Security filtering (ch8 managing gp)

- There are two types of GPO filtering
    - Security filtering
    - Windows Management Instrumentation WMI filtering
- Security Filtering
    - Uses permissions to restrict objects from accessing a GPO.
- WMI filtering
    - Uses queries to select a group of computers based on certain attributes, and then applies or doesn't apply policies based on the query's results

Stale resource record (ch10 Config Adv. DNS)

- Stale resource record – A DNS record that is no longer valid either because the resource is offline for an extended period or permanently or because the resource's name or address has changed.

DNS resolver

- Computer making a DNS query is called a DNS client or DNS resolver

DNS policy (ch10 Config Adv. DNS)

- Two primary types of policy
    - Query resolution policy – specifies how DNS queries are handled by the DNS server
    - Zone transfer policy –specifies whether a zone transfer is allowed
- DNS objects you can create and manage using PowerShell cmdlets include:
    - Client subnet
    - Zone scope – a subset of a zone where a zone can contain multiple zone scopes and each zone scope has its own set of resource records
    - Recursion scope – defines which queries will use DNS recursion

DNS naming hierarchy(root,sub-lvl,ect)

Global catalog (ch4 Introduction to AD)

- Global Catalog – Distributed data storage stored in Domain Controllers, used for faster searching of all objects in every domain.
- First DC installed in a forest is automatically designated as a global Catalog server but others can be configured. Functions
    - Facilitates Domain and forest-wide searches
    - Facilitates logon across domains – upn user principal name
    - Holds universal group membership information

Template accounts (ch5 Managing OUs and AD Accounts)

- User template is a user account that's copied to create users with common attributes
    - Create one template account for each department or O U
    - Disable the template account to eliminate security risks
    - Add an underscore or other special character to the beginning of a template account's name to make it easy to recognize

    - Fill in as many common attributes as you can so that after the account is created, less customizing is necessary

PTR records (ch9 Config DNS)

- PTR records are used to resolve a known IP address to a hostname.
- PTR records are found only in RLZs
- Have much of the same information as a host record.
    - When you create a host record you have the option to create the related PTR record for the host automatically

Built-in service account (ch6 User and Service Account Config)

- 3 built-in service accounts
    - Local service - intended for services and background applications that need few rights and privileges.
    - Network service - intended for services that need local and network access.
    - Local System - Use with caution, has more privileges than administrator.

Security principal (ch8 Managing group policies) (ch4) (ch5)

- Three types of security principals can be assigned permission to an object:
    - Users
    - Groups
    - Computers
- Foreign Security principals - contains user accounts from other domains added as members of local domain groups
- Groups are the main security principal used to grant rights and permission
- A computer account is a security principal with an SID and a password and must authenticate to the domain

Active directory partitions (ch4)

- Directory partitions are sections of the Active Directory database that holds varied types of data and are managed by different processes
- There are 5 directory partitions in Active Directory database
    - Domain directory partition – contains all objects in a domain including users, groups, computers, OUs.
    - Schema directory partition – Contains info needed to defines AD objects and object attributes.
    - Global Cataloq partition – Holds the global catalog which is a replica of all objects in the forest.
    - Application directory partition – used by applications and services to hold info that benefits from.
    - Configuration Partition – holds configuration information that can affects entire forest

Member server (ch1)

- **Member Server** is a windows server that is in the management scope of a domain but doesn't have AD.

GP Update (ch8)

- To update group policies use the gp update.exe command with the following options:
    - No options - the command's default behavior takes place
    - /force - all settings from all applicable G P O s are reapplied, even if unchanged
    - /wait: value - specifies the number of seconds the command should wait for policy processing to finish before returning to the command prompt
    - /logoff - the user is logged off after policy processing is finished
    - /boot - the computer restarts after policy processing is finished
    - /sync - causes synchronous processing during the next computer restart or user logon
    - /target: Computer or User - specify that you want only computer or user policy settings to be updated

SysVol (ch4,7)

- Folder which resides on each and every domain controller within the domain
- Contains the domains public files needed to be accessed by clients and kept synchronized between domain controllers
- Default location C:\\Windows\SYSVOL

Intra-site replication (ch4)

- **Intrasite replication** - replication between domain controllers in the same site. Intrasite replication occurs 15 seconds after a change is made on a domain controller with a 3-second delay between each replication partner.
- **Intersite replication** - occurs between two or more sites

FRS (File rep service)

- File Replication Service (FRS) - used when running in a mixed environment of differing Windows Server operating systems
- Distributed File System Replication (DFSR) - used when all DCs are running Windows Server 2008

Schema (ch4)

- Schema is information that defines the type, organization and structure of data stored in the active directory
- **Schema classes** – define the types of objects that can be stored in Active directory
- **Schema attributes** – Define type of information stored in each object.
- **Attribute value –** Information stored in each attribute.
  Schema master – Responsible for replicating the schema directory to all other DCs in the forest when changes occur

Group service account

- **Managed service account (MSA)** - enables administrators to manage rights and permissions for services but with automatic password management

- **Group managed service account (gMSA)** - provides the same functions as an MSA but can be managed across multiple servers.

GPO Inheritance

- GPO inheritance is enabled by default
- There are several ways to affect GPO inheritance:
    - Blocking inheritance
    - GPO enforcement

IANA - Internet assigned numbers authority

Post-Installation (ch2)

- Post-Installation configuration tasks include giving the server a name, configuring network protocols, setting time zone information, selecting a network model, and installing and configuring Windows Updates
    - Server roles can then be installed

GPO Scope (ch7)

- **GPO scope –** Defines which objects a GPO affects
- When AD is installed, two GPOs are created and linked to two containers:
    - Default Domain Policy - linked to the domain object and specifies default settings for all users and computers in the domain
    - Default Domain Controllers Policy - linked to the Domain Controllers O U and specifies default policy settings for all domain controllers in the domain

Publish (ch7)

- A software package can only be assigned to a computer, but there are two options for deploying software to users:
    - Published - isn't installed automatically; a link to install the application is available in Control Panel's Programs and Features
    - Assigned - can be installed automatically when the user logs on to a computer in the domain

GPO Linking (ch7)

- Creating and Linking – GPOs are created in the Group Policy management console and can be linked to one or more AD containers.
- Each domain object has a default GPO linked to it that affect all objects in the domain
- Password settings object (PSO) - enables an administrator to configure password settings for users or groups that are different from those defined in a GPO linked to the domain. Also called Fine-grained password policies.

Delegation for AD (ch4,5,6,8,9,10)

- **DNS Delegation –** Allows windows to create records on the DNS server for the new domain.
- **Delegation of control –** A person with higher security privileges assigns authority to a person of lesser privileges to perform certain tasks

- **Kerberos delegation –** a feature of the Kerberos authentication protocol that allows a server to impersonate a client. Relieving the client from having to authenticate to more than one service.
- Zone delegation – transferring authority for a subdomain to a new one

GPO Enforcement (ch8)

- GPO Enforcement
    - Forces inheritance of settings on all child objects in the GPO's scope, even if a GPO with conflicting settings is linked to a container at a deeper level
    - GPO that's enforced has the strongest precedence of all GPOs in its scope

System services

Stub zone (ch9,ch10 Config Adv. DNS)

- Stub zones are special type of zone that contain only an SOA record, one or more NS records and the necessary glue A records to resolve NS records.
- Reasons for using stub zones
    - Maintenance of zone delegation information
    - In lieu of conditional forwarders
    - Faster recursive queries
    - Distribution of zone information

Administrative templates (ch8,4)

- Administrative templates are collections of policy definition files in XML format referred to as ADMX files because of their .admx extension.
    - They specify Registry entries that should be controlled and the type of data the entries take
- **Administrative Template files** – XML-formatted text files that define policies in the administrative Templates folder in a GPO

Guest Account (ch5)

- Guest account is disabled by default after install, and must be enabled before it can be used for log on
- Guest account can have a blank password
- Should be renamed if it is to be used
- Guest account has limited access to a computer or domain, but does have access to any resource for which the Everyone group has permission

Types of DNS Servers

- DNS servers can perform one or more of the following roles
    - **Authoritative server** – Holds a complete copy of a zone's resource records.
    - **Forwarder** – DNS server to which other DNS servers send requests they can't resolve themselves.
    - **Conditional forwarder** – DNS server to which other DNS servers send requests targeted for a specific domain

- **Caching-only server –** Does not have zones and its job is to field DNS queries, do recursive lookups to root servers or send requests to forwarders and then cache the results.

Restricted groups (ch7)

- Restricted Groups policy - allows an administrator to control the membership of both domain groups and local groups on member computers
  - This node is empty by default and you configure it by adding groups you want to restrict

SOA Records (ch10 Config Adv. DNS)

- SOA records contain information about a zone including its serial number and a number of timers used for zone transfers.
- SOA records are found in every zone and contain information that identifies the server primarily responsible for the zone as well as some operation properties of the zone
- SOA record contains the following info
  - Serial number
  - Primary server
  - Responsible person
  - Minimum default TTL
  - Refresh interval
  - Retry interval
  - Expires after

C-name Canonical Name Records (ch9)

- CNAME record is an alias for another domain name record in the DNS database.
  - Used when multiple services are running on the same server and you want users to be able to refer to each service with a different name
- Can also create CNAME records that point to records in other domains

DNS Zone (Primary,Sec,Stub) (ch9,10)

- **Zone** is a grouping of DNS information that represents one or more domains and possibly sub-domains
- Zones contain a variety of record types called **resource records** which contain information about network resources.
- A zone can be a forward lookup zone or a reverse lookup zone
  - **Forward lookup zone (FLZ)** – Contains records that translate name to IP addresses such as A, AAAA and MX records.
  - **Reverse lookup zone RLZ** – Contains PTR records that may map IP addresses to names and is named after the IP address (IPV4 OR IPV6) of the computers whose records it contains.
- DNS databases consist of the following types:
  - **Primary zone** – contains a read/write master copy of all resource records for the zone; it's considered authoritative for the zone.
  - **Secondary zone** – contains a read only copy of all resource records for the zone, it is considered authoritative for the zone.

- **Stub zone**- contains a read only copy if the SOA start of authoritative and NS records for a zone and the necessary A records to resolve NS records, not authoritative.
-

Dynamic DNS (ch9)

- Dynamic DNS records are created and updated by the resource or by the DHCP server when an IP address is leased or renewed.
- Each time a dynamic record is created or updated a time-to-live TTL value and timestamp are added to the record.
  - TTL specifies how long the record should remain in the DNS database
  - If the record expires, its deleted from the database.

Fine-grained control (ch6)

- Password settings object (PSO) - enables an administrator to configure password settings for users or groups that are different from those defined in a GPO linked to the domain. Also called Fine-grained password policies.

Dynamic Updates(ch9)

- Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
- Dynamic updates can be configured in one of three ways
  - Allow only secure dynamic updates
  - Allow both nonsecure and secure dynamic updates
  - Do not allow dynamic updates.

The order that Group Policies (GP) are applied (ch7,4)

- Local computer
  - Site
    - Domain
      - Organizational unit

Different types of DNS query(ch9,10)

- Recursive query
- Iterative quesry
- Referral Query

Log on hours options(ch5)

Group type conversion

- There are two group types
  - Security
  - Distribution

- Group type can be changed from security to distribution and vice versa

- Only security groups can be added to a DACL (Discretionary access control list)
- If a security group is converted to a distribution group, the entry will remain in a DACL, but it has no effect on access to the resource
- Converting group types is not commonly done
    - Usually a distribution group is converted to a security group

GPO Administrative templates(ch7)

- **Administrative Template files** – XML-formatted text files that define policies in the administrative Templates folder in a GPO
- Administrative templates are collections of policy definition files in XML format referred to as ADMX files because of their .admx extension.
    - They specify Registry entries that should be controlled and the type of data the entries take.

Resource records(ch9)

- Zones contain a variety of record types called **resource records** which contain information about network resources.
- Resource records can be created dynamically or as static records
    - Dynamic records are created by the resource or with a DHCP server
    - Static records are created manually by an administrator or automatically by windows.

SRV records for AD(ch9)

Service Location (SRV) Records

- An SRV record specifies a hostname and port number for the servers that supply specific services.
- SRV records are critical to the operation of an Active Directory domain – without them client computers couldn't find a domain controller or global catalog server to log on or join a domain.
- SRV records for Active Directory are created automatically when Active Directory is installed

Built-in administrator accounts(ch5)

- The following guidelines apply to the built-in Administrator account:
    - Local administrator account has full access to all aspects of a computer, while domain administrator account has full access to all aspects of the domain
    - The domain administrator account in the forest root domain has full access to all aspects of the forest
    - Default Administrator account should be renamed and given a strong password
    - Administrator account should only be used while performing administrative operations

Administrator account can be renamed or disabled but not deleted - **TRUE**

Zone aging and scavenging(ch10)

- Scavenging is the process of scanning the records in each zone and deleting stale records.
- Enabling scavenging – It must be enabled in two places

    - On the server by right clicking the server icon in DNS manager, click properties, advanced tab, enable automatic scavenging of stale records
    - For specific zones
    - Parameters set at the zone level override those set at the server level.
- Scavenging process is set for 7 days by default.
- Zone data is replicated to all DNS server so scavenging needs to be enabled on only one server.
- Scavenging consumes server resources
    - Enabling it on a DNS server with a fairly light workload is best

GPO Scope(ch6,7)

- **GPO scope –** Defines which objects a GPO affects
- When AD is installed, two GPOs are created and linked to two containers:
    - Default Domain Policy - linked to the domain object and specifies default settings for all users and computers in the domain
    - Default Domain Controllers Policy - linked to the Domain Controllers OU and specifies default policy settings for all domain controllers in the domain

Reverse lookup zone(ch9)

- **Reverse lookup zone RLZ** – Contains PTR records that may map IP addresses to names and is named after the IP address (IPV4 OR IPV6) of the computers whose records it contains.

GPO Modeling wizard(ch8)

- Group Policy Results - a wizard built into the GPMC that creates a report to show which policy settings apply to a user, computer, or both

DNS Record(ch9)

- Dynamic DNS records are created and updated by the resource or by the DHCP server when an IP address is leased or renewed.
- Each time a dynamic record is created or updated a time-to-live TTL value and timestamp are added to the record.
    - TTL specifies how long the record should remain in the DNS database
    - If the record expires, its deleted from the database.
- Static DNS records do not expire and are created manually by an administrator.
- To create a static record in DNS Manager
    - Right click the zone and select the record type
    - In a FLZ most common type of record is the New Host Record
    - Enter name to create the FQDN automatically
    - If you select create associated point PTR record check box, a PTR record is created if a suitable RLZ exists for the IP address entered.

Operation Master Role(ch4)

- First domain controller in the forest takes role of the operations master.

- A number of operations in a forest require having a single domain controller, called the **operations master**, with sole responsibility for certain functions. In most cases, the first DC in the forest takes on the role of operations master.
- 5 operations master roles referred to as Flexible single master operations FSMO roles:
    - Schema master
    - Infrastructure master
    - Domain naming master
    - RID master relative identifier domain
    - PDC emulator master

DS Query(ch5)

DNS Security(ch10)

Domain Name System Security Extension (DNSSEC)

- A suite of features and protocols for validating DNS server response.
- 3 methods to ensure received data is secure include
    - Origin authentication of DNS data
    - Authenticated denial of existence
    - Data integrity
- Zone signing uses digital signatures in DNSSEC related resource records to verify DNS responses.
- Zones using DNSSEC have the following additional resource records
    - DNSKEY
    - RRSIG
    - NSEC/NSCE3
    - NSEC3PARAM
    - DS
- Zone signing uses public key cryptography, with two keys generated:
    - Key-signing key (KSK) – has a private and public key associated with it

Zone-signing key (ZSK) – a public and private key combination stored in a certificate used to sign the zone.

Command DC GPO Fix

Hot Add

Time to live(ch9)

- TTL specifies how long the record should remain in the DNS database

Remove DNS server role (ch2)

- **- Unistall-WindowsFeature DNS -Remove** DNS server role

GP Update (ch6)

Active Directory recycle bin (ch4)

- Active directory recycle bin is disabled by default and can be enabled in ADAC.
- After enabled, the Recycle Bin can't be disabled without reinstalling all domain controllers in the forest.

SAM Database

Windows stores and manages the local user and group accounts in a database file called Security Account Manager (SAM). It authenticates local user logons on local machines. SAM database resides in the Windows registry. On a domain controller, it simply stores the administrator account from the time it was a server, which serves as the Directory Services Restore Mode (DSRM) recovery account.

ADML file (ch7)

- Administrative templates are collections of policy definition files in XML format referred to as ADMX files because of their .admx extension.
    - They specify Registry entries that should be controlled and the type of data the entries take.

Clean Installation (ch2)

A **clean installation** is one in which the OS is installed on a new disk partition and isn't an upgrade from any previous version of Windows.

Registry Editor

The **Windows Registry Editor (regedit.msc)** is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry. Registry Editor is one of the few graphical utilities available in Server Core. Applications and the OS rely on its integrity.

Password Setting Object pso (ch6)

- A password settings object enables an administrator to configure password settings for users or groups that are different from those defined in a GPO linked to the domain.

GPO order applied (ch8)

The Policy Definition Directory

It's a folder named PolicyDefinitions on the SYSVOL share of a DC that makes sure all policy definitions are replicated to other DCs. Also located at ***%systemroot%*\PolicyDefinitions** folder. Used to add custom administrative templates to group policy.

Zone Replication (ch10)

- Zone replication is the transfer of zone changes from one DNS server to another.
- For a standard zone, zone replication is called zone transfer
- Active directory-integrated zones have the following advantages over a standard zone
    - Automatic zone replication
    - Multimaster replication and update

- Secure updates
- Use permissions to restrict which users can modify zone data
- Efficient replication

DSRM (ch4)

Directory Services Restore Mode DSRM – A boot mode used to perform restore operations on active directory if it becomes corrupted or parts are deleted accidentally.

Command to rename PC

netdom renamecomputer *currentname* /newname:*newname*

Trust relationship (ch4)

- Defines whether and how security principals from one domain can access network resources in another domain
- Established automatically betn all domains in the forest.

Trust do not equal permissions – Permissions are still required to access resources.

Feature on Demand (ch2)

- Feature on Demand enables you to remove Windows feature installation files from the local disk

Makes it possible to save disk space and allows Windows Update to run faster

Account Lockout policy

Account Lockout Policy – Contains 3 policies that control user account lockout. If a user account is locked, the user can't sign in until the account is unlocked.

- **Account lockout duration**: How long is the user locked out, and unable to sign in. Suggested value of 30 minutes. Value of 0 means account remains locked forever, until admin unlocks it.
- **Account lockout threshold**: How many times can a user's password be entered incorrectly before lockout starts. Default is 0, which means accounts are never locked. Value between 0 and 999
- **Reset account lockout counter after**: umber of minutes that must elapse between failed logon attempts before the failed logon attempt counter is reset to 0. Default is Not defined, while suggested value is 30 minutes.

User template (ch5)

A user account that's copied to create users with common attributes. You can copy many user account attributes in this template to accounts you're creating, except for name, logon name, password

Service User Account

User account that Windows services use to log on to a computer or domain with a specific set of rights and permissions. A service needs to log on with a service account if it runs in the background because a user doesn't start it. **Three** built-in service accounts, each with its own rights and permissions.

- *Local Service* – Primarily for services that run in the background and require few rights/privileges

- *Network Service* – Primarily for services that need network access.
- *Local System* – Use with caution, has more privileges than administrator.

Script (ch7,4,5)

- A script is a series of commands saved in a text file to be repeated easily at any time.

SOA(ch9)

SOA records are found in every zone and contain information that identifies the server primarily responsible for the zone as well as some operation properties of the zone

GPO Filtering (ch8)

- GPO filtering – A method to alter the normal scope of a GPO and exclude certain objects being affected by its settings.
- 2 types of GPO filtering
    - Security filtering
    - Windows Management Instrumentation WMI filtering
- Security Filtering
    - Uses permissions to restrict objects from accessing a GPO.
- WMI filtering
    - Uses queries to select a group of computers based on certain attributes, and then applies or doesn't apply policies based on the query's results

Users Profile (ch5,7)

Refresh interval (ch9)

- Refresh Interval – Species how often a secondary DNS server attempts to renew its zone information
- Retry interval – Amount of time a secondary server waits before retrying a zone transfer that has failed.
- Expires after – Amount of time before a secondary server considers its zone data obsolete if it can't contact the primary DNS server.

Host file

Hosts file is an operating system file that maps hostnames to IP addresses. Located %SystemRoot%\System32\drivers\etc\hosts

Processing of GP

- Group policy processing can be synchronous or asynchronous.

Synchronous processing

- **Synchronous processing** - forces group policy processing to finish before other system tasks can be performed
    - Computer Configuration polices are processed during system boot and user logon prompt isn't displayed until all processing is finished.
- **Asynchronous processing** - allows displaying the user logon prompt while Computer Configuration policies are still being processed

Command to invoke GP update

gpupdate

RO DC

DNS Forwarder

- Referring a DNS query to a forwarder can be more efficient under the following conditions
    - When the DNS server address for the target domain is known
    - When only one DNS server in a network should make external queries
    - When a forest trust is created
    - When the target domain is external to the network and an external DNS server's address is known
- Conditional forwarding allows queries for particular domains to particular name servers and all other unresolved queries to a different server.
- Conditional forwarders are configured in the conditional forwarders node in the DNS Manager
- With forwarders and or conditional forwarders configured the DNS server attempts to resolve DNS queries in this order
    - From locally store zone resource records
    - From the DNS cache
    - From the conditional forwarders
    - From the traditional forwarders
    - Recursively by using root hints

DFSR

- Distributed File System Replication (DFSR) - used when all DCs are running Windows Server 2008

KERBEROS

- Kerberos is the authentication protocol used in a Windows domain environment to authenticate logons and grant accounts access to domain resources.
- Kerberos provides mutual authentication between a client and server or between two servers - Means the identity of both parties is verified
- Kerberos uses shared key encryption to ensure privacy and passwords are never sent across the network.

Directory services

- A directory service is a database that stores network resource information and can be used to manage users, computers, and resources throughout the network.
- Directory services provides a centralized management tool. Users use it to find resources

DNS Record Types:

- A (Host address) – Computer name & ipv4 addres
- AAAA (IPv6 host address)
- CNAME (Canonical name for an alias) – i.e. create cname record to make www. & ftp. Point to the same A record (host)

- MX (Mail exchange) – Address of email server for the domain.
- NS (Name Server) - FQDN of a name server that has authority over the domain. NS records are used by DNS servers to refer queries to another server that's authoritative for the requested domain.
- PTR (Pointer) - Used for reverse DNS lookups, resolve a known IP address to a hostname.
- SOA (Start of Authority) - Informational record, an SOA identifies the name server that's authoritative for the domain
- SRV (location of service) - specifies a hostname and port number for servers that supply specific services.