types of CA:

1. Enterprise root CA
2. Standalone root CA
3. Enterprise subordinate CA
4. and Standalone subordinate CA

**3. Enterprise root CA:**

An enterprise root CA is certificate server that has signed its own certificate, is installed on a computer that is a member of the domain, and can issue certificates based on templates stored in Active Directory.

Note: Enterprise CAs are integrated into Active Directory. You can configure them to automatically enroll certificates based on the requestor’s attributes in Active Directory.

**4. Standalone root CA:**  
Standalone CAs are not directly integrated into Active Directory, and you need to take special steps to configure all clients in a forest to trust the certificates issued by a specific standalone CA.

**5. Enterprise subordinate CA:**  
An enterprise subordinate CA can obtain its signing certificate from a standalone root CA or an enterprise root CA. Enterprise subordinate CAs are able to issue certificates based on certificate templates that are stored in Active Directory.

**6. Standalone subordinate CA:**  
You can deploy a standalone subordinate CA on a computer that is a member of a domain or a computer that is not domain joined. Standalone subordinate CAs are often deployed on perimeter networks.

**7. CA hierarchies**:  
The CA hierarchy determines how CAs are deployed in your organization. A CA hierarchy has two or more CAs. A root CA sits at the top, or apex of a hierarchy. An issuing CA sits at the base of the hierarchy.

**Note:**

■ You can install standalone CAs on computers that are both domain joined and not joined to a domain.  
■ Root CAs are the apex of a certificate services hierarchy. Root CAs use self-signed CA certificates.  
■ Subordinate CAs must have their CA certificate signed by another CA.

**8. Online responders:**

Online responders enable clients to perform certificate revocation checks without requiring them to download the entire CRL and delta CRL.

9. You configure CA role separation by assigning one of the following permissions:

1. Read
2. Issue and Manage Certificates
3. Manage CA
4. Request Certificates

**10. Which console you can use to back up the CA certificate, private key, certificate database, and certificate database log?**

Ans. You can use the Certificate Services console to back up the CA certificate, private key, certificate database, and certificate database log.

**CA backup and recovery**

Although you automatically back up a CA when you perform a full server or system state backup, you can also perform a backup and recovery of a certificate server from the Certification Authority console. A user needs to be assigned the Manage CA permission or be a member of the Backup Operators group to be able to back up a CA.

■ CDPs host lists of revoked certificates.  
■ By configuring CA security, you can allow users to approve and revoke certificates  
without giving them the permission to manage the CA.

**Lesson-2:**

**1. Certificate templates:**  
Certificate templates enable you to configure the properties of certificates that are issued by enterprise CAs. Certificate templates are stored in Active Directory and replicate throughout  
the forest.

2. What step do you need to take after revoking a certificate if you want clients to be aware of the certificate’s new status?  
**Ans.** You need to publish either a CRL or delta CRL.

■ Certificate template compatibility settings determine the minimum CA and certificate  
recipient that can be used with the certificate. The more stringent the requirement, the  
more options available on the template.  
■ Certificate revocation enables you to deem an existing certificate invalid. The Certificate Hold option is the only one that allows you to unrevoke a certificate.  
■ Certificate renewal properties determine the frequency at which the certificate is  
renewed. You can force renewal on certificates issued by enterprise CAs by reenrolling  
all certificate holders.

3. Certificate renewal:  
Automatic certificate renewal makes it possible for a certificate to be reissued with a new expiry date after a certain period of enrollment has expired. Automatic renewal ensures that certificates are updated and don’t expire because someone forgot to manually renew them.

**4. Autoenrollment:**  
Autoenrollment allows certificates to be automatically deployed to users, services, and computers from an enterprise CA without requiring the client requesting the certificate.

■ Autoenrollment allows certificates to be automatically requested and deployed.  
■ Autoenrollment must be enabled through permissions on the certificate template and  
through the Certificate Services Client – Auto-Enrollment policy.

■ You can configure private key recovery if a user has been enrolled in a key recovery agent certificate and the certificate template has been configured so that the private key is archived.

**Chapter-5: Backup and recovery**

Lesson-1:

1. What is Windows Server Backup?

Ans. Windows Server Backup enables you to back up and recover the following:

1. Full server (all volumes)
2. Specific volumes
3. Specific folders
4. Specific files
5. System State data

■ Windows Server Backup can write backups to a local disk, volume, or network share.  
■ Wbadmin.exe is the command-line version of Windows Server Backup. Windows Server  
2012 also includes more than 45 Windows PowerShell cmdlets for Windows Server Backup.

2. What is Windows Azure Backup?

Ans. Windows Azure Backup enables you to back up files and folders to Microsoft’s public Windows Azure cloud.

3. What are system restore points?

System restore points are a Windows 8 client technology that provides snapshots of a system’s configuration that are automatically taken prior to changes such as the installation of new software, updates, or drivers.  
■ Vssadmin enables you to manage volume shadow copy snapshots.

**Lesson-2:**

■ You can use Windows Server Backup to restore files, folders, and volumes other than the operating system volume.  
■ When restoring files, you can restore in the original or an alternative location. When restoring to the original location, you can choose to create copies of duplicate files, overwrite duplicate files, or not restore duplicate files.  
■ When restoring you have the option of applying the file permissions that existed on the restored items when they were backed up.  
  
■ You use Windows RE to perform bare metal recovery and operating system volume restore.  
■ You can restore files and folders from Windows Azure Backup.  
■ You can use BCDEdit command line utility to configure the boot configuration data store.

■ You can boot into Safe Mode when you need to access the operating system with a minimal set of drivers and services.

**Chapter-6: Advanced file services and Storage**

Lesson 1:

1. **What are Quotas?**

Ans. Quotas enable you to control the amount of storage space (data) consumed by a user on a volume, folder tree, or individual folder.

Or, Quotas enable you to limit the amount of data that can be written to a specific path.

1. **What is the different between a hard quota and a soft quota?**

Ans. The difference between a hard quota and a soft quota is as follows:  
■ A hard quota blocks users from exceeding the specified limit. They can’t write additional data to the folder tree to which the quota template applies.  
■ A soft quota doesn’t block users from exceeding the specified limit.

**Note:**

* In previous versions of the Windows server operating system, NTFS quotas enabled you to apply quotas on a per-volume basis.
* FSRM quotas are more sophisticated, enabling you to apply different quotas to different folder trees on the same volume.
* Quotas are path based, you can have different and separate quotas applied on the same volume.

1. **What are file screens?**

Ans. File screens enable you to block users from writing specific types of files, on the basis of the file name extension to volumes, folder trees, or individual folders.

You apply file screens to shared folders by applying them to the folder on the file server that is associated with the shared folder.

**Note:**

* You configure file screens by selecting a specific file group to the screen or by selecting a file screen template and applying it to a specific location.
* A file group is a collection of file types associated with a particular kind of file. For ex- ample, the Image Files file group includes the file extensions associated with common image file formats such as .bmp, .jpg, .gif, and .png.
* You can edit which file extensions are associated with existing file groups or create custom file groups.
* A file screen exception enables you to create an exemption to an existing file screen.

1. **You want to allow file types to be written to a subfolder that are blocked by a file screen applied to the folder. How can you accomplish this goal?**  
   **Ans.** Configure a file screen exception.
2. **What is File classification?**

Ans. File classification enables you to apply metadata to files based on file properties.

Note:

File classification properties can use one of the following property types:

* **Yes/no:** A Boolean value of either YES or NO. When multiple values apply, NO overrides YES.
* **Date-Time:** A date and time property.
* **Number:** A numeric property.
* **Multiple Choice List:** A list of values that can be assigned to a property. Multiple  
  values are allowed.
* **Ordered List:** A fixed list of values. If multiple values apply, the one closest to the top of the list is used.
* **String:** A text string that can be assigned to the property.
* **Multi-string:** A list of strings that can be assigned to a property.

1. What are file management tasks?

Ans. File management tasks enable you to perform tasks on files based on the file metadata.

1. What is report?

Ans. A Storage report enables you to generate information about the type and nature of files stored on a storage server. Storage reports give you the information that you need to configure effective file screens and quotas.

1. Server for NFS Data Store:

Ans: Server for NFS Data Storeallows clients that use the Network File System (NFS) protocol to access data stored on computers running Windows Server 2012. NFS is primarily used by UNIX and Linux clients, but it is also used by some third-party hypervisors.

Or, Server for NFS Data Store enables you to share files with clients that access files using the NFS protocol.

1. What is BranchCache?

Ans. BranchCache allows clients located in branch offices to cache shared files and website data retrieved from servers in remote offices either in a local peer cache or on a host cache.

BranchCache supports two configurations: **Hosted cache mode and Peer cache mode**

**File access auditing:** File access auditing enables you to track which users access specific files and folders and how those users access those files and folders.

**Lesson-2:**

1. **Define iSCSI target and iSCSI initiator.**

**Ans. iSCSI target:** The iSCSI target on Windows Server 2012 enables you to provide storage across the network to Windows computers through iSCSI initiators.  
**iSCSI initiator:** The iSCSI initiator component enables Windows clients and servers to connect to iSCSI targets.

■ The iSNS server role enables a computer running the Windows Server 2012 operating system to function as a repository for information about iSCSI targets and initiators.

**iSNS server:**  
The iSNS Serverrole enables you to centralize the discovery of iSCSI initiators and targets in an organization.

1. What is thin provisioning?

Ans. Thin provisioning enables you to create virtual disks by specifying a maximum size but where the virtual disks only consume storage in the storage pool equal to the data stored on the volumes hosted on the virtual disk.

Or, The volume uses space from the storage pool as needed up to the volume size.

■ Trim makes it possible for the operating system to reclaim space allocated to a virtual disk when data is deleted from the volumes hosted on the virtual disk.  
■ Features on Demand make it possible for you to configure Windows Server 2012 so that the payload files for roles and features are not stored on the computer.