A CLOUD GURU
A PLURALSIGHT COMPANY

AZ-800: Administering Windows Server Hybrid Core Infrastructure

Wayne Hoggett
TRAINING ARCHITECT

Introduction

KEY CONCEPTS

- Use Datacenter Edition if you require unlimited virtual machines or containers. Also use Datacenter Edition for unlimited Storage Replica.
- Use Datacenter: Azure Edition if you require Azure Extended Network or Hotpatch support.
- Use the Server Core installation option to improve the availability and security of your servers, unless you have a reason not to use it.
- Ensure you complete the initial configuration of your server to avoid future downtime.
- The Windows Server Nano image is available for containerized workloads, including support for .NET Core.

KEY TERMS

Server App Compatibility Features on Demand (FOD)

Improves the compatibility of the core installation option with more roles, features, and applications.

Remote Server Administration Tools (RSAT)

Enables management of Windows Server roles and features from a Windows PC or Server.

Role and Features

Roles are a server's purpose, whereas features are additional Windows capabilities that can improve the functionality of the server or improve application support.

Preparing for Active Directory Domain Services

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Conditional forwarders are used to forward requests for a specific domain.
- Server forwarders are used to forward all unknown requests to another DNS server.
- DNSSEC allows you to sign a DNS zone on an authoritative DNS server and allow other DNS servers to validate the responses.
- Trust anchors (or trust points) must be distributed to the recursive DNS server.
- Name Resolution Policy Table (NRPT) rules can be configured on the client to enforce DNSSEC.

KEY TERMS

A/AAAA Record

Maps an FQDN to an IP address.

NS Record

Stores the IP address of all the servers that store the zone.

CNAME

Also referred to as an alias record. Maps an FQDN to another FQDN.

SRV Record

Stores IP address and port information for servers that host services in the domain.

Implementing Active Directory Domain Services: Part 1

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Domain controllers store the Active Directory database and provide authentication.
- Active Directory domains exist within a forest, and a forest can have more than one domain.
- A DNS zone hosts resource records for a domain. DNS zones can be either forward or reverse lookups.
- A primary DNS zone is a read-write copy of a zone, whereas secondary zones are a read-only copy of the zone.

KEY TERMS

Forest

A forest is an Active Directory Domain Services security and configuration boundary.

Domain

A domain is an administrative unit with an Active Directory Domain Services forest.

Domain Controller

Domain controllers authenticate users and computers, host the Active Directory database, and distribute settings to domain-joined computers.

KEY COMMANDS

You can create a custom application partition for DNS with either the `ntdsutil` or `dnscmd` command-line tools.

Implementing Active Directory Domain Services: Part 2

KEY CONCEPTS

- An Active Directory forest is made up of one or more domain trees.
- An Active Directory forest is a security boundary. All domains in the forest trust each other.
- An Active Directory forest is also a replication boundary. The schema and global catalog are shared within the forest.
- The schema is the definition of the objects and properties that can be assigned to an object within the forest.
- The global catalog is a reference of every object in the forest. It's used to locate objects within the forest.
- A domain is a replication boundary and an administrative unit within a forest.
- You must be a member of the Enterprise Admins Group to add a new domain to an existing forest.
- Domain controllers provide authentication and authorization within a domain.
- Domain controllers update, store, and replicate the Active Directory database.
- A domain join can be performed offline or online. Offline is useful where connectivity is an issue or speed is important.

Implementing Active Directory Domain Services: Part 3

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Deploy multiple domain controllers to improve performance and availability of Active Directory Domain Services.
- Membership of the Domain Admins or Enterprise Admins group is required to promote a domain controller in an existing forest.
- Install from media (IFM) can be used to reduce replication traffic when deploying a domain controller.
- To create media, you must log on interactively to a domain controller and use the command-line tool: `ntdsutil`.

KEY TERMS

SYSVOL

The System Volume or SYSVOL is a public directory that is shared with all domain computers and users.

Active Directory Site

An Active Directory Site is a representation of a physical location.

Site Link

Replication between sites is performed over a Site Link.

KEY COMMANDS

`ntdsutil` can be used to create an IFM with the `ntdsutil ifm` command.

The command-line tool `Djoin` is used to perform an offline join.

Implementing Active Directory Domain Services: Part 4

KEY CONCEPTS

- The Active Directory database is split into partitions. The default partitions are configuration, schema, and domain.
- The configuration and schema partitions are replicated to all domain controllers in the forest.
- The domain partition is replicated to all domain controllers in a domain.
- Custom application partitions can be created and configured to replicate as required. DNS is an example of an application partition.
- Active Directory sites are used to control replication and help clients locate services close to them.
- Sites are defined by the subnets and domain controllers that exist at the site.
- Replication between sites occurs once over a site link between 2 bridgehead servers.
- Read-Only Domain Controllers (RODCsR) can be used to control the replication of privileged credentials to the domain controller.
- Installation and administration of an RODC can be delegated to a non-privileged user account.
- There are 2 steps in the deployment of an RODC. First the account is staged, and then the domain controller account is attached.

Implementing Active Directory Domain Services: Part 5

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- There are 2 forest operations masters. They are the schema master and domain naming master.
- The schema master is required when updating the schema. The domain naming master is required when adding domains or directory partitions.
- There are 3 domain operations masters: RID master, infrastructure master, and PDC emulator.
- The PDC emulator is the most critical of the domain-level operations masters.
- You can transfer or forcefully seize operations masters roles to move them between domain controllers.

KEY TERMS

Schema Master

Forest-level operations master. Used to introduce schema changes.

Domain Naming Master

Forest-level operations master. Required to add or remove domains.

RID Master

Domain-level operations master. Allocates Relative Identifier (RID) pools to new and existing domain controllers.

Infrastructure Master

Domain-level operations master. Updates cross-domain references from the global catalog.

PDC Emulator

Domain-level operations master. Receives updates when passwords are changed for users and computers.

Implementing Active Directory Domain Services: Part 6

KEY CONCEPTS

- Trust relationships enable access to resources across domains and forests.
- Trusts can be created either in one direction or both directions. The trust direction is the opposite of the direction of access.
- Trusts can be either transitive or non-transitive. Transitive trusts allow access where a direct trust does not exist.
- Authentication can be either selective or forest-wide. Use selective authentication to provide granular control over who can access resources using the trust.
- There are 4 trust types: forest, external, realm, and shortcut.

KEY TERMS

Forest Trust

Used to provide access between 2 forests.

External Trust

Used to provide access between 2 domains in separate forests where no forest trust exists.

Shortcut Trust

Used to reduce authentication time between 2 non-adjacent domains in the same forest.

Managing Active Directory Domain Services (AD DS) Security Principals: Part 1

Group Nesting

Accounts → **G**lobal → **U**niversal → **D**omain **L**ocal → **P**ermissions

KEY CONCEPTS

- User accounts represent a person in the Active Directory database.
- User accounts are used in authentication and authorization with a domain controller.
- There are 2 group types: security groups and distribution groups.
- There are 4 group scopes: local, domain local, global, and universal.
- The Active Directory Recycle Bin can be used to completely restore deleted Active Directory users and groups.
- The Active Directory Administrative Center and Windows PowerShell provide the latest functionality, including support for the Active Directory Recycle Bin.

KEY COMMANDS

```
Enable-ADOptionalFeature -Identity 'Recycle Bin Feature'
```

Managing Active Directory Domain Services (AD DS) Security Principals: Part 2

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Virtual Accounts are configured per server and provide access to the network using the computer account.
- Managed Service Accounts are configured in Active Directory for each application on a server.
- Group Managed Service Accounts are configured in Active Directory and can be shared between servers.
- Domain controllers require a Key Distribution Service root key to create gMSA passwords.
- Create a KDS root key using the **Add-KdsRootKey** PowerShell cmdlet.

KEY COMMANDS

```
Add-KdsRootKey -EffectiveImmediately
```

```
New-ADServiceAccount -Name 'BNE Web Farm'
-PrincipalsAllowedToRetrieveManagedPassword CORP-BNE-
WEB01, CORP-BNE-WEB02
```

```
Install-ADServiceAccount -Name 'BNE Web Farm'
```

Modernizing with Hybrid Identity: Part 1

KEY CONCEPTS

- Azure Active Directory is a cloud-based identity service designed to work with cloud applications using modern authentication.
- Azure AD Connect sync or Azure AD Connect cloud sync can be used to synchronize AD DS and Azure AD.
- Providing single sign-on requires either password hash sync, Pass-through Authentication, or federation to be implemented.
- Passwords, groups, and devices can be written back to AD DS. Security group writeback is not supported.
- Azure AD Connect sync can be deployed to support multiple forests and a single Azure AD tenant.
- A staging server can be used to provide disaster recovery for Azure AD Connect sync.
- You must configure and verify a domain in Azure AD and create a matching UPN suffix in AD DS.
- IDFix can be used to find and resolve issues with AD DS identities prior to synchronization.
- Azure AD Connect sync can be deployed using the express or custom installation option.

Modernizing with Hybrid Identity: Part 2

KEY CONCEPTS

- Azure AD Connect cloud sync is a new offering from Microsoft used to synchronize hybrid identities.
- Cloud sync provides high availability and can support multiple disconnected AD DS forests.
- Cloud sync cannot be used with Pass-through Authentication and does not provide group or device writeback.
- Cloud sync cannot be used with Azure AD Domain Services.
- Choose password hash sync (PHS) if you want business continuity, leaked credential reports, or smart password lockout.
- Choose Pass-through Authentication (PTA) if you want to enforce AD DS account restrictions.
- Choose federation if you need support for on-premises multi-factor authentication (MFA).
- Use Azure AD Connect Health to monitor your hybrid identity infrastructure.

Exploring Hybrid Networking Foundations: Part 1

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- A route-based VPN gateway can be used to configure multi-site and point-to-site connectivity to Azure virtual networks.
- ExpressRoute private peering can be used to configure private connectivity to an Azure Virtual Network.
- Azure Virtual WAN can be used to configure multi-site, point-to-site, and ExpressRoute connections.
- Virtual networks can be secured by network security groups, Azure Firewall, or Network Virtual Appliances (NVAs).
- Network Address Translation (NAT) can be used with VPN gateway and Azure Virtual WAN to resolve IP address overlap issues.
- Azure Public DNS zones provide name resolution for internet-facing DNS domains.
- Azure Private DNS zones provide registration and name resolution for VMs within a virtual network.
- Enable autoregistration so virtual machines automatically register their DNS records with a linked private DNS zone.
- Autoregistration can only be enabled in one private DNS zone per VNet.
- Reverse lookups can be performed within a VNet.

AZ-800: ADMINISTERING WINDOWS SERVER HYBRID CORE INFRASTRUCTURE

Exploring Hybrid Networking Foundations: Part 2

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Azure Private Link provides private connectivity to Azure platform-as-a-service offerings.
- Integrate Azure Private Link with private DNS zones to simplify the management of associated resource records.
- Deploy a DNS forwarder virtual machine in Azure to forward requests from on-premises networks to the Azure DNS resolver.
- Implement split-horizon DNS using an Azure public and private DNS zone with the same domain name.
- Use IPConfig, NSLookup, and PowerShell to troubleshoot DNS.

KEY COMMANDS

```
IPConfig /displaydns
Get-DNSClientCache
```

```
IPConfig /flushdns
Clear-DNSClientCache
```

```
IPConfig /registerdns
Register-DNSClient
```

```
NSLookup www.rivercityai.com
Resolve-DNSName www.rivercityAI.com
```

Deploying and Managing Azure Virtual Machines

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Use the Standard VM Tier for production VMs.
- Use Generation 2 VMs for larger VM operating system disks, more memory, and advanced security features.
- Use a VM size marked with the **s** additive feature to have access to Premium Storage.
- Always generalize a VM using `sysprep` before capturing the VM as an image.
- A VM must be restarted to change the VM size.
- You can add data disks to a running VM, but you must detach a disk to modify it.
- Use route tables to control VM traffic flow and network security groups to allow or deny network traffic.
- Azure Bastion requires a special subnet named AzureBastionSubnet with a /27 subnet.
- Serial Console requires a custom diagnostic storage account and Contributor role.

AZ-800: ADMINISTERING WINDOWS SERVER HYBRID CORE INFRASTRUCTURE

Deploying Active Directory Domain Services on Azure: Part 1

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Active Directory Domain Services provides Kerberos and NTLM authentication and LDAP functionality that is not provided by Azure AD.
- Azure AD Domain Services is limited to one managed domain per Azure AD tenant.
- Synchronization to Azure AD Domain Services is one-way from Azure AD to the managed domain.
- Passwords cannot be changed in Azure AD Domain Services.
- Active Directory Domain Services on virtual machines require network connectivity between on-premises and Azure.
- Choose a unique, routable domain name containing less than 15 characters.
- Network connectivity is required when using an Azure AD DS resource forest.
- Choose a non-standard SKU for resource forests.
- Password hash sync is required for AD DS users when using an Azure AD DS user forest.
- Azure AD Connect cloud sync does not support Azure AD DS.

Deploying Active Directory Domain Services on Azure: Part 2

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Azure AD Domain Join provides secure login and authorization using Azure RBAC.
- To connect to an Azure AD-joined VM, you need either the Virtual Machine Administrator Login or Virtual Machine User Login role.
- To join an Azure VM to a managed Azure AD DS domain, you must have network connectivity and DNS configured.
- You can join an Azure VM to a managed domain using the `Set-AzVMAdDomainExtension` PowerShell cmdlet.
- Configure Active Directory sites to match your network topology.
- You must have the Domain Services Contributor role or a more privileged role assigned to manage Azure AD DS resources.
- Your Azure AD user account must be a member of the AAD DC Administrators group to manage the Azure AD DS managed domain.
- Azure AD DS must be managed from an Azure AD DS domain-joined VM.
- Use a static IP address for your domain controller and do not assign a public IP address.
- Ensure the disk caching option for the Active Directory database and SYSVOL is set to None.
- Do not shut down domain controllers from the Azure portal. Instead, shut down using the VM operating system.

Configuring Group Policy: Part 1

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Group Policy is used to centrally administer Active Directory users and domain-joined computers.
- Group Policy cannot be applied to groups.
- Do not modify built-in Group Policy Objects.
- Computer settings take precedence over user settings.
- Use the Group Policy Management Console (GPMC) or Windows PowerShell to manage Group Policy in an Active Directory domain.
- Use the `GPUPDATE` command-line tool to trigger a Group Policy refresh.
- The Group Policy processing order is local, site, domain, organizational units.
- Group Policy links with a lower link order to override those with a higher link order.
- Block inheritance prevents GPO settings from higher-level GPOs applying below the block.
- Settings in enforced GPO links always take precedence.

Configuring Group Policy: Part 2

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Security filtering enables you to filter Group Policy Objects to allow access to apply the policy to specific groups.
- WMI filters enable you to filter Group Policy Objects to computers or users that match a WMI query.
- With loopback processing, user configuration settings in GPOs that apply to the computer are applied to every user logging on to that computer.
- Create a PolicyDefinitions folder on SYSVOL to create a Group Policy Central Store.
- Copy additional administrative templates to the central store to extend Group Policy functionality.
- All ADMX and ADML files must be copied from a client when configuring a central store.
- Group Policy settings take precedence over preferences.
- Membership to the Azure AAD DC Administrators group is required to manage Group Policy in Azure AD DS.
- You cannot modify Default Domain or Default Domain Controllers Policy in Azure AD DS.
- Create fine-grained password policies to override the default password policy in Azure AD DS.

Managing Windows Server: Part 1

KEY CONCEPTS

- PowerShell remoting enables you to execute PowerShell commands against remote computers using WinRM and WSMan.
- Enable PowerShell remoting using the `Enable-PSRemoting` cmdlet.
- Enter an interactive remote PowerShell session with the `Enter-PSSession` cmdlet.
- Create a remote PowerShell session with the `New-PSSession` cmdlet.
- Use `Invoke-Command` to execute commands against remote computers with or without a persistent session.
- The principle of least privilege restricts permissions to those required for a task or role.
- Just Enough Administration (JEA) allows you to implement the principle of least privilege with PowerShell remoting.
- Create a role capability file with `New-PSRoleCapabilityFile` to define what can be done in a JEA session.
- Create a session configuration file with `New-PSSessionConfigurationFile` to define who can use the defined roles.
- Register session configurations with `Register-PSSessionConfiguration`.

Managing Windows Server: Part 2

KEY CONCEPTS

- You can solve the second hop problem using CredSSP, which caches credentials.
- You can enable CredSSP using the `Enable-WSManCredSSP` PowerShell cmdlet on both the client and server.
- You can also solve the second hop problem with Kerberos delegation.
- Kerberos constrained delegation is configured on the intermediate server Active Directory computer object.
- Resource-based constrained delegation is configured on the resource server Active Directory computer object.
- Windows Admin Center complements existing management tools with web-based management.
- Windows Admin Center requires remote management, Kerberos delegation, and WMF 5.1.
- Deploy the Windows Admin Center extension to manage Windows Virtual Machines directly from the Azure portal.
- Deploy Windows Admin Center on-premises or in Azure and manage Windows computers anywhere there is network connectivity.
- Register Windows Admin Center with Azure to unlock a range of Azure hybrid services.

Managing Windows Server: Part 3

KEY CONCEPTS

- Azure Arc extends Azure management capabilities outside of the Azure public cloud.
- To onboard Azure Arc Connected Machines, you require the Azure Connected Machine Onboarding role.
- To modify connected machines, the Azure Connected Machine Resource Administrator role is required.
- Use a service principal to onboard multiple servers.
- Enable additional Azure functionality by installing extensions on Azure Arc Connected Machines.
- Collect metrics and logs in a Log Analytics workspace by deploying a monitoring agent.
- Use Azure Monitor insights to get a guided monitoring and troubleshooting experience for your resources.
- Microsoft Defender for Servers provides advanced security protection for your servers.
- Azure Sentinel can be linked to a Log Analytics workspace to provide threat intelligence, detection, and investigation.

Configuring and Automating Windows Server: Part 1

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Azure Automation provides update management, process automation, and configuration management capabilities.
- Update Management enables you to deploy software updates to your virtual machines and report on compliance.
- Process automation enables you to automate hybrid processes using runbooks.
- Configuration management enables you to configure, inventory, and track changes in your hybrid environment.
- Link a Log Analytics workspace to your Automation account to enable configuration management and update management solutions.
- PowerShell runbooks can be text based or graphical and use either Windows PowerShell or Python.
- You need to publish your runbook before you can run it.
- You can execute runbooks in Azure using the sandbox or on hybrid workers.
- Executed runbooks create jobs that store details of the runbook execution.
- Create user hybrid worker groups to distribute jobs between multiple hybrid workers.

Configuring and Automating Windows Server: Part 2

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- A configuration is made up of nodes, the resources to be configured on those nodes, and the properties of those resources.
- You import resources into your configuration using the `Import-DscResource` PowerShell cmdlet.
- Use `DependsOn` to control the order that resources in a configuration are applied in.
- The `node` block in a configuration declares which servers you want the configuration to apply to.
- An Azure Automation account is responsible for compiling the configuration.
- An Azure Automation account acts as a Desired State Configuration Pull Server.
- The Local Configuration Manager (LCM) is responsible for pulling, applying, and reporting the compliance of a configuration.
- Use the `Update-DscConfiguration` cmdlet to manually pull a configuration from the Automation account.
- Use the `Start-DscConfiguration` cmdlet to manually apply configuration.
- The configuration mode of the LCM determines how configuration is applied.

Configuring and Automating Windows Server: Part 3

KEY CONCEPTS

- Automatic VM guest patching can provide simple update management automation.
- Update Management provides a greater level of control over patch management and supports hybrid management.
- Azure VMs require the Log Analytics agent and Update Management solution.
- On-premises servers require the Log Analytics agent, Update Management solution, and ideally are onboarded into Azure Arc.
- Deployment schedules are configured to automatically deploy updates.
- Azure Policy helps ensure compliance by auditing and remediating compliance issues.
- Policies can be bundled together into policy initiatives.
- Guest configuration allows you to extend Azure Policy to manage operating systems and software.
- Azure Arc extends guest configuration to servers on-premises and in other clouds.
- Custom guest policies can be created to apply settings using Desired State Configuration.

Managing Hyper-V Virtual Machines: Part 1

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Install Hyper-V role on Server Core where possible.
- Manage Hyper-V with Hyper-V Manager, PowerShell, and Windows Admin Center.
- Use generation 2 VMs for improved security features like secure boot.
- Use the core hypervisor scheduler to improve the security posture of your VMs.
- Use VHD Sets to share disks between virtual machines.
- Use differencing disks or dynamically expanding disks to conserve disk space.
- Use production checkpoints to ensure an application consistency for your checkpoints.
- Use host and guest clusters to improve the availability of your virtual machines.
- Use Hyper-V Replica to replicate a virtual machine between 2 Hyper-V hosts.

Managing Hyper-V Virtual Machines: Part 2

KEY CONCEPTS

- Virtual network adapters provide network connectivity for your Hyper-V virtual machines.
- Virtual adapters connect to virtual switches to provide connectivity between VMs, the Hyper-V host, and physical network.
- Use an external virtual switch to VM connectivity to the physical network.
- Use Switch Embedded Teaming (SET) to combine network adapters for performance and availability.

KEY TERMS

Private Virtual Switch

Provides connectivity between each of the VMs on a Hyper-V host.

Internal Virtual Switch

Provides connectivity between the VMs and the Hyper-V host they are running on.

External Virtual Switch

Provides connectivity between the VMs, Hyper-V, and the physical network.

Managing Hyper-V Virtual Machines: Part 3

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Upgrade a VM version using the `Update-VMVersion` PowerShell cmdlet.
- Hyper-V uses integration services to enhance the performance and usability of the guest virtual machines.
- Hyper-V Dynamic Memory improves VM consolidation by dynamically allocating memory to guest VMs.
- Use enhanced session mode when connecting to VMs to improve the usability and security.
- PowerShell Direct provides connectivity to the guest operating system using PowerShell from the Hyper-V host.
- Nested virtualization enables you to run Hyper-V within a guest virtual machine.
- Run the `Set-VMProcessor` cmdlet to enable nested virtualization for a VM.
- Use an internal virtual switch and the `New-NetNat` PowerShell cmdlet to provide external network access for nested VMs.

Deploying and Managing Windows Containers

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- A containerized application is stored in a container **image** in a container **registry**.
- A `Dockerfile` contains the instructions to create your container image and which command to run when your container starts.
- Running your containers directly on the container host as an isolated process is referred to as **process isolation**.
- Running your containers in a lightweight virtual machine on the container host is referred to as **Hyper-V isolation**.
- The 5 container networking drivers are: NAT, transparent, overlay, Layer 2 bridge, and Layer 2 tunnel.
- The `docker build` command is used to create a container image from a `Dockerfile`.
- In a `Dockerfile`, the `FROM` instruction sets the base image for your container.
- In a `Dockerfile`, the `CMD` and `ENTRYPOINT` instructions set the default executable for your container.
- Use Windows Admin Center to manage container instances and images on your Windows container hosts.

Managing IP Addressing On-Premises: Part 1

KEY CONCEPTS

- DHCP servers lease IP addresses to DHCP clients.
- DHCP servers also provide DHCP configuration options like DNS server and gateway (router) IP addresses.
- A DHCP server must be authorized to lease IP addresses in an Active Directory domain.
- A DHCP relay can be used to forward DHCP discovery requests to DHCP servers in a separate subnet.
- Configure DHCP scopes with 2 servers using DHCP failover to provide high availability.
- Use `Add-DhcpServerSecurityGroup` cmdlet to create DHCP Administrators and DHCP Users groups.
- DHCP server options apply to all scopes on the server. DHCP scope options are scope specific. Class options are more device specific.
- Use reservations to ensure a device is leased a specific address.
- Use exclusions to prevent IP addresses from being leased.
- To update the subnet mask for a scope and allocate more addresses, delete and recreate the scope.

Managing IP Addressing On-Premises: Part 2

KEY CONCEPTS

- An IPAM server discovers and stores IP address and server management data.
- The IPAM client is part of Server Manager and is used to manage IPAM.
- IPAM can use either the Windows Internal Database or a SQL Server database.
- IPAM RBAC has 3 main components. Roles and scopes are combined in access policies.
- Use the `Invoke-IpamGpoProvisioning` cmdlet to create the configuration GPOs to automatically configure your discovered servers.
- Security filtering is used to apply Group Policy settings to servers managed by IPAM.
- Permissions are assigned to the IPAM server using a group in Active Directory.

Providing Hybrid Network Connectivity: Part 1

KEY CONCEPTS

- DirectAccess provides transparent, always-on connectivity for domain-joined Windows computers.
- The Windows Server Remote Access role can provide VPN, routing, NAT, and Web Application Proxy services.
- RADIUS servers are used to centrally authorize and authenticate network access.
- Network Policy Server (NPS) is Microsoft's implementation of a RADIUS server.
- NPS network policies are used to authenticate and authorize network access.
- Connection request policies determine which RADIUS server(s) should process authentication requests.
- Network policies determine who can connect and under what conditions they can connect.

Providing Hybrid Network Connectivity: Part 2

KEY CONCEPTS

- Web Application Proxy provides remote access to on-premises web applications.
- Web Application Proxy requires Active Directory Federation Services.
- Kerberos delegation is used to access web-based apps that use integrated Windows authentication.
- Azure AD Application Proxy provides simple and secure remote access to on-premises applications.
- Azure AD Application Proxy requires Azure AD Premium.
- Kerberos delegation is used to access web-based apps that use integrated Windows authentication.

Providing Hybrid Network Connectivity: Part 3

KEY CONCEPTS

- Azure Relay allows you to expose on-premises services to applications running in the cloud.
- Use Windows Communication Foundation (WCF) Relays for legacy .NET Framework and WCF applications.
- Use Hybrid Connections for all other application types.
- The relay service contains a namespace and connections and controls access with shared access policies.
- Azure Network Adapter enables you to connect individual Windows servers to an Azure Virtual Network.
- Extended network for Azure allows you to migrate a server to Azure and retain its private IP address.
- Both Azure Network Adapter and extended network for Azure are deployed using Windows Admin Center.
- Extended network for Azure uses 2 virtual appliances deployed as nested VMs on Hyper VMs.

Configuring and Managing Windows Server Storage: Part 1

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- SATA and SAS are considered to be direct attached storage.
- SCSI, iSCSI, and FC are considered to be shared storage.
- You should use the GPT partition style for all modern computers.
- You should use **simple** volumes on **basic** disks wherever possible.
- The NTFS file system is required for a range of Windows Server features.
- Storage Spaces allow you to pool together a variety of inexpensive disks to provide resilient storage.
- Storage Spaces require direct attached disks using SAS or SATA.
- Storage Spaces virtual disks support 3 storage layouts: simple, mirror, and parity.
- Two tiers are available to improve performance.
- Two provisioning types are available: thin and fixed.

Configuring and Managing Windows Server Storage: Part 2

KEY CONCEPTS

- File shares are accessed over the network using the UNC path.
- Share names that end with a $ character are hidden.
- To avoid managing both share and NTFS permissions, set share permissions to Full Control and use NTFS permissions.
- Avoid using **deny** when configuring NTFS permissions as deny permissions override all other permissions.
- Use SMB 3.0 and later for improved performance and security.
- File Server Resource Manager (FSRM) assists with managing Windows file servers.
- FSRM requires an NTFS-formatted volume.
- Quota management can be used to ensure storage space is not excessively used.
- File screens can be used to ensure only appropriate file types are uploaded to file servers.

Configuring and Managing Windows Server Storage: Part 3

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- DFS enables the replication of file shares and the publishing of file shares using a single name.
- DFS namespaces can be either domain based or stand alone.
- DFS replication can be configured as either a hub and spoke or full mesh topology.
- Storage Spaces Direct pools together storage on separate servers.
- Storage Replica performs one-way replication.
- Storage Replica can only have a primary and secondary replica.
- Choose synchronous replication to avoid data loss when using Storage Replica.
- Use the stretched cluster Storage Replica deployment option to limit downtime during a failure.

Configuring and Managing Windows Server Storage: Part 4

A CLOUD GURU
A PLURALSIGHT COMPANY

KEY CONCEPTS

- Data Deduplication can improve storage utilization of your Windows Server volumes.
- Deduplication is performed by an optimization task.
- Garbage collection to reclaim space runs every week.
- Deduplicated volumes can only be used on servers that have the feature enabled.
- Avoid incompatible products like database servers.
- BranchCache can be used to reduce bandwidth requirements by caching content locally.
- BranchCache is ideal for software distribution and operating system updates.
- Use hosted cache mode if you want to ensure all clients see improved performance.
- Use distributed cache mode if you don’t want servers at the branch office.
- Windows 10/11 Enterprise is required for HTTP and SMB traffic.

Configuring Hybrid File Synchronization

KEY CONCEPTS

- Azure File Sync allows you to synchronize or cache Azure Files share data outside Azure on Windows file servers.
- Synchronization is managed by the Storage Sync Service.
- A sync group contains one cloud endpoint and one or more server endpoints on one or more servers.
- A server can only be registered with one Storage Sync Service at a time.
- Cloud tiering can be used to free up space on your server endpoints.
- You can use DFS namespaces with Azure File Sync server endpoints.
- You can use a combination of DFS replication and Azure File Sync.
- Do not use DFS replication with cloud tiering.
- Do not use Azure File Sync with read-only DFS replication targets.