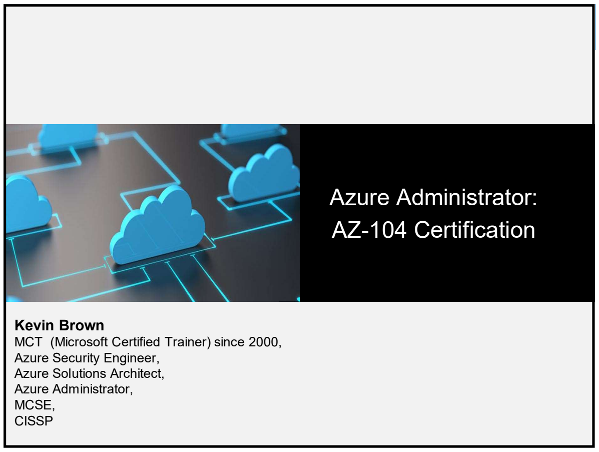
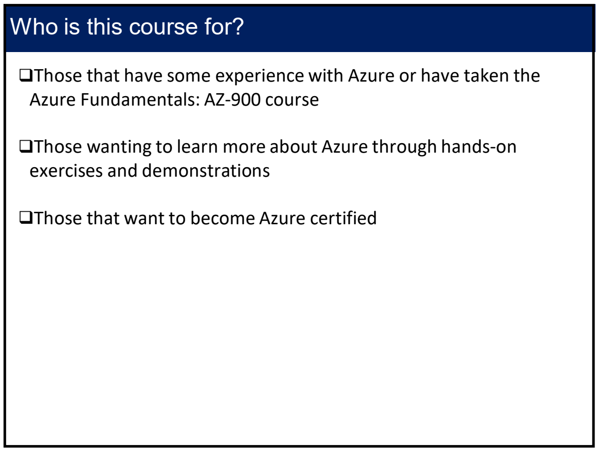


Azure Administrator: AZ-104 Certification

Kevin Brown
MCT (Microsoft Certified Trainer) since 2000,
Azure Security Engineer,
Azure Solutions Architect,
Azure Administrator,
MCSE,
CISSP

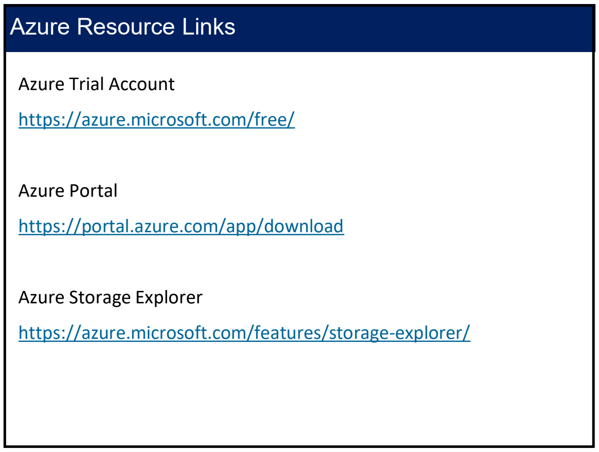


Who is this course for?

❑Those that have some experience with Azure or have taken the Azure Fundamentals: AZ-900 course

❑Those wanting to learn more about Azure through hands-on exercises and demonstrations

❑Those that want to become Azure certified



Azure Resource Links

Azure Trial Account

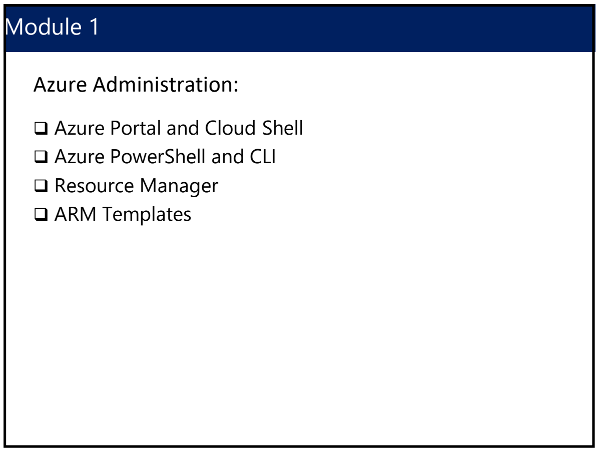
https://azure.microsoft.com/free/

Azure Portal

https://portal.azure.com/app/download

Azure Storage Explorer

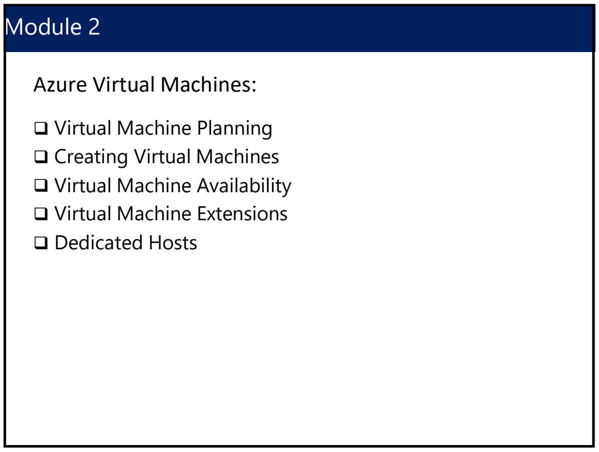
https://azure.microsoft.com/features/storage-explorer/



Module 1

Azure Administration:

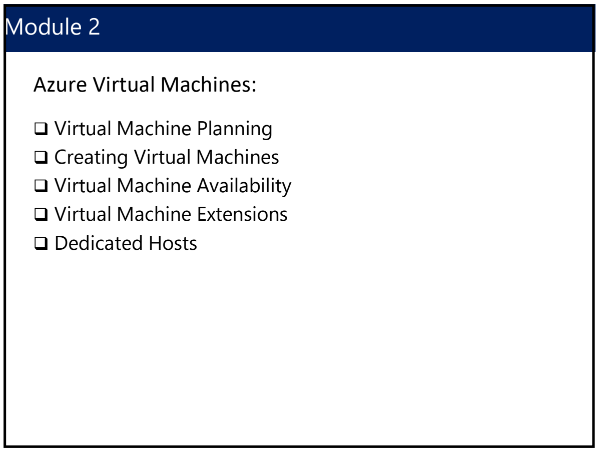
- ❑ Azure Portal and Cloud Shell
- ❑ Azure PowerShell and CLI
- ❑ Resource Manager
- ❑ ARM Templates



Module 2

Azure Virtual Machines:

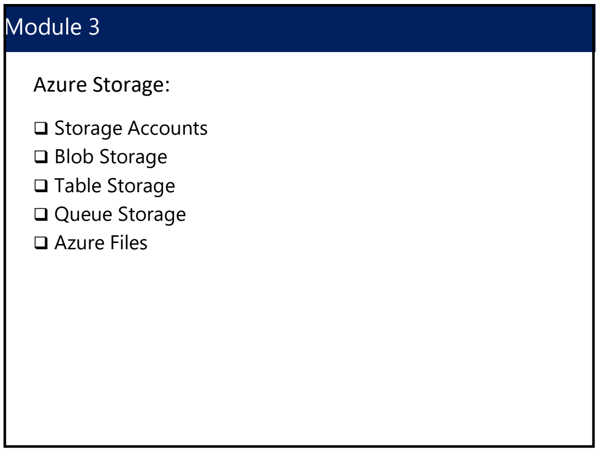
- ❑ Virtual Machine Planning
- ❑ Creating Virtual Machines
- ❑ Virtual Machine Availability
- ❑ Virtual Machine Extensions
- ❑ Dedicated Hosts



Module 2

Azure Virtual Machines:

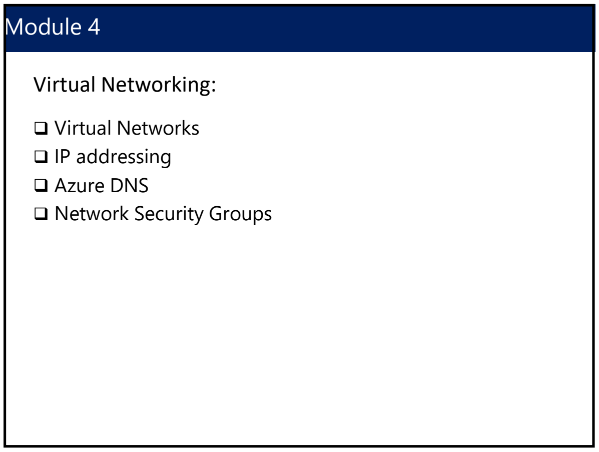
- ❑ Virtual Machine Planning
- ❑ Creating Virtual Machines
- ❑ Virtual Machine Availability
- ❑ Virtual Machine Extensions
- ❑ Dedicated Hosts



Module 3

Azure Storage:

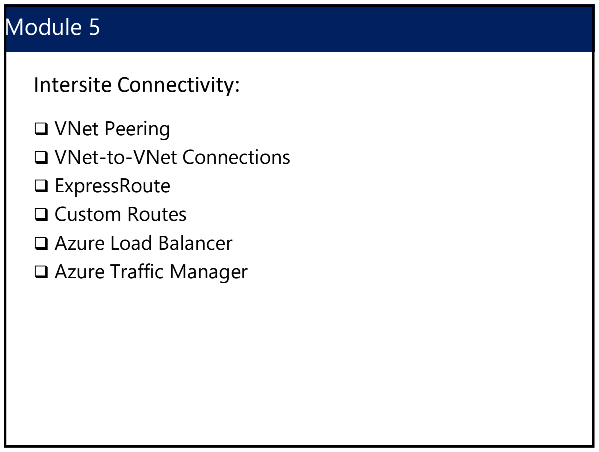
□ Storage Accounts
□ Blob Storage
□ Table Storage
□ Queue Storage
□ Azure Files



Module 4

Virtual Networking:

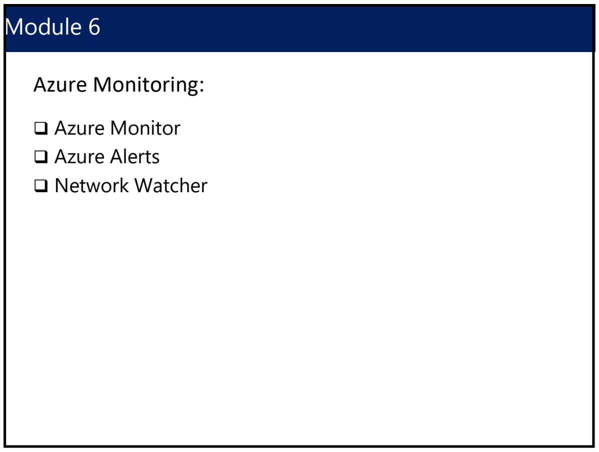
□ Virtual Networks
□ IP addressing
□ Azure DNS
□ Network Security Groups



Module 5

Intersite Connectivity:

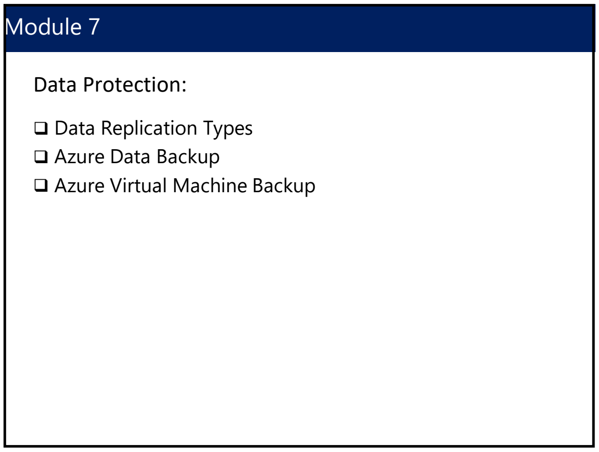
□ VNet Peering
□ VNet-to-VNet Connections
□ ExpressRoute
□ Custom Routes
□ Azure Load Balancer
□ Azure Traffic Manager



Module 6

Azure Monitoring:

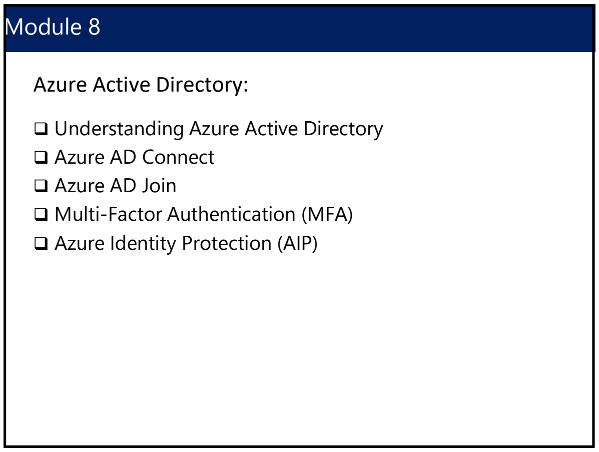
- □ Azure Monitor
- □ Azure Alerts
- □ Network Watcher



Module 7

Data Protection:

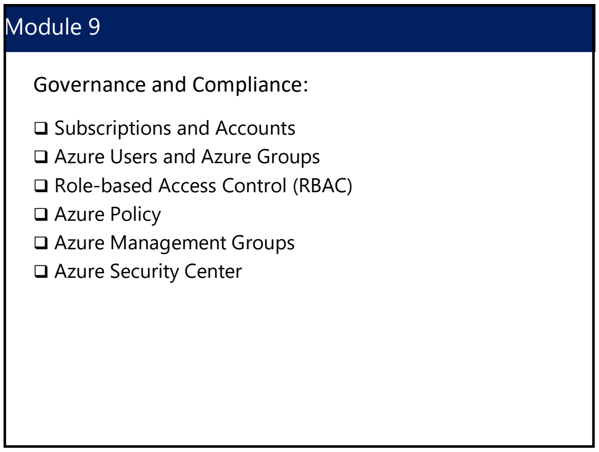
- □ Data Replication Types
- □ Azure Data Backup
- □ Azure Virtual Machine Backup



Module 8

Azure Active Directory:

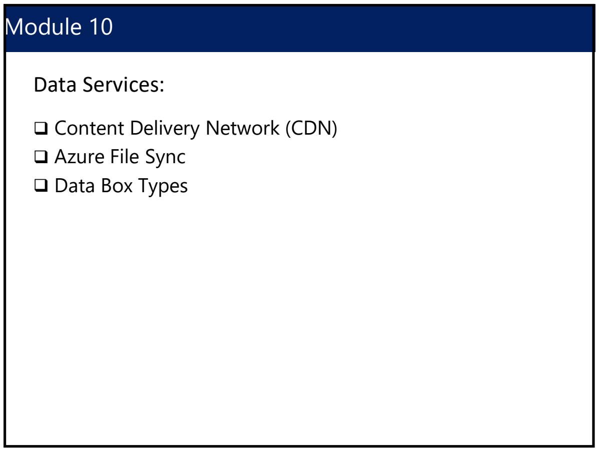
- □ Understanding Azure Active Directory
- □ Azure AD Connect
- □ Azure AD Join
- □ Multi-Factor Authentication (MFA)
- □ Azure Identity Protection (AIP)



Module 9

Governance and Compliance:

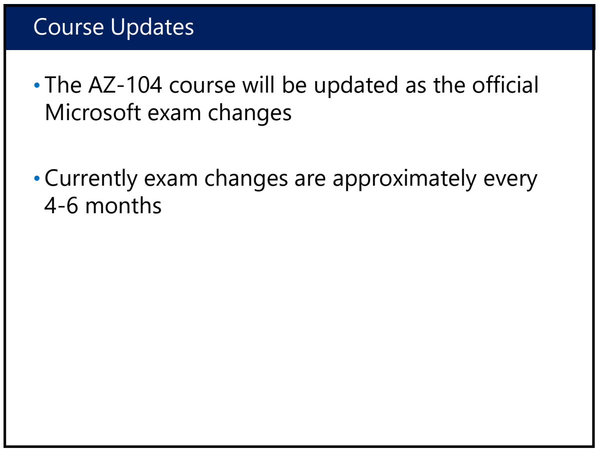
- ❑ Subscriptions and Accounts
- ❑ Azure Users and Azure Groups
- ❑ Role-based Access Control (RBAC)
- ❑ Azure Policy
- ❑ Azure Management Groups
- ❑ Azure Security Center



Module 10

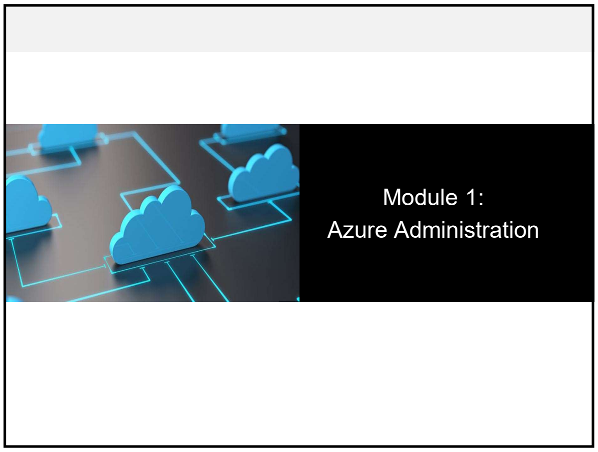
Data Services:

- ❑ Content Delivery Network (CDN)
- ❑ Azure File Sync
- ❑ Data Box Types

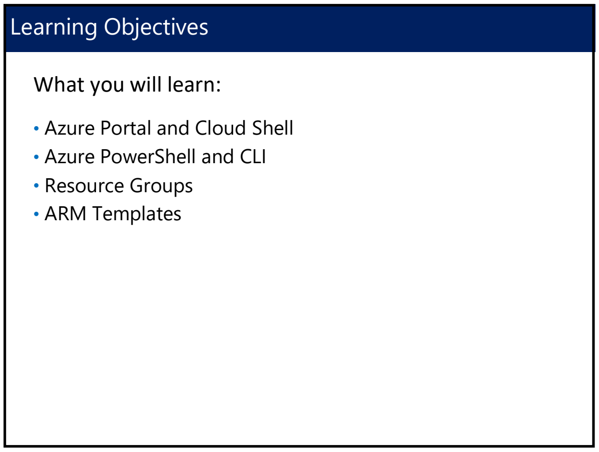


Course Updates

- The AZ-104 course will be updated as the official Microsoft exam changes
- Currently exam changes are approximately every 4-6 months



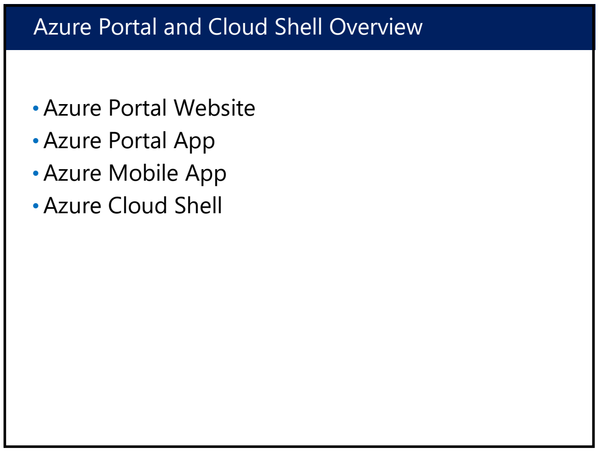
Module 1: Azure Administration



Learning Objectives

What you will learn:

- Azure Portal and Cloud Shell
- Azure PowerShell and CLI
- Resource Groups
- ARM Templates

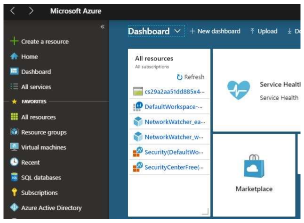


Azure Portal and Cloud Shell Overview

- Azure Portal Website
- Azure Portal App
- Azure Mobile App
- Azure Cloud Shell

Azure Portal

- Search and manage resources
- Create customized dashboards and favorites
- Access the Cloud Shell
- Receive notifications
- Managing subscriptions and billing



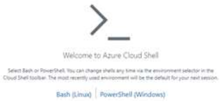
https://portal.azure.com/App/Download

Azure Mobile App

- Stay connected to the cloud, when mobile
- Check status and alerts
- Troubleshoot issues from any location
- Run commands to manage your Azure resources from mobile devices

Azure Cloud Shell

- Interactive, browser-accessible shell
- Offers either Bash or PowerShell
- Is temporary and provided on a per-session, per-user basis
- Requires a resource group, storage account, and Azure File share
- Authenticates automatically
- Times out after 20 minutes



Welcome to Azure Cloud Shell

Select Bash or PowerShell. You can change shells any time via the environment selector in the Cloud Shell toolbar. The most recently used environment will be the default for your next session.

Azure PowerShell

- Authenticate to your Azure subscription and manage resources
- Available as a local installation on Linux, macOS, or Windows

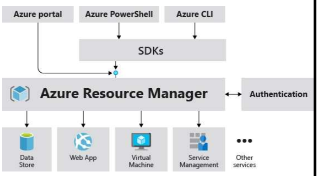
Azure Command Line Interface (CLI)

- Runs on Linux, macOS, and Windows
- Can be used interactively or used to run scripts
- Syntax is not the same as Bash or Powershell
- Use ***find*** to locate commands
- Use ***--help*** for more detailed information
- Can be used with Python and Java

https://aka.ms/InstallAzureCLIwindows

Resource Manager

- Provides a consistent management layer
- Enables you to work with the resources in your solution as a group
- Create, update or delete in a single operation
- Provides security and auditing
- Choose the tools that work best for you



Azure portal

Azure PowerShell

Azure CLI

SDKs

Azure Resource Manager

Authentication

Data Store

Web App

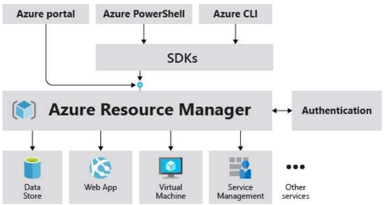
Virtual Machine

Service Management

Other services

Azure Resources

- A **resource** is simply a single service instance in Azure
- A **resource group** is a logical grouping of resources



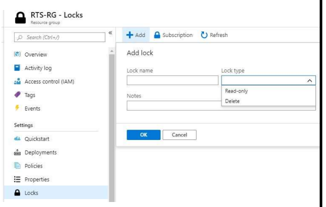
Azure portal
Azure PowerShell
Azure CLI
SDKs
Azure Resource Manager
Authentication
Data Store
Web App
Virtual Machine
Service Management
Other services

Azure Resources

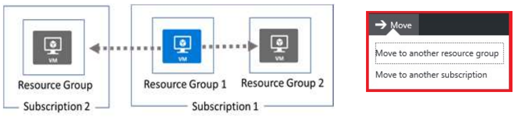
- Resources can only exist in one resource group
- Groups cannot be renamed
- Groups can have resources of many different types (services)
- Groups can have resources from many different regions

Azure Resource Locks

- Associate the lock with a subscription, resource group, or resource
- Locks are inherited by child resources
- Read-Only locks prevent any changes to the resource
- Delete locks prevent deletion



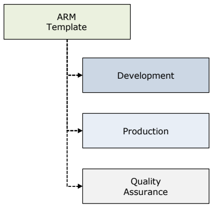
Moving Resources between Resource Groups



- When moving resources, both the source group and the target group are locked during the operation

ARM Templates Overview

- Improves consistency
- Define complex deployments
- Reduce errors
- Define requirements through code
- Can be reused


ARM Template

Development

Production

Quality Assurance

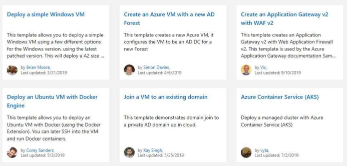
Template Variables

- Define values that are used throughout the template
- Makes your templates easier to maintain
- This example provides variables that describe network configuration for a virtual machine

```
"variables": {
  "nicName": "myVMNic",
  "addressPrefix": "10.0.0.0/16",
  "subnetName": “RTSSubnet",
  "subnetPrefix": "10.0.0.0/24",
  "publicIPAddressName": “RTSPublicIP",
  "virtualNetworkName": “RTSVNET"
}
```

QuickStart Templates

- Resource Manager templates provided by the Azure community
- Provides everything you need to deploy your solution or serves as a starting point for your template



Deploy a simple Windows VM

This template allows you to deploy a simple Windows VM using a few different options for the Windows version, using the latest patched version. This will deploy a A2 size ...

by Brian Moore, Last updated: 3/21/2019

Create an Azure VM with a new AD Forest

This template creates a new Azure VM, it configures the VM to be an AD DC for a new Forest

by Simon Davies, Last updated: 4/6/2019

Create an Application Gateway v2 with WAF v2

This template creates an Application Gateway v2 with Web Application Firewall v2. This template is used by the Azure Application Gateway documentation Sam...

by Vic, Last updated: 9/10/2019

Deploy an Ubuntu VM with Docker Engine

This template allows you to deploy an Ubuntu VM with Docker (using the Docker Extension). You can later SSH into the VM and run Docker containers.

by Corey Sanders, Last updated: 5/3/2019

Join a VM to an existing domain

This template demonstrates domain join to a private AD domain up in cloud.

by Kay Singh, Last updated: 5/25/2018

Azure Container Service (AKS)

Deploy a managed cluster with Azure Container Service (AKS)

by vyta, Last updated: 7/2/2019

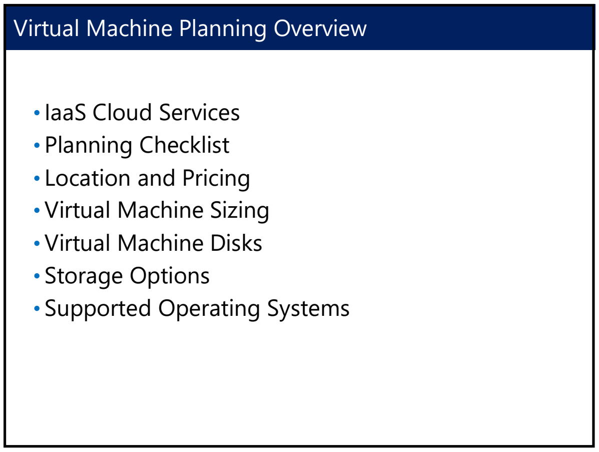
https://azure.microsoft.com/resources/templates/

Module 2:
Azure Virtual Machines

Learning Objectives

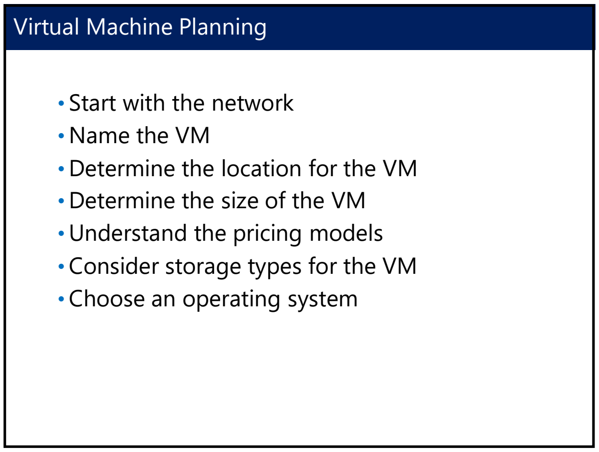
What you will learn:

- Virtual Machine Planning
- Creating Virtual Machines
- Virtual Machine Availability



Virtual Machine Planning Overview

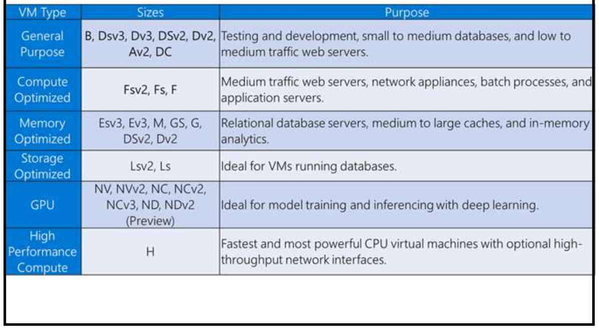
- IaaS Cloud Services
- Planning Checklist
- Location and Pricing
- Virtual Machine Sizing
- Virtual Machine Disks
- Storage Options
- Supported Operating Systems



Virtual Machine Planning

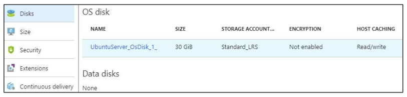
- Start with the network
- Name the VM
- Determine the location for the VM
- Determine the size of the VM
- Understand the pricing models
- Consider storage types for the VM
- Choose an operating system

Virtual Machine Types



VM Type	Sizes	Purpose
General Purpose	B, Dsv3, Dv3, DSv2, Dv2, Av2, DC	Testing and development, small to medium databases, and low to medium traffic web servers.
Compute Optimized	Fsv2, Fs, F	Medium traffic web servers, network appliances, batch processes, and application servers.
Memory Optimized	Esv3, Ev3, M, GS, G, DSv2, Dv2	Relational database servers, medium to large caches, and in-memory analytics.
Storage Optimized	Lsv2, Ls	Ideal for VMs running databases.
GPU	NV, NVv2, NC, NCv2, NCv3, ND, NDv2 (Preview)	Ideal for model training and inferencing with deep learning.
High Performance Compute	H	Fastest and most powerful CPU virtual machines with optional high-throughput network interfaces.

Understanding Virtual Machine Disks



OS disk

NAME	SIZE	STORAGE ACCOUNT...	ENCRYPTION	HOST CACHING
UbuntuServer_OsDisk_1_	30 GiB	Standard_LRS	Not enabled	Read/write

Data disks

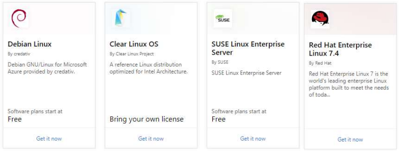
None

- **Operating System Disks** are SATA drives, labeled as C:
- **Temporary Disks** provides short term storage
- **Data Disks** are SCSI drives and depend on your virtual machine type

Storage Types

- Premium storage offers high-performance, low-latency SSD disk support
- Use premium storage for virtual machines with input/output (I/O)-intensive workloads
- Two types of disks: Unmanaged and Managed
  - Unmanaged disks require you to manage the storage accounts and VHDs
  - Managed disks are maintained by Azure (recommended)

Linux Virtual Machines



Debian Linux
By credativ
Debian GNU/Linux for Microsoft Azure provided by credativ.
Software plans start at
Free
Get it now

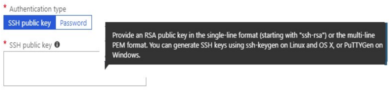
Clear Linux OS
By Clear Linux Project
A reference Linux distribution optimized for Intel Architecture.
Bring your own license
Get it now

SUSE Linux Enterprise Server
By SUSE
SUSE Linux Enterprise Server
Software plans start at
Free
Get it now

Red Hat Enterprise Linux 7.4
By Red Hat
Red Hat Enterprise Linux 7 is the world's leading enterprise Linux platform built to meet the needs of toda...
Get it now

- Hundreds of community-built images in the Azure Marketplace
- Linux has the same deployment options as for Windows VMs
- Manage Linux VMs with many popular open-source DevOps tools

Linux VM Connections



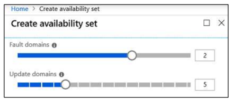
* Authentication type
SSH public key | Password

* SSH public key

Provide an RSA public key in the single-line format (starting with "ssh-rsa") or the multi-line PEM format. You can generate SSH keys using ssh-keygen on Linux and OS X, or PuTTYGen on Windows.

- Authenticate with a SSH public key or password
- SSH is an encrypted connection protocol that allows secure logins over unsecured connections
- There are public and private keys

Availability Sets



Home > Create availability set

Create availability set

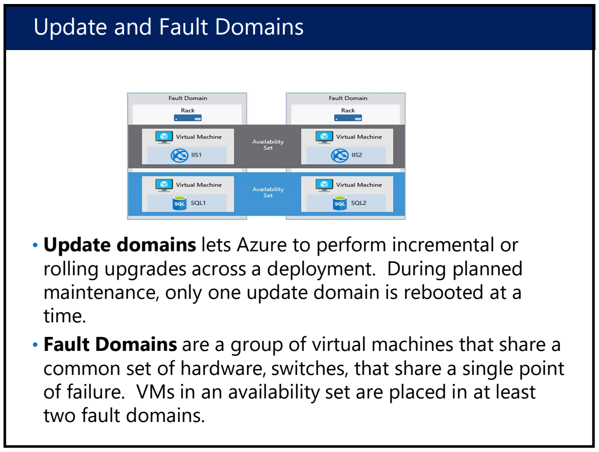
Fault domains: 2

Update domains: 5

Two or more instances in two or more availability zones = 99.99% uptime

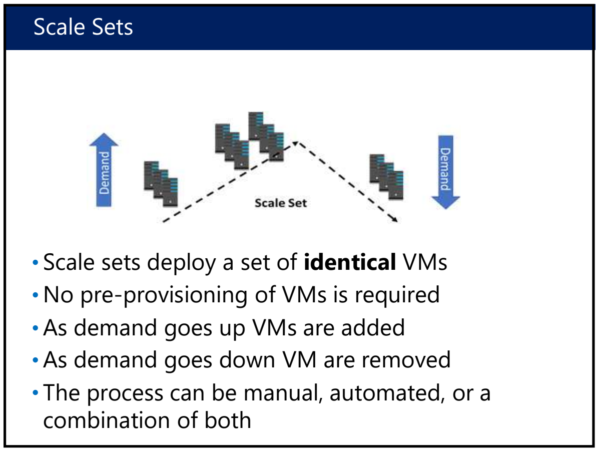
- Configure multiple virtual machines in an Availability Set

- Configure each application tier into separate Availability Sets



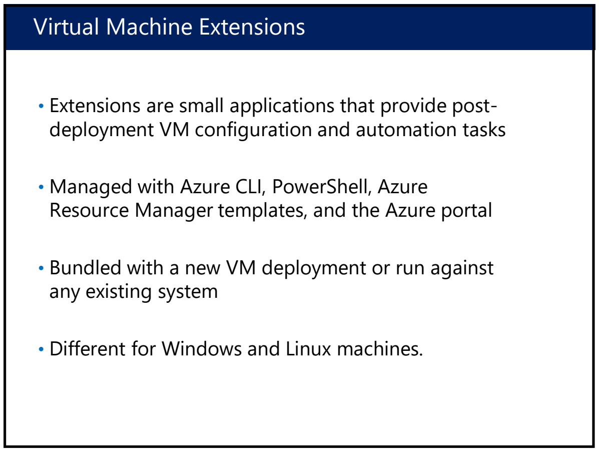
Update and Fault Domains

- **Update domains** lets Azure to perform incremental or rolling upgrades across a deployment. During planned maintenance, only one update domain is rebooted at a time.
- **Fault Domains** are a group of virtual machines that share a common set of hardware, switches, that share a single point of failure. VMs in an availability set are placed in at least two fault domains.



Scale Sets

- Scale sets deploy a set of **identical** VMs
- No pre-provisioning of VMs is required
- As demand goes up VMs are added
- As demand goes down VM are removed
- The process can be manual, automated, or a combination of both



Virtual Machine Extensions

- Extensions are small applications that provide post-deployment VM configuration and automation tasks
- Managed with Azure CLI, PowerShell, Azure Resource Manager templates, and the Azure portal
- Bundled with a new VM deployment or run against any existing system
- Different for Windows and Linux machines.

Changes to Azure Information Protection Licensing

AIP Licensing
https://azure.microsoft.com/pricing/details/information-protection/

Microsoft 365
https://www.microsoft.com/en-us/microsoft-365/try

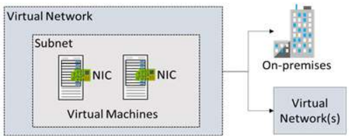
Module 4:
Virtual Networking

Learning Objectives

What you will learn:

- Virtual Networks
- IP Addressing and Endpoints
- Azure DNS
- Network Security Groups

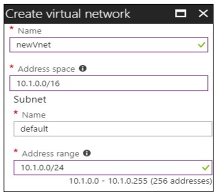
Virtual Networks



- Logical representation of your own network
- Create a dedicated private cloud-only VNet
- Securely extend your datacenter With VNets
- Enable hybrid cloud scenarios

Implementing Virtual Networks

- Create new virtual networks at any time
- Add virtual networks when you create a virtual machine
- Need to define the address space, and at least one subnet
- Be careful with overlapping address spaces



Create virtual network

* Name

newVnet ✓

* Address space

10.1.0.0/16

Subnet

* Name

default

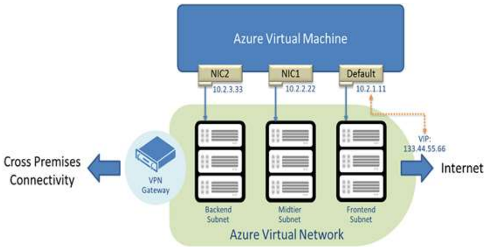
* Address range

10.1.0.0/24 ✓

10.1.0.0 - 10.1.0.255 (256 addresses)

Multiple NICs in Virtual Machines

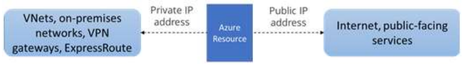
- You can create virtual machines with multiple NICs
- The VM size determines the number of NICs that can be supported



IP Addressing Overview

- IP Addressing
- Public IP Addresses
- Private IP Addresses
- Demonstration – Manage IP Addresses
- Service Endpoints
- Service Endpoint Services
- Secure Access to Storage
- Demonstration – Service Endpoints

IP Addressing



VNets, on-premises networks, VPN gateways, ExpressRoute

Private IP address

Azure Resource

Public IP address

Internet, public-facing services

- **Private IP addresses** are used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure
- **Public IP addresses** is used for communication with the Internet, including Azure public-facing services

Public IP Addresses

	NIC	Yes	Yes
	Front-end configuration	Yes	Yes
	Gateway IP configuration	Yes	No
	Front-end configuration	Yes	No

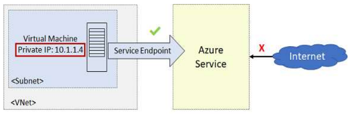
- A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways.

Private IP Addresses

	NIC	Yes	Yes
	Front-end configuration	Yes	Yes
	Front-end configuration	Yes	Yes

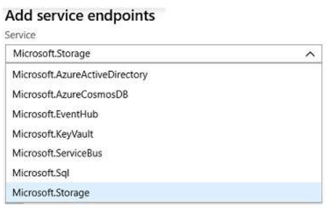
- **Dynamic (default)**. Azure assigns the next available unassigned or unreserved IP address in the subnet's address range
- **Static.** You select and assign any unassigned or unreserved IP address in the subnet's address range

Service Endpoints



- Endpoints limit network access to specific subnets and IP addresses
- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Endpoints use the Microsoft Azure backbone network

Service Endpoint Services



Add service endpoints

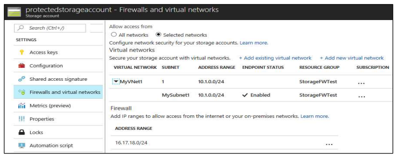
Service

Microsoft.Storage

Microsoft.AzureActiveDirectory
Microsoft.AzureCosmosDB
Microsoft.EventHub
Microsoft.KeyVault
Microsoft.ServiceBus
Microsoft.Sql
Microsoft.Storage

✓ Adding service endpoints can take up to 15 minutes to complete

Secure Access to Storage Endpoints



protectedstorageaccount - Firewalls and virtual networks
Storage account

Search (Ctrl+/)

SETTINGS
- Access keys
- Configuration
- Shared access signature
- Firewalls and virtual networks
- Metrics (preview)
- Properties
- Locks
- Automation script

Allow access from
○ All networks ● Selected networks
Configure network security for your storage accounts. Learn more.

Virtual networks
Secure your storage account with virtual networks. + Add existing virtual network + Add new virtual network

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
MyVNet1	1	10.1.0.0/24		StorageFWTest	...
	MySubnet1	10.1.0.0/24	✓ Enabled	StorageFWTest	...

Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

ADDRESS RANGE	
16.17.18.0/24	...

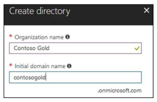
- Must configure both sides of the endpoints. For example, the virtual network side and the storage account side.
- Each service endpoint has its own Azure documentation page

Azure DNS Overview

- Domains and Custom Domains
- Verifying Custom Domain Names
- Azure DNS Zones
- DNS Record Sets
- DNS Delegation
- DNS for Private Domains
- Private Zones Scenarios
- Demonstration – DNS Name Resolution

Domains and Custom Domains

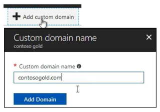
- When you create an Azure subscription an Azure AD domain is created for you
- The domain has initial domain name in the form *domainname.onmicrosoft.com*
- You can customize/change the name
- After the custom name is added it must be verified (next topic)



Create directory

* Organization name: Contoso Gold

* Initial domain name: contosogold .onmicrosoft.com

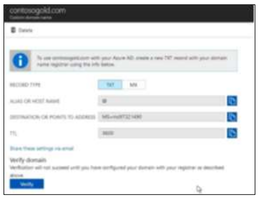


Custom domain name
contoso gold

* Custom domain name: contosogold.com

Verify the Custom Domain Name

- Verification demonstrates ownership of the domain name
- Add a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone
- Azure will query the DNS domain for the presence of the record
- This could take several minutes or several



contosogold.com
Custom domain name

Delete

To use contosogold.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE: TXT | MX

ALIAS OR HOST NAME: @

DESTINATION OR POINTS TO ADDRESS: MS=ms09732 1490

TTL: 3600

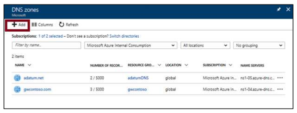
Share these settings via email

Verify domain

Verification will not succeed until you have configured your domain with your registrar as described above.

Verify

Azure DNS Zones



DNS zones
Microsoft

+ Add | Columns | Refresh

Subscriptions: 1 of 2 selected – Don't see a subscription? Switch directories

Filter by name... | Microsoft Azure Internal Consumption | All locations | No grouping

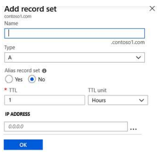
2 items

NAME	NUMBER OF RECOR...	RESOURCE GRO...	LOCATION	SUBSCRIPTION	NAME SERVERS
adatum.net	2 / 5000	adatumDNS	global	Microsoft Azure In...	ns1-05.azure-dns.c...
gwcontoso.com	3 / 5000	gwcontoso	global	Microsoft Azure In...	ns1-04.azure-dns.c...

- A DNS zone hosts the DNS records for a domain
- The name of the zone must be unique within the resource group
- Where multiple zones share the same name, each instance is assigned different name server addresses
- Only one set of addresses can be configured with the domain name registrar

DNS Record Sets

- A record set is a collection of records in a zone that have the same name and are the same type
- You can add up to 20 records to any record set
- A record set cannot contain two identical records
- Changing the drop-down Type, changes the information required



Add record set
contoso1.com

Name: .contoso1.com

Type: A

Alias record set: ○ Yes ● No

* TTL: 1

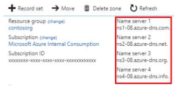
TTL unit: Hours

IP ADDRESS: 0.0.0.0

OK

DNS Delegation

- When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four
- Once the DNS zone is created, update the parent registrar
- For child zones, register the NS records in the parent domain

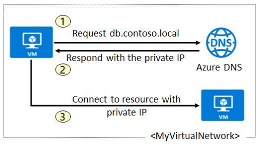


Resource group (change)
contosorg
Subscription (change)
Microsoft Azure Internal Consumption
Subscription ID
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

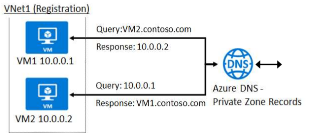
Name server 1
ns1-08.azure-dns.com.
Name server 2
ns2-08.azure-dns.net.
Name server 3
ns3-08.azure-dns.org.
Name server 4
ns4-08.azure-dns.info.

DNS for Private Domains

- Use your own custom domain names
- Provides name resolution for VMs within a VNet and between VNets
- Automatic hostname record management
- Removes the need for custom DNS solutions
- Use all common DNS records types
- Available in all Azure regions


1
Request db.contoso.local
VM
DNS
Respond with the private IP
2
Azure DNS
Connect to resource with private IP
3
VM
<MyVirtualNetwork>

Private Zone Scenarios

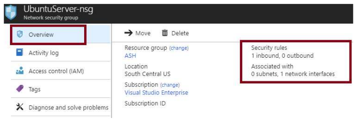


- DNS resolution in VNet1 is private and not accessible from the Internet
- DNS queries across the virtual networks are resolved
- Reverse DNS queries are scoped to the same virtual network

Network Security Groups Overview

- Network Security Groups
- NSG Rules
- NSG Effective Rules
- Creating NSG Rules
- Demonstration - NSGs

Network Security Groups (NSG)



Resource group (change)
ASH

Location
South Central US

Subscription (change)
Visual Studio Enterprise

Subscription ID

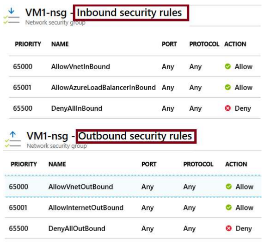
Security rules
1 inbound, 0 outbound

Associated with
0 subnets, 1 network interfaces

- You can limit network traffic to resources in a virtual network using a NSG
- A NSG contains a list of security rules that allow or deny inbound or outbound network traffic
- An NSG can be associated to a subnet or a network interface

NSG Rules

- Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces.
- There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority.



VM1-nsg - Inbound security rules

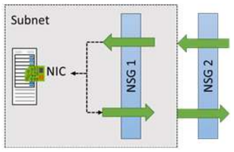
PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetInBound	Any	Any	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	✓ Allow
65500	DenyAllInBound	Any	Any	✗ Deny

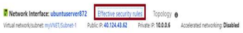
VM1-nsg - Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetOutBound	Any	Any	✓ Allow
65001	AllowInternetOutBound	Any	Any	✓ Allow
65500	DenyAllOutBound	Any	Any	✗ Deny

NSG Effective Rules

- NSGs are evaluated independently for the subnet and NIC
- An “allow” rule must exist at both levels for traffic to be admitted
- Use the Effective Rules link if you are not sure which security rules are being applied

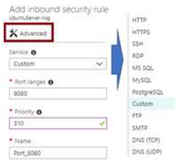



Network Interface: ubuntuserver872 | Effective security rules | Topology

Virtual network/subnet: myVNET/Subnet-1 | Public IP: 40.124.43.62 | Private IP: 10.0.0.6 | Accelerated networking: Disabled

Creating NSG Rules

- Select from a large variety of services
- **Service** - The destination protocol and port range for this rule
- **Port ranges** – Single port or multiple ports
- **Priority** - The lower the number, the higher the priority


Add inbound security rule

UbuntuServer-nsg

Advanced

Service: Custom

* Port ranges: 8080

* Priority: 310

* Name: Port_8080

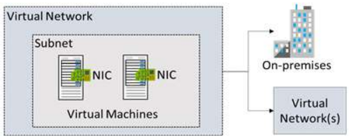
Module 4:
Virtual Networking

Learning Objectives

What you will learn:

- Virtual Networks
- IP Addressing and Endpoints
- Azure DNS
- Network Security Groups

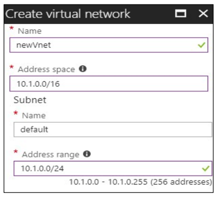
Virtual Networks



- Logical representation of your own network
- Create a dedicated private cloud-only VNet
- Securely extend your datacenter With VNets
- Enable hybrid cloud scenarios

Implementing Virtual Networks

- Create new virtual networks at any time
- Add virtual networks when you create a virtual machine
- Need to define the address space, and at least one subnet
- Be careful with overlapping address spaces


Create virtual network

* Name: newVnet ✓

* Address space: 10.1.0.0/16

Subnet

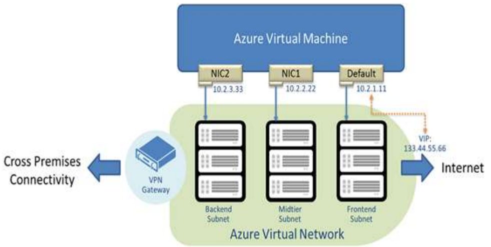
* Name: default

* Address range: 10.1.0.0/24 ✓

10.1.0.0 - 10.1.0.255 (256 addresses)

Multiple NICs in Virtual Machines

- You can create virtual machines with multiple NICs
- The VM size determines the number of NICs that can be supported



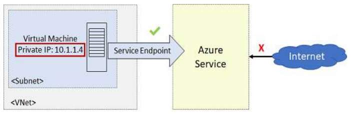
IP Addressing

- **Private IP addresses** are used within an Azure virtual network (VNet) and your on-premises network

- **Public IP addresses** is used for communication with the Internet, including Azure public-facing services

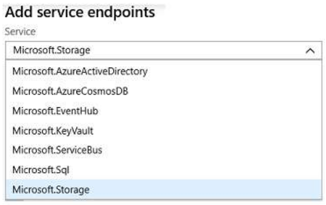
- IP addresses can be **Static** or **Dynamic**

Service Endpoints



- Endpoints limit network access to specific subnets and IP addresses
- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Endpoints use the Microsoft Azure backbone network

Service Endpoint Services



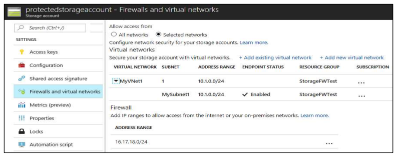
Add service endpoints

Service

Microsoft.Storage

✓ Adding service endpoints can take up to 15 minutes to complete

Secure Access to Storage Endpoints



protectedstorageaccount - Firewalls and virtual networks

Storage account

Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more.

Virtual networks

Secure your storage account with virtual networks. + Add existing virtual network + Add new virtual network

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
MyVNet1	1	10.1.0.0/24		StorageFWTest	...
	MySubnet1	10.1.0.0/24	✓ Enabled	StorageFWTest	...

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

ADDRESS RANGE	
16.17.18.0/24	...

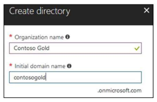
- Must configure both sides of the endpoints. For example, the virtual network side and the storage account side.
- Each service endpoint has its own Azure documentation page

Azure DNS Overview

- Domains and Custom Domains
- Verifying Custom Domain Names
- Azure DNS Zones
- DNS Record Sets
- DNS Delegation
- DNS for Private Domains
- Private Zones Scenarios
- Demonstration – DNS Name Resolution

Domains and Custom Domains

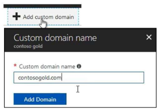
- When you create an Azure subscription an Azure AD domain is created for you
- The domain has initial domain name in the form *domainname.onmicrosoft.com*
- You can customize/change the name
- After the custom name is added it must be verified (next topic)



Create directory

* Organization name: Contoso Gold

* Initial domain name: contosogold .onmicrosoft.com



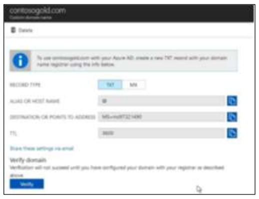
Custom domain name

contoso gold

* Custom domain name: contosogold.com

Verify the Custom Domain Name

- Verification demonstrates ownership of the domain name
- Add a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone
- Azure will query the DNS domain for the presence of the record
- This could take several minutes or several



contosogold.com

Custom domain name

To use contosogold.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE: TXT MX

ALIAS OR HOST NAME: @

DESTINATION OR POINTS TO ADDRESS: MS=ms[illegible]

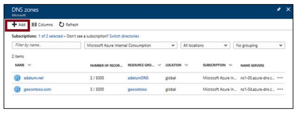
TTL: 3600

Share these settings via email

Verify domain

Verification will not succeed until you have configured your domain with your registrar as described above.

Azure DNS Zones



DNS zones

Microsoft

Subscriptions: 1 of 2 selected – Don't see a subscription? Switch directories

Filter by name... | Microsoft Azure Internal Consumption | All locations | No grouping

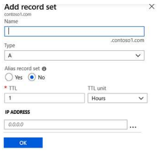
2 items

NAME	NUMBER OF RECOR...	RESOURCE GRO...	LOCATION	SUBSCRIPTION	NAME SERVERS
adatum.net	2 / 5000	adatumDNS	global	Microsoft Azure In...	ns1-05.azure-dns.c...
gwcontoso.com	3 / 5000	gwcontoso	global	Microsoft Azure In...	ns1-04.azure-dns.c...

- A DNS zone hosts the DNS records for a domain
- The name of the zone must be unique within the resource group
- Where multiple zones share the same name, each instance is assigned different name server addresses
- Only one set of addresses can be configured with the domain name registrar

DNS Record Sets

- A record set is a collection of records in a zone that have the same name and are the same type
- You can add up to 20 records to any record set
- A record set cannot contain two identical records
- Changing the drop-down Type, changes the information required



Add record set

contoso1.com

Name: .contoso1.com

Type: A

Alias record set: ○ Yes ● No

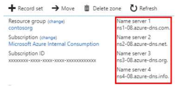
* TTL: 1

TTL unit: Hours

IP ADDRESS: 0.0.0.0

DNS Delegation

- When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four
- Once the DNS zone is created, update the parent registrar
- For child zones, register the NS records in the parent domain



Resource group (change)
contosorg

Subscription (change)
Microsoft Azure Internal Consumption

Subscription ID
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Name server 1
ns1-08.azure-dns.com.

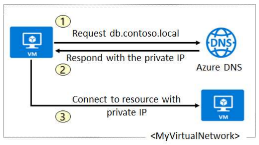
Name server 2
ns2-08.azure-dns.net.

Name server 3
ns3-08.azure-dns.org.

Name server 4
ns4-08.azure-dns.info.

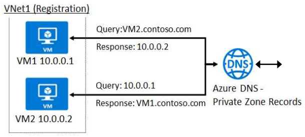
DNS for Private Domains

- Use your own custom domain names
- Provides name resolution for VMs within a VNet and between VNets
- Automatic hostname record management
- Removes the need for custom DNS solutions
- Use all common DNS records types
- Available in all Azure regions



1
Request db.contoso.local
2
Respond with the private IP
3
Connect to resource with private IP
VM
DNS
Azure DNS
VM
<MyVirtualNetwork>

Private Zone Scenarios

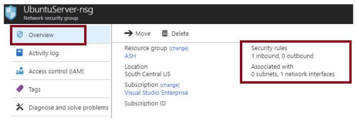


- DNS resolution in VNet1 is private and not accessible from the Internet
- DNS queries across the virtual networks are resolved
- Reverse DNS queries are scoped to the same virtual network

Network Security Groups Overview

- Network Security Groups
- NSG Rules
- NSG Effective Rules
- Creating NSG Rules
- Demonstration - NSGs

Network Security Groups (NSG)



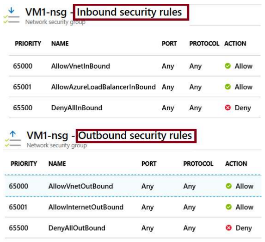
Resource group (change)
ASH
Location
South Central US
Subscription (change)
Visual Studio Enterprise
Subscription ID

Security rules
1 inbound, 0 outbound
Associated with
0 subnets, 1 network interfaces

- You can limit network traffic to resources in a virtual network using a NSG
- A NSG contains a list of security rules that allow or deny inbound or outbound network traffic
- An NSG can be associated to a subnet or a network interface

NSG Rules

- Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces.
- There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority.



VM1-nsg - Inbound security rules
Network security group

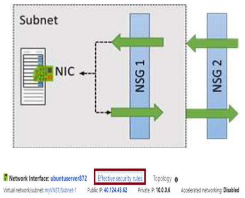
PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetInBound	Any	Any	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	✓ Allow
65500	DenyAllInBound	Any	Any	✕ Deny

VM1-nsg - Outbound security rules
Network security group

PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetOutBound	Any	Any	✓ Allow
65001	AllowInternetOutBound	Any	Any	✓ Allow
65500	DenyAllOutBound	Any	Any	✕ Deny

NSG Effective Rules

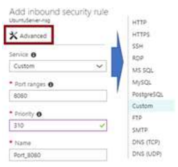
- NSGs are evaluated independently for the subnet and NIC
- An "allow" rule must exist at both levels for traffic to be admitted
- Use the Effective Rules link if you are not sure which security rules are being applied



Network Interface: ubuntuserver872
Virtual network/subnet: myVNET/Subnet-1 Public IP: 40.124.43.62 Private IP: 10.0.0.6 Accelerated networking: Disabled

Creating NSG Rules

- Select from a large variety of services
- **Service** - The destination protocol and port range for this rule
- **Port ranges** – Single port or multiple ports
- **Priority** - The lower the number, the higher the priority



Add inbound security rule
UbuntuServer-nsg

Service: Custom

* Port ranges: 8080

* Priority: 310

* Name: Port_8080

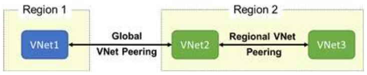
Module 5: Virtual Network Connectivity

Learning Objectives

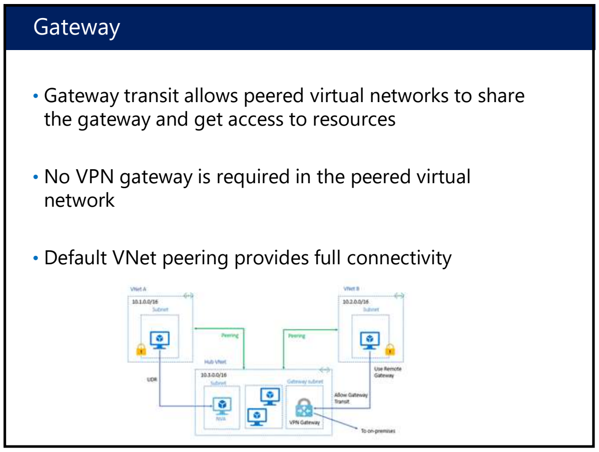
What you will learn:

- VNet Peering
- VNet-to-VNet Connections
- ExpressRoute

VNet Peering

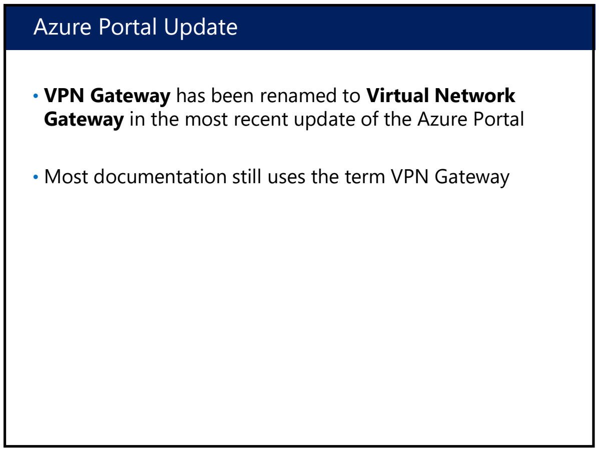


- VNet peering connects two Azure virtual networks
- Two types of peering: Regional and Global



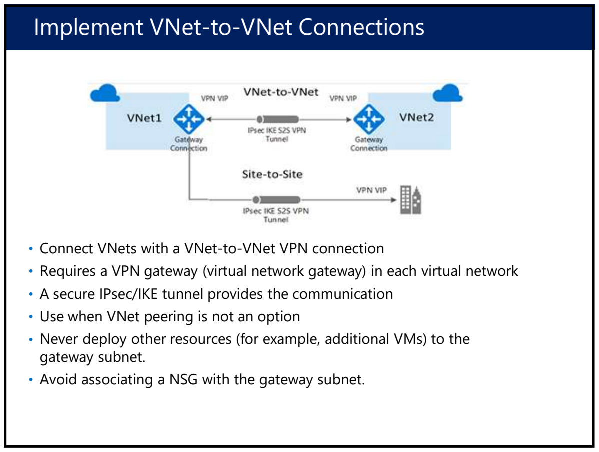
Gateway

- Gateway transit allows peered virtual networks to share the gateway and get access to resources
- No VPN gateway is required in the peered virtual network
- Default VNet peering provides full connectivity



Azure Portal Update

- **VPN Gateway** has been renamed to **Virtual Network Gateway** in the most recent update of the Azure Portal
- Most documentation still uses the term VPN Gateway



Implement VNet-to-VNet Connections

- Connect VNets with a VNet-to-VNet VPN connection
- Requires a VPN gateway (virtual network gateway) in each virtual network
- A secure IPsec/IKE tunnel provides the communication
- Use when VNet peering is not an option
- Never deploy other resources (for example, additional VMs) to the gateway subnet.
- Avoid associating a NSG with the gateway subnet.

Connect your datacenter to Azure

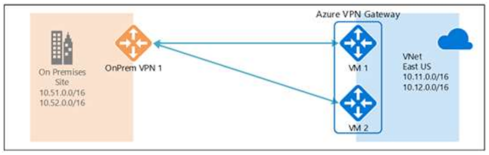
- Azure Virtual Network Gateway connects your on-premises networks to Azure through Site-to-Site VPNs in a similar way that you set up and connect to a remote branch office. The connectivity is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

Connect your datacenter to Azure

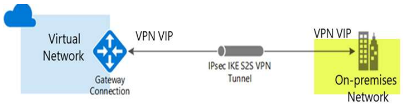
- Azure Virtual Network Gateway connects your on-premises networks to Azure through Site-to-Site VPNs in a similar way that you set up and connect to a remote branch office. The connectivity is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

Active-Active VPN

You can now create an Azure virtual network gateway in an active-active configuration, where both instances of the gateway VMs will establish S2S VPN tunnels to your on-premises VPN device, as shown the following diagram:



Configure the On-Premises VPN Device

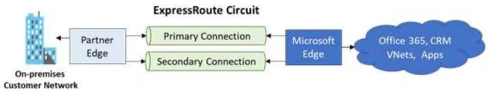


- Consult the list of supported VPN devices (Cisco, Juniper, Ubiquiti, Barracuda Networks)
- A VPN device configuration script may be available
- Remember the shared key for the Azure connection (next step)
- Specify the public IP address (previous step)

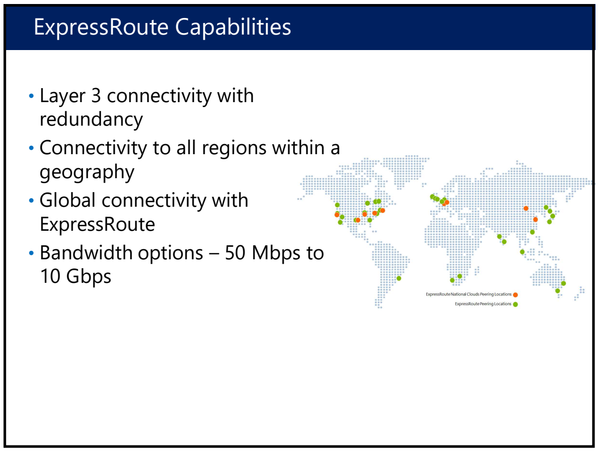
ExpressRoute Connections Overview

- ExpressRoute
- ExpressRoute Capabilities
- ExpressRoute Connections
- Coexisting Site-to-Site and ExpressRoute

ExpressRoute



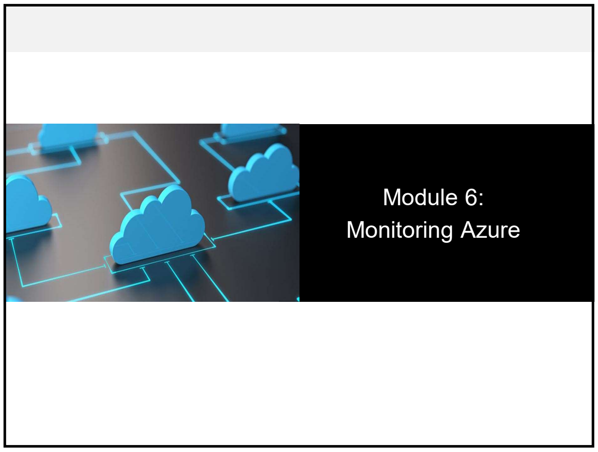
- Extends on-premises networks into Microsoft cloud with dedicated private connections
- Excellent for data migration, business continuity, and disaster recovery
- Cost-effective option for transferring datasets
- Adds high throughput and fast latency capacity to your datacenter



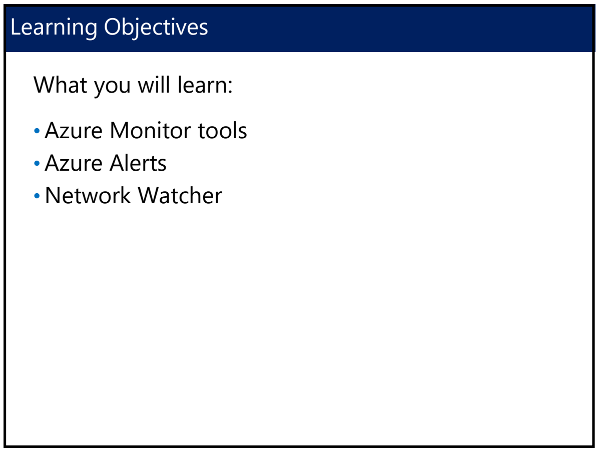
ExpressRoute Capabilities

- Layer 3 connectivity with redundancy
- Connectivity to all regions within a geography
- Global connectivity with ExpressRoute
- Bandwidth options – 50 Mbps to 10 Gbps

ExpressRoute National Clouds Peering Locations 🟠
ExpressRoute Peering Locations 🟢



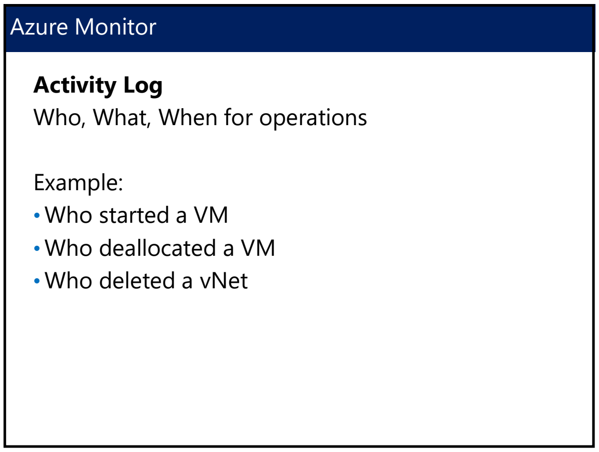
Module 6:
Monitoring Azure



Learning Objectives

What you will learn:

- Azure Monitor tools
- Azure Alerts
- Network Watcher

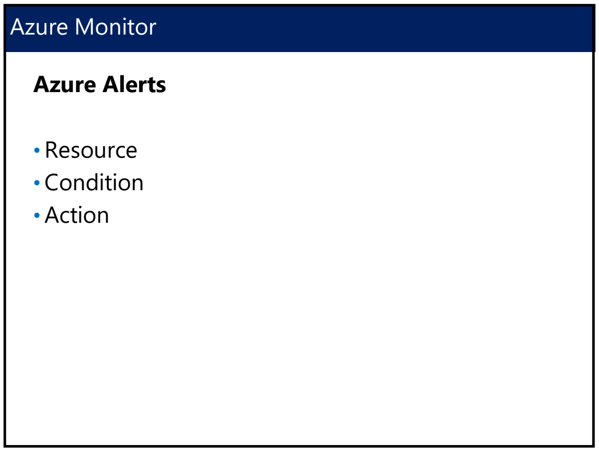


Azure Monitor

Activity Log
Who, What, When for operations

Example:

- Who started a VM
- Who deallocated a VM
- Who deleted a vNet

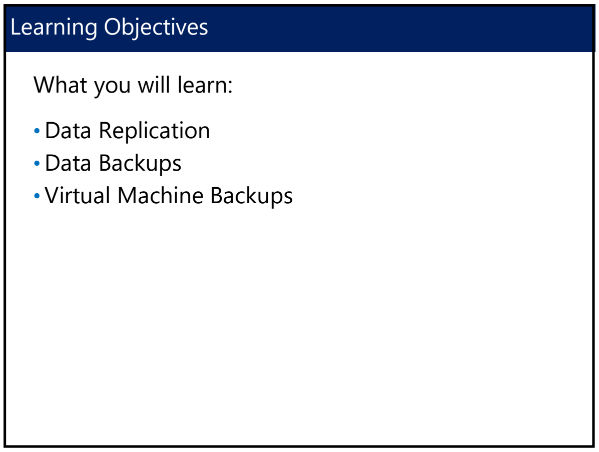


Azure Monitor

Azure Alerts

- Resource
- Condition
- Action

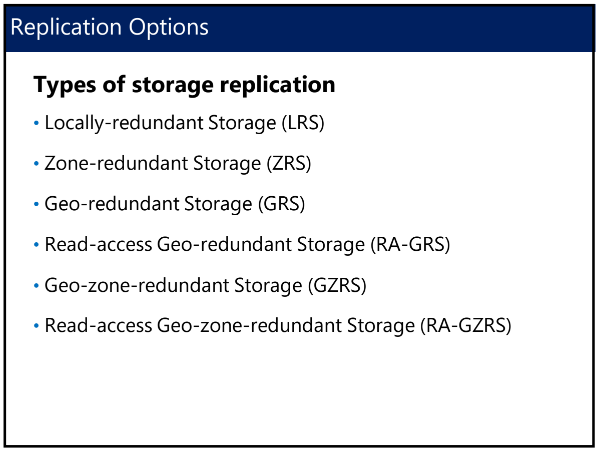
Module 7:
Data Protection



Learning Objectives

What you will learn:

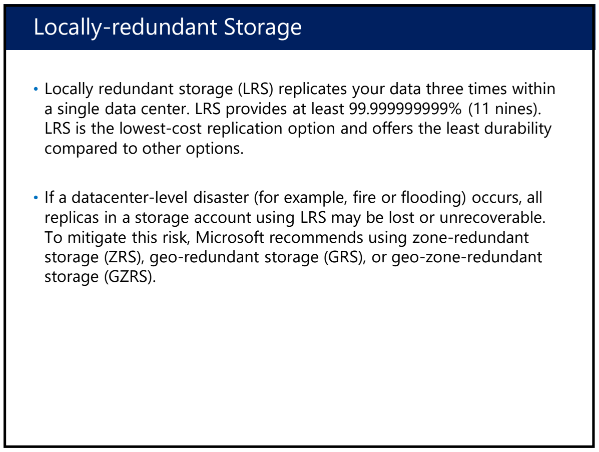
- Data Replication
- Data Backups
- Virtual Machine Backups



Replication Options

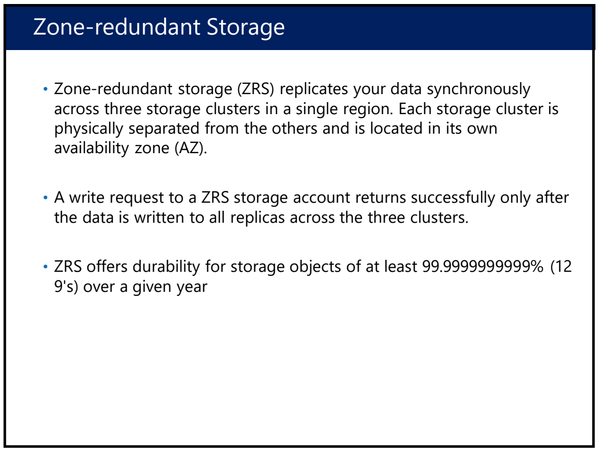
Types of storage replication

- Locally-redundant Storage (LRS)
- Zone-redundant Storage (ZRS)
- Geo-redundant Storage (GRS)
- Read-access Geo-redundant Storage (RA-GRS)
- Geo-zone-redundant Storage (GZRS)
- Read-access Geo-zone-redundant Storage (RA-GZRS)



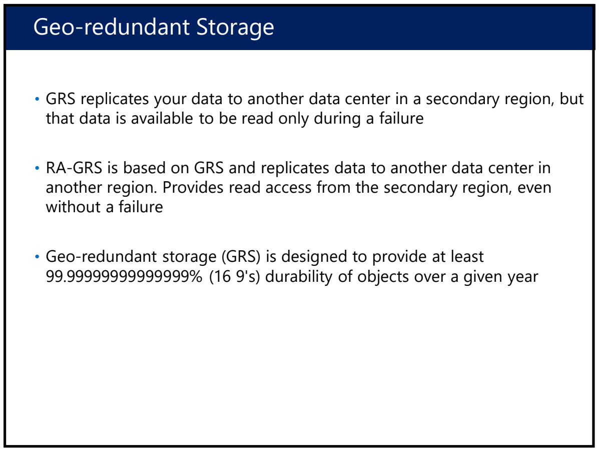
Locally-redundant Storage

- Locally redundant storage (LRS) replicates your data three times within a single data center. LRS provides at least 99.999999999% (11 nines). LRS is the lowest-cost replication option and offers the least durability compared to other options.
- If a datacenter-level disaster (for example, fire or flooding) occurs, all replicas in a storage account using LRS may be lost or unrecoverable. To mitigate this risk, Microsoft recommends using zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS).



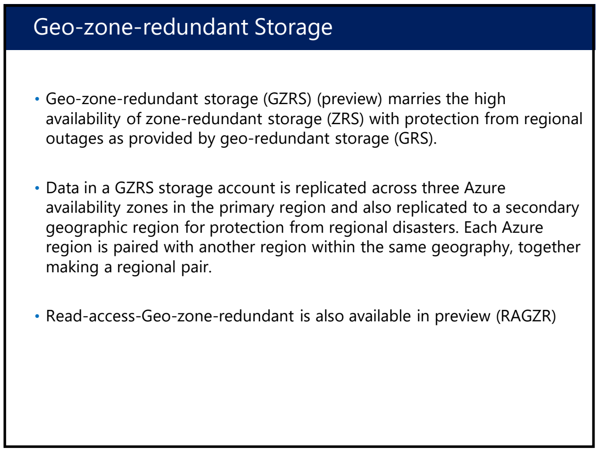
Zone-redundant Storage

- Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region. Each storage cluster is physically separated from the others and is located in its own availability zone (AZ).
- A write request to a ZRS storage account returns successfully only after the data is written to all replicas across the three clusters.
- ZRS offers durability for storage objects of at least 99.9999999999% (12 9's) over a given year



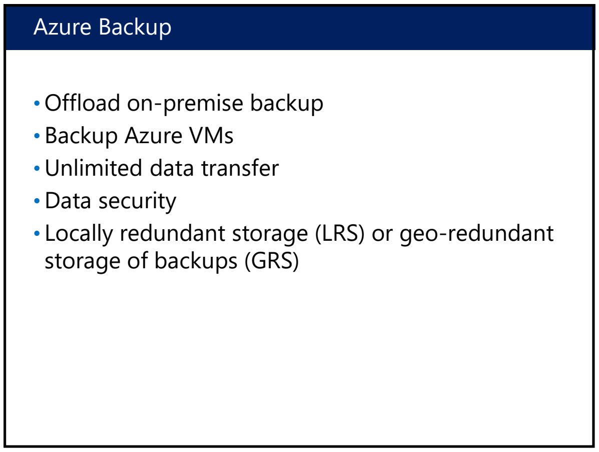
Geo-redundant Storage

- GRS replicates your data to another data center in a secondary region, but that data is available to be read only during a failure
- RA-GRS is based on GRS and replicates data to another data center in another region. Provides read access from the secondary region, even without a failure
- Geo-redundant storage (GRS) is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year



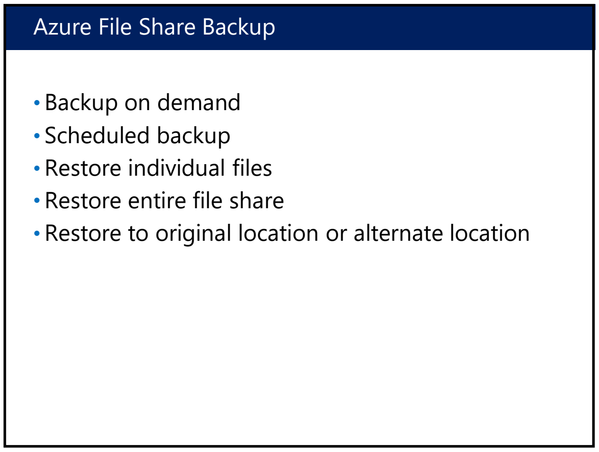
Geo-zone-redundant Storage

- Geo-zone-redundant storage (GZRS) (preview) marries the high availability of zone-redundant storage (ZRS) with protection from regional outages as provided by geo-redundant storage (GRS).
- Data in a GZRS storage account is replicated across three Azure availability zones in the primary region and also replicated to a secondary geographic region for protection from regional disasters. Each Azure region is paired with another region within the same geography, together making a regional pair.
- Read-access-Geo-zone-redundant is also available in preview (RAGZR)



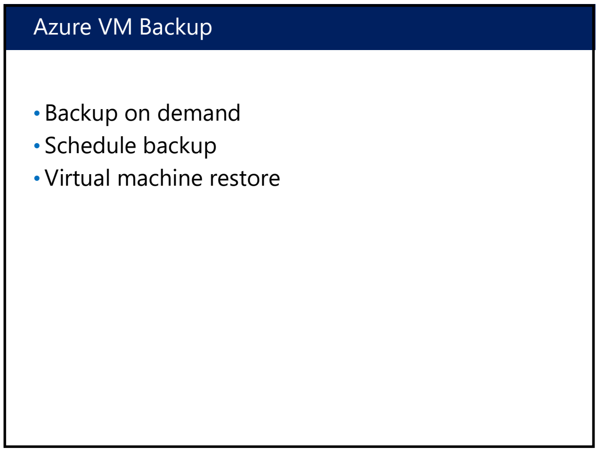
Azure Backup

- Offload on-premise backup
- Backup Azure VMs
- Unlimited data transfer
- Data security
- Locally redundant storage (LRS) or geo-redundant storage of backups (GRS)



Azure File Share Backup

- Backup on demand
- Scheduled backup
- Restore individual files
- Restore entire file share
- Restore to original location or alternate location



Azure VM Backup

- Backup on demand
- Schedule backup
- Virtual machine restore

Recovery Services Vault

On-premise backup to Azure

- Download and Install MARS agent
  - Files and Folders
  - Hyper-V virtual machines
  - Vmware virtual machines
  - SQL Servers
  - SharePoint Servers
  - Exchange Servers
  - System State
  - Bare Metal Recovery

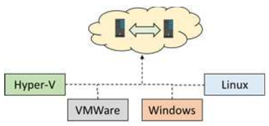
Recovery Services Vault

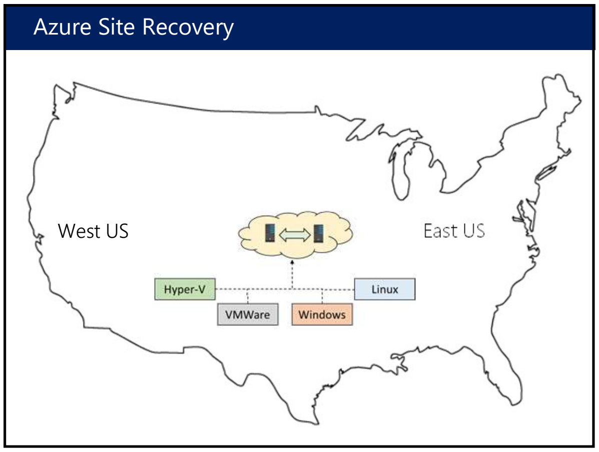
Azure Backup Items

- Virtual Machines
- Azure File Share
- SQL Server in Azure VM

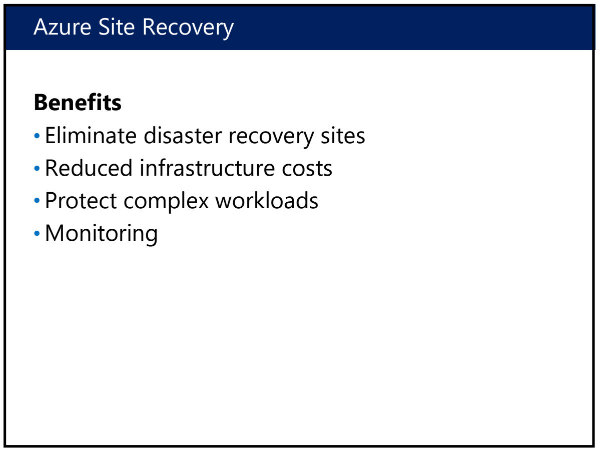
Azure Site Recovery

- Replicate Azure VMs from one Azure region to another
- Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux) to Azure
- Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site





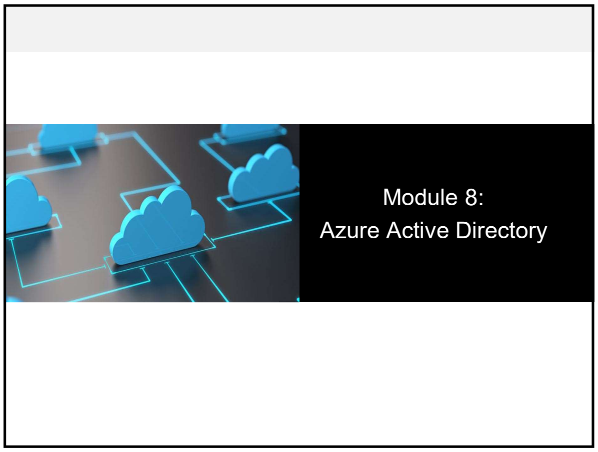
Azure Site Recovery



Azure Site Recovery

Benefits

- Eliminate disaster recovery sites
- Reduced infrastructure costs
- Protect complex workloads
- Monitoring



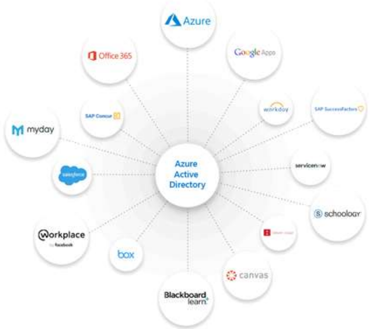
Module 8:
Azure Active Directory

Learning Objectives

What you will learn:

- The purpose of Azure Active Directory
- Azure AD Connect
- AD Join

Azure Active Directory

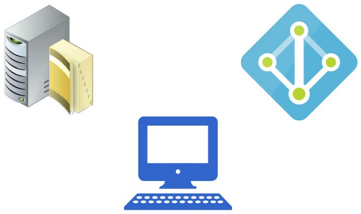


Comparing Active Directory on-premise to Azure AD

- Authentication is performed using LDAP over port 389

- Authentication is performed through a number of protocols such as SAML, WS-Federation, and OAuth. It's possible to query Azure AD but instead of using LDAP you use a REST API called AD Graph API. These all work over HTTP and HTTPS

Hybrid AD Joined Devices



- You can join personal devices to Azure AD
- Company owned/Domain joined devices can be joined to Azure AD

Multi-Factor Authentication

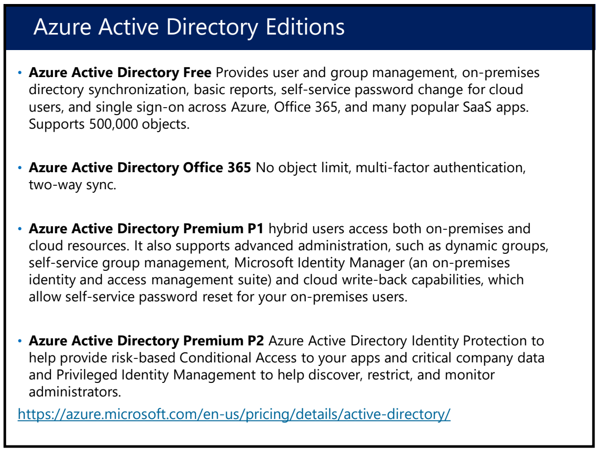
- Requires Azure AD Premium
- Global Administrators: MFA is free of charge
- Call to phone
- Text message to phone
- Mobile app notification
- Verification through mobile app
- Cache 1-60 days

Azure AD Identity Protection

Azure AD Premium 2 or Enterprise Mobility Suite (EMS)

Risk Events

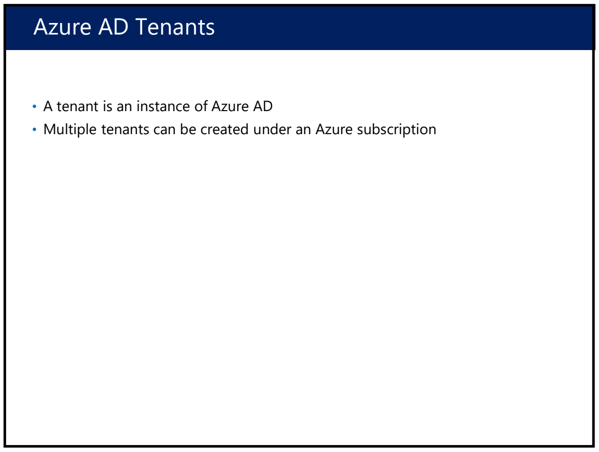
- Leaked Credentials
- Sign-in from anonymous IPs
- Impossible travel
- Sign-in from unfamiliar locations
- Sign-in from infected devices



Azure Active Directory Editions

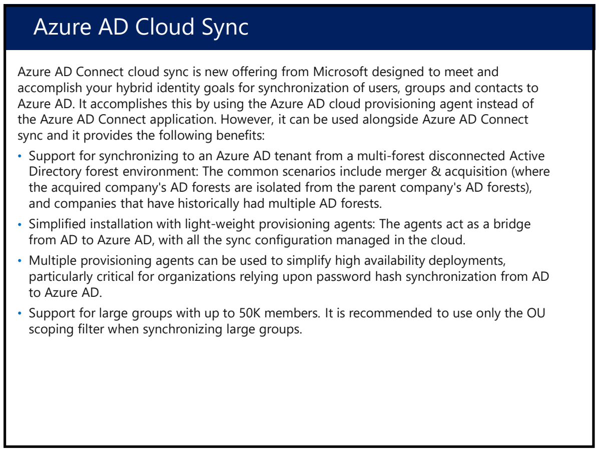
- **Azure Active Directory Free** Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Office 365, and many popular SaaS apps. Supports 500,000 objects.
- **Azure Active Directory Office 365** No object limit, multi-factor authentication, two-way sync.
- **Azure Active Directory Premium P1** hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
- **Azure Active Directory Premium P2** Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators.

https://azure.microsoft.com/en-us/pricing/details/active-directory/



Azure AD Tenants

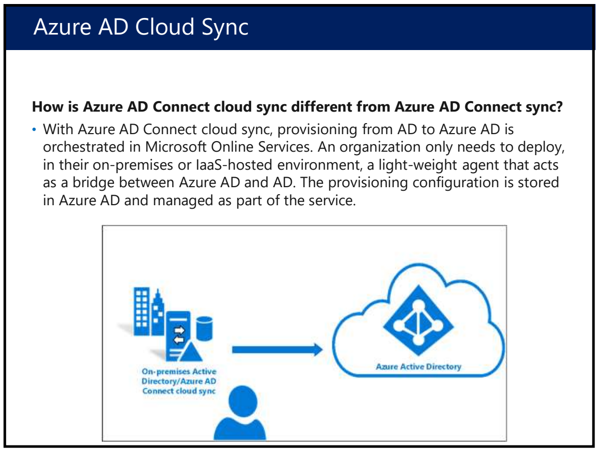
- A tenant is an instance of Azure AD
- Multiple tenants can be created under an Azure subscription



Azure AD Cloud Sync

Azure AD Connect cloud sync is new offering from Microsoft designed to meet and accomplish your hybrid identity goals for synchronization of users, groups and contacts to Azure AD. It accomplishes this by using the Azure AD cloud provisioning agent instead of the Azure AD Connect application. However, it can be used alongside Azure AD Connect sync and it provides the following benefits:

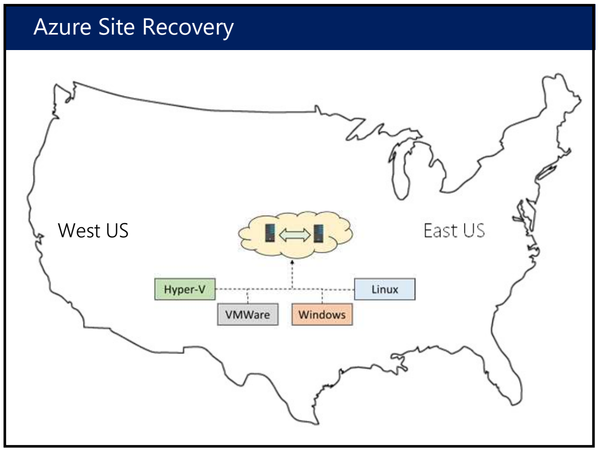
- Support for synchronizing to an Azure AD tenant from a multi-forest disconnected Active Directory forest environment: The common scenarios include merger & acquisition (where the acquired company's AD forests are isolated from the parent company's AD forests), and companies that have historically had multiple AD forests.
- Simplified installation with light-weight provisioning agents: The agents act as a bridge from AD to Azure AD, with all the sync configuration managed in the cloud.
- Multiple provisioning agents can be used to simplify high availability deployments, particularly critical for organizations relying upon password hash synchronization from AD to Azure AD.
- Support for large groups with up to 50K members. It is recommended to use only the OU scoping filter when synchronizing large groups.



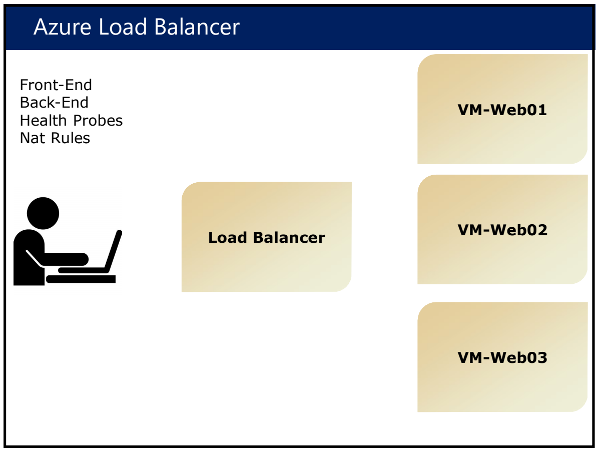
Azure AD Cloud Sync

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

- With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

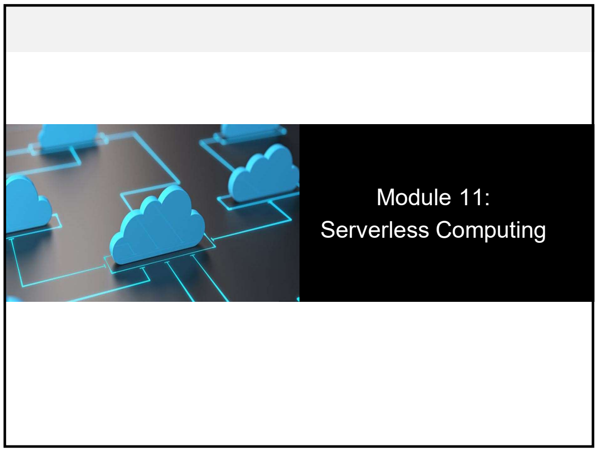


Azure Site Recovery

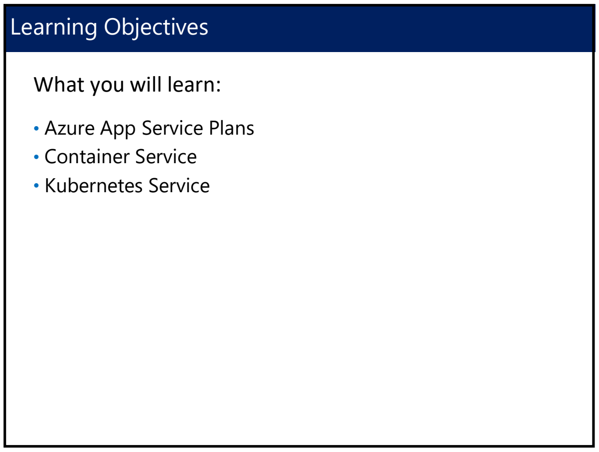


Azure Load Balancer

Front-End
Back-End
Health Probes
Nat Rules



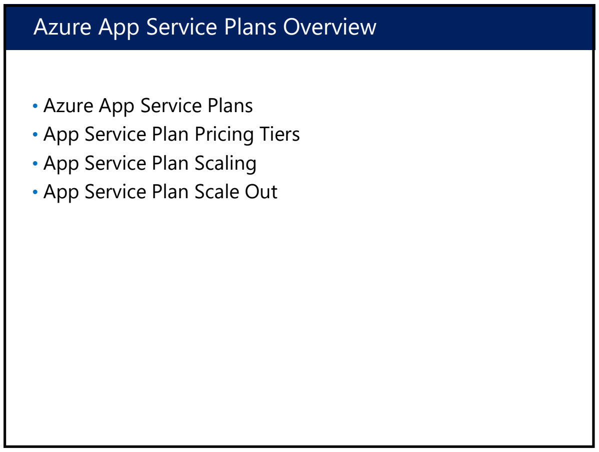
Module 11:
Serverless Computing



Learning Objectives

What you will learn:

- Azure App Service Plans
- Container Service
- Kubernetes Service



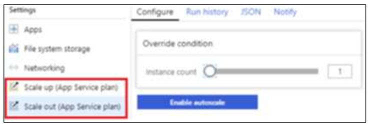
Azure App Service Plans Overview

- Azure App Service Plans
- App Service Plan Pricing Tiers
- App Service Plan Scaling
- App Service Plan Scale Out

Azure App Service Plans

- Define a set of compute resources for a web app to run
- Determines performance, price, and features
- One or more apps can be configured to run in the same App Service plan
- App Service plans define:
  - Region where compute resources will be created
  - Number of virtual machine instances
  - Size of virtual machine instances (Small, Medium, Large)
  - Pricing tier

App Service Plan Scaling

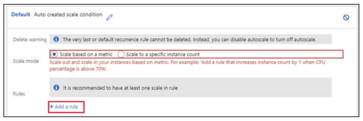


Override condition

Instance count 1

- Scale up (change the App Service plan)
  - More hardware (CPU, memory, disk)
  - More features (dedicated virtual machines, staging slots, autoscaling)
- Scale out (increase the number of VM instances)
  - Manual (fixed number of instances)
  - Autoscale (based on predefined rules and schedules)

App Service Plan Automatic Scale



Default Auto created scale condition

Delete warning: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode: ● Scale based on a metric ○ Scale to a specific instance count

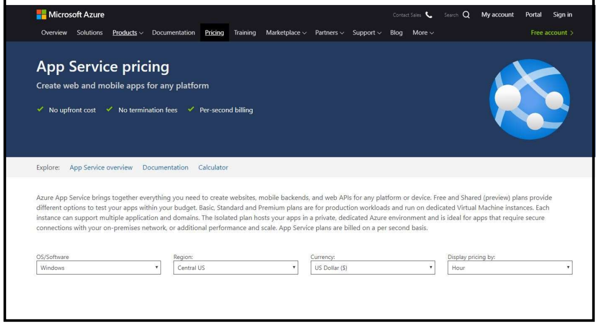
Scale out and scale in your instances based on metric. For example: 'Add a rule that increases instance count by 1 when CPU percentage is above 70%'

Rules: It is recommended to have at least one scale in rule

- Adjust available resources based on the current demand
- Improves availability and fault tolerance
- Scale based on a metric (CPU percentage, memory percentage, HTTP requests)
- Scale according to a schedule (weekdays, weekends, times, holidays)
- Can implement multiple rules – combine metrics and schedules
- Don’t forget to scale down

App Service Pricing

https://azure.microsoft.com/en-us/pricing/details/app-service/windows/



App Service pricing

Create web and mobile apps for any platform

✓ No upfront cost ✓ No termination fees ✓ Per-second billing

Explore: App Service overview Documentation Calculator

Azure App Service brings together everything you need to create websites, mobile backends, and web APIs for any platform or device. Free and Shared (preview) plans provide different options to test your apps within your budget. Basic, Standard and Premium plans are for production workloads and run on dedicated Virtual Machine instances. Each instance can support multiple application and domains. The Isolated plan hosts your apps in a private, dedicated Azure environment and is ideal for apps that require secure connections with your on-premises network, or additional performance and scale. App Service plans are billed on a per second basis.

OS/Software: Windows

Region: Central US

Currency: US Dollar ($)

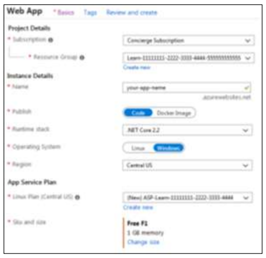
Display pricing by: Hour

Azure App Service

- Includes Web Apps API Apps, Mobile Apps, and Function apps
- Fully managed environment enabling high productivity development
- Platform-as-a-service (PaaS) offering for building and deploying highly available cloud apps for web and mobile
- Platform handles infrastructure so developers focus on core web apps and services
- Developer productivity using .NET, .NET Core, Java, Python and a host of others
- Provides enterprise-grade security and compliance

Creating an App Service

- Name must be unique
- Access using *azurewebsites.net* – can map to a custom domain
- Publish Code (Runtime Stack)
- Publish Docker Image (Image source)
- Linux or Windows
- Region closest to your users
- App Service Plan



Project Details

* Subscription: Concierge Subscription

* Resource Group: Learn-11111111-2222-3333-4444-555555555555

Create new

Instance Details

* Name: your-app-name .azurewebsites.net

* Publish: [✓ Code] Docker Image

* Runtime stack: .NET Core 2.2

* Operating System: Linux [✓ Windows]

* Region: Central US

App Service Plan

* Linux Plan (Central US): (New) ASP-Learn-11111111-2222-3333-4444

Create new

* Sku and size: Free F1 1 GB memory

Change size

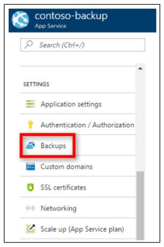
Deployment Slots

- Deploy to a different deployment slots (depends on service plan)
- Validate changes before sending to production
- Deployment slots are live apps with their own hostnames
- Avoids a cold start – eliminates downtime
- Fallback to a last known good site

Service	Slots
Free, Shared, Basic	0
Standard	Up to 5
Premium	Up to 20
Isolated	Up to 20

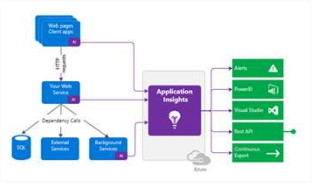
Backup an App Service

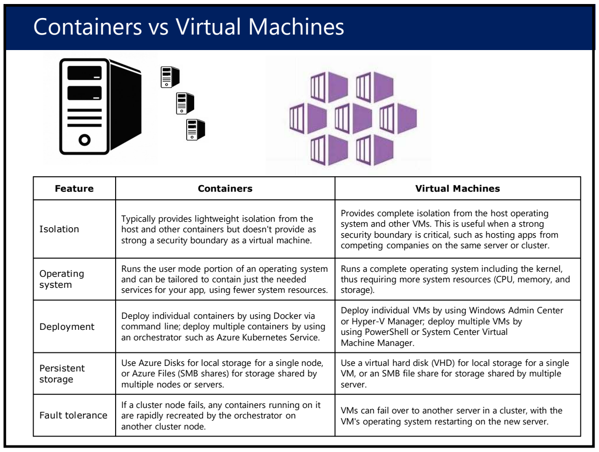
- Create app backups manually or on a schedule
- Backup the configuration, file content, and database connected to the app
- Requires Standard or Premium plan
- Backups can be up to 10 GB of app and database content
- Configure partial backups and exclude items from the backup
- Restore your app on-demand to a previous state, or create a new app



Application Insights

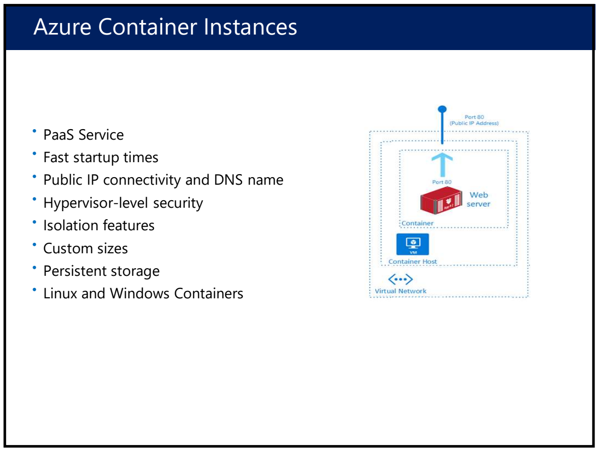
- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates
- Page views and load performance
- User and session counts
- Performance counters
- Diagnostics and Exceptions





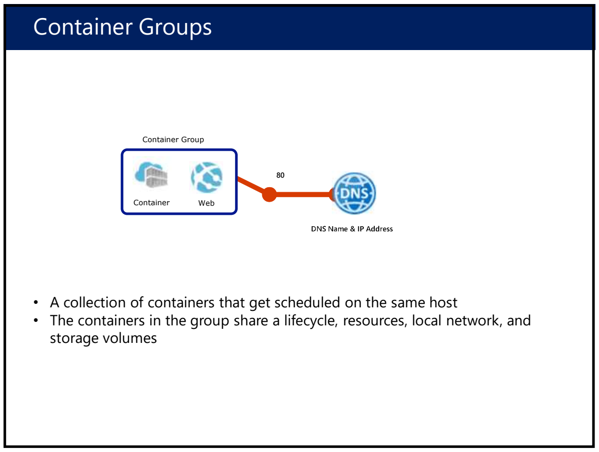
Containers vs Virtual Machines

Feature	Containers	Virtual Machines
Isolation	Typically provides lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.	Provides complete isolation from the host operating system and other VMs. This is useful when a strong security boundary is critical, such as hosting apps from competing companies on the same server or cluster.
Operating system	Runs the user mode portion of an operating system and can be tailored to contain just the needed services for your app, using fewer system resources.	Runs a complete operating system including the kernel, thus requiring more system resources (CPU, memory, and storage).
Deployment	Deploy individual containers by using Docker via command line; deploy multiple containers by using an orchestrator such as Azure Kubernetes Service.	Deploy individual VMs by using Windows Admin Center or Hyper-V Manager; deploy multiple VMs by using PowerShell or System Center Virtual Machine Manager.
Persistent storage	Use Azure Disks for local storage for a single node, or Azure Files (SMB shares) for storage shared by multiple nodes or servers.	Use a virtual hard disk (VHD) for local storage for a single VM, or an SMB file share for storage shared by multiple server.
Fault tolerance	If a cluster node fails, any containers running on it are rapidly recreated by the orchestrator on another cluster node.	VMs can fail over to another server in a cluster, with the VM's operating system restarting on the new server.



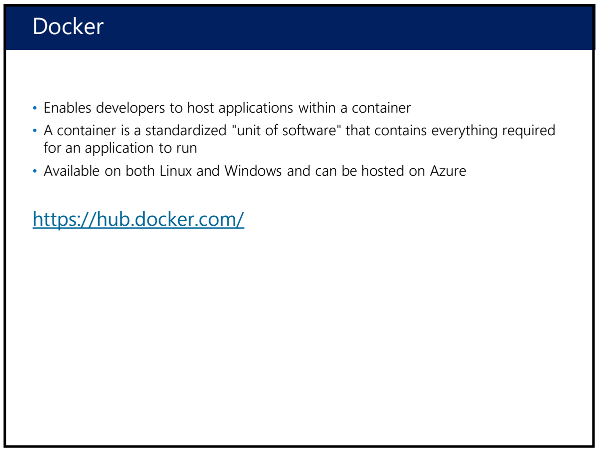
Azure Container Instances

- PaaS Service
- Fast startup times
- Public IP connectivity and DNS name
- Hypervisor-level security
- Isolation features
- Custom sizes
- Persistent storage
- Linux and Windows Containers



Container Groups

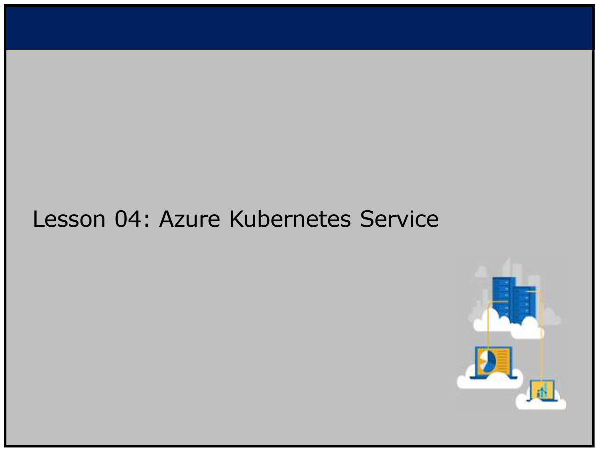
- A collection of containers that get scheduled on the same host
- The containers in the group share a lifecycle, resources, local network, and storage volumes



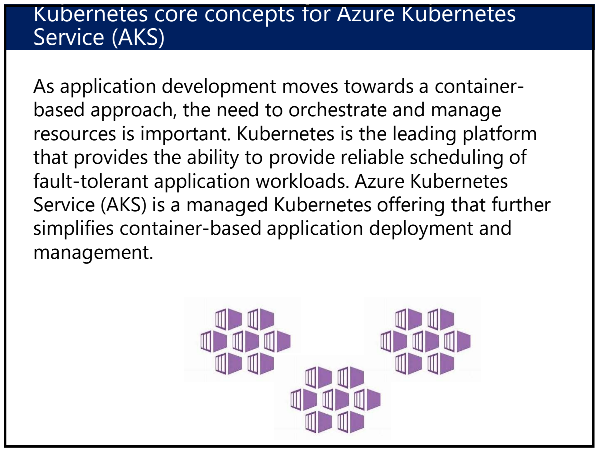
Docker

- Enables developers to host applications within a container
- A container is a standardized "unit of software" that contains everything required for an application to run
- Available on both Linux and Windows and can be hosted on Azure

https://hub.docker.com/



Lesson 04: Azure Kubernetes Service



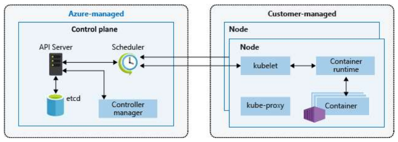
Kubernetes core concepts for Azure Kubernetes Service (AKS)

As application development moves towards a container-based approach, the need to orchestrate and manage resources is important. Kubernetes is the leading platform that provides the ability to provide reliable scheduling of fault-tolerant application workloads. Azure Kubernetes Service (AKS) is a managed Kubernetes offering that further simplifies container-based application deployment and management.

What is Kubernetes?

- Kubernetes is a rapidly evolving platform that manages container-based applications and their associated networking and storage components. The focus is on the application workloads, not the underlying infrastructure components.
- You can build and run modern, portable, microservices-based applications that benefit from Kubernetes and manage the availability of those application components.
- As an open platform, Kubernetes allows you to build your applications with your preferred programming language.
- The AKS control plane is managed by the Azure platform, and you only pay for the AKS nodes that run your applications. AKS is built on top of the open-source Azure Kubernetes Service Engine

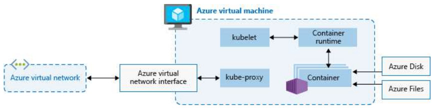
Kubernetes Cluster Architecture



The control plane includes the following core Kubernetes components:

- *kube-apiserver* - The API server is how the underlying Kubernetes APIs are exposed. This component provides the interaction for management tools, such as the Kubernetes dashboard.
- *etcd* - To maintain the state of your Kubernetes cluster and configuration, the highly available *etcd* is a key value store within Kubernetes.
- *kube-scheduler* - When you create or scale applications, the Scheduler determines what nodes can run the workload and starts them.
- *kube-controller-manager* - The Controller Manager oversees a number of smaller Controllers that perform actions such as replicating pods and handling node operations.

Kubernetes Cluster Architecture



- To run your applications and supporting services, you need a Kubernetes *node*. An AKS cluster has one or more nodes, which is an Azure virtual machine (VM) that runs the Kubernetes node components and container runtime:
- The kubelet is the Kubernetes agent that processes the requests from the control plane and scheduling of running the requested containers.
- Virtual networking is handled by the *kube-proxy* on each node. The proxy routes network traffic and manages IP addressing for services and pods.
- The *container runtime* is the component that allows containerized applications to run and interact with additional resources such as the virtual network and storage. In AKS, Moby is used as the container runtime.

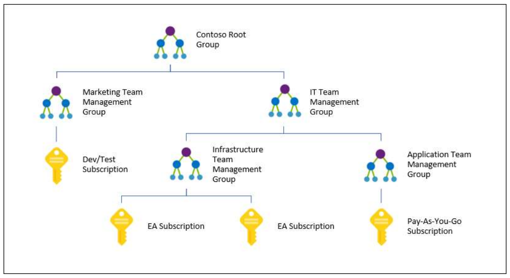
Module 9: Azure Governance and compliance

Learning Objectives

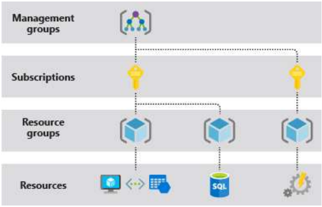
What you will learn:

- Subscription types
- Management groups
- Role based access (RBAC) control
- Azure policies

Azure Management Groups


Contoso Root Group
Marketing Team Management Group
IT Team Management Group
Dev/Test Subscription
Infrastructure Team Management Group
Application Team Management Group
EA Subscription
EA Subscription
Pay-As-You-Go Subscription

Azure Subscriptions



- Authentication is performed using LDAP ov er port 389

Azure File Sync

- .NET Framework 4.7.2 or newer
- AZ PowerShell Module
- Install Azure File Sync Agent and Register

- Storage Account
- Azure File Share
- Azure File Sync
- Define Server Endpoint

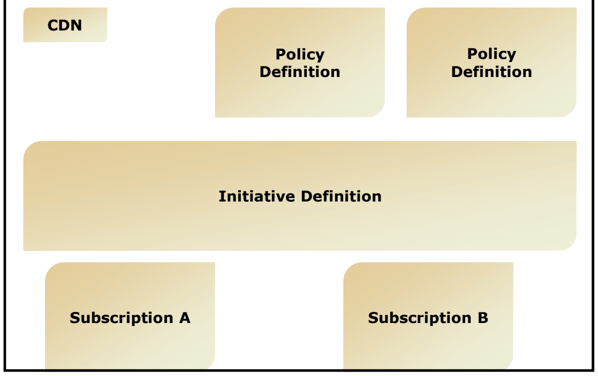
Azure AD Identity Protection

Azure AD Premium 2 or Enterprise Mobility Suite (EMS)

Risk Events

- Leaked Credentials
- Sign-in from anonymous IPs
- Impossible travel
- Sign-in from unfamiliar locations
- Sign-in from infected devices

Azure Policies



CDN

Policy Definition

Policy Definition

Initiative Definition

Subscription A

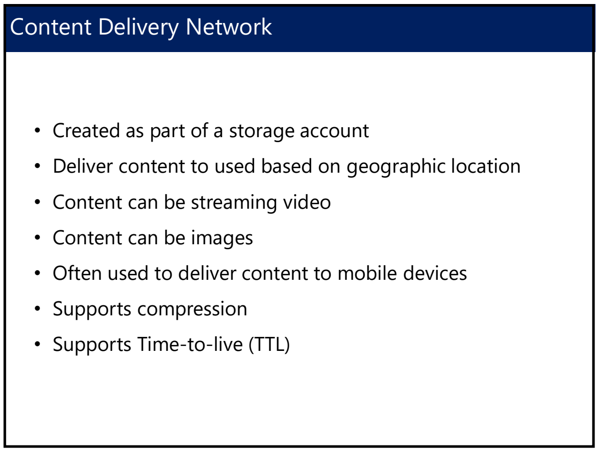
Subscription B

Module 10: Managing Data Services

Learning Objectives

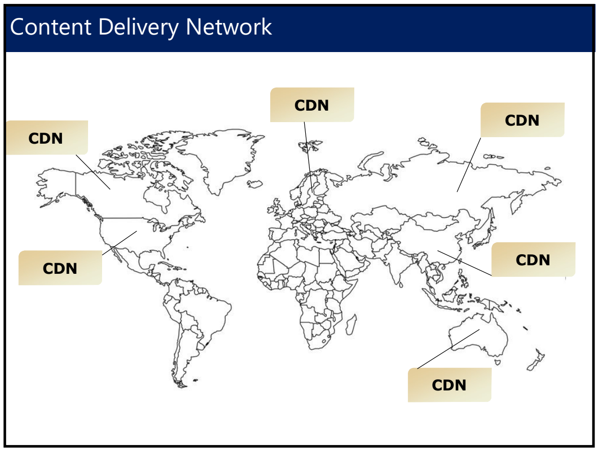
What you will learn:

- Content Deliver Networks
- Azure File Sync
- Data Box

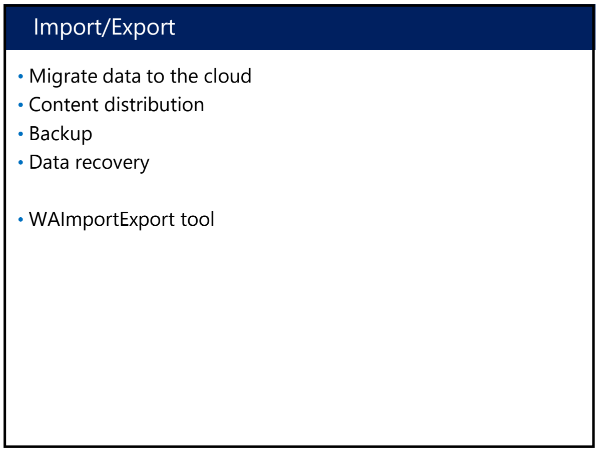


Content Delivery Network

- Created as part of a storage account
- Deliver content to used based on geographic location
- Content can be streaming video
- Content can be images
- Often used to deliver content to mobile devices
- Supports compression
- Supports Time-to-live (TTL)



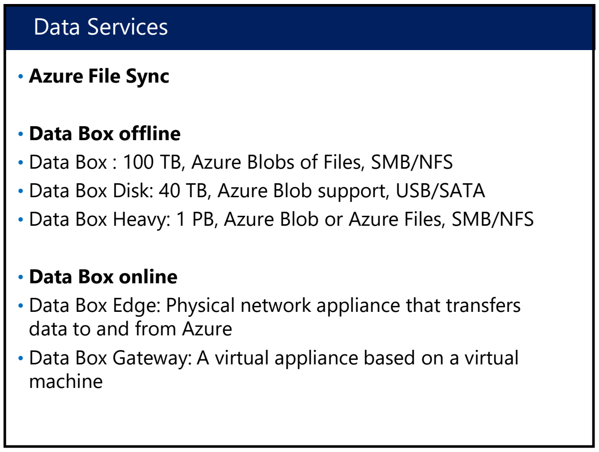
Content Delivery Network



Import/Export

- Migrate data to the cloud
- Content distribution
- Backup
- Data recovery

- WAImportExport tool



Data Services

- **Azure File Sync**

- **Data Box offline**
- Data Box : 100 TB, Azure Blobs of Files, SMB/NFS
- Data Box Disk: 40 TB, Azure Blob support, USB/SATA
- Data Box Heavy: 1 PB, Azure Blob or Azure Files, SMB/NFS

- **Data Box online**
- Data Box Edge: Physical network appliance that transfers data to and from Azure
- Data Box Gateway: A virtual appliance based on a virtual machine