



Azure Administrator Associate

EXAM: AZ-104



#1: Course Introduction

Hello! Instructor Introduction



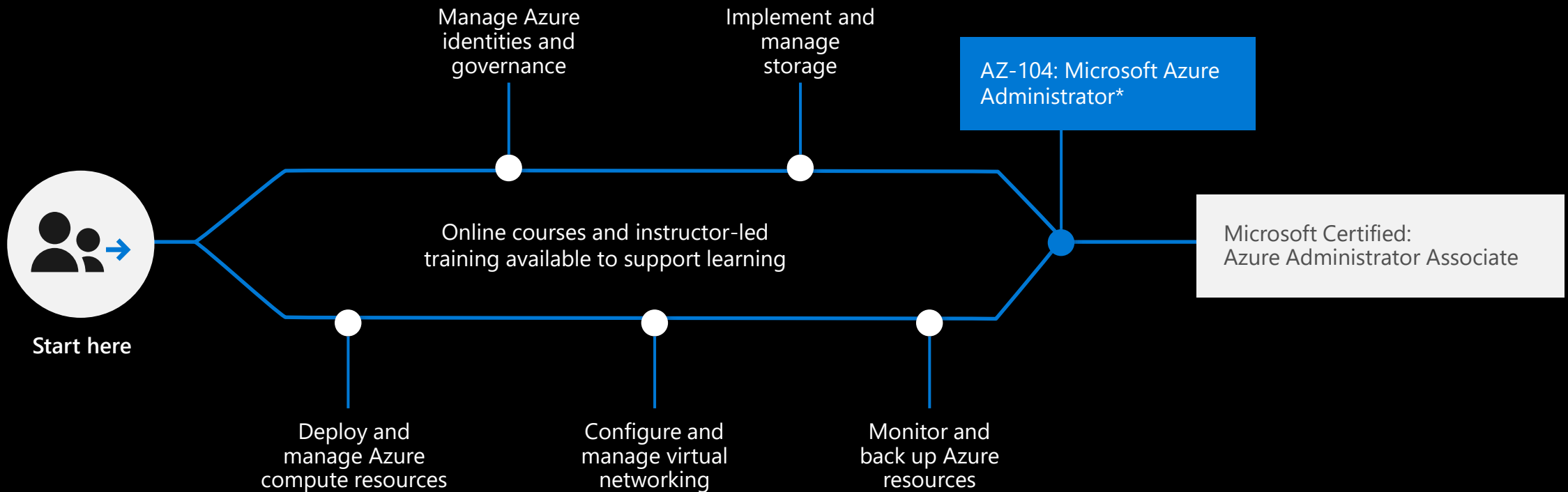
Susanth Sutteesh

Blog: AGuideToCloud.com

 [@AGuideToCloud](https://twitter.com/AGuideToCloud)



Learning path for Azure Administrator Associate



Skills Measured



Skills	Weights
Manage Azure identities and governance	15-20%
Implement and manage storage	10-15%
Deploy and manage Azure compute resources	25-30%
Configure and manage virtual networking	30-35%
Monitor and back up Azure resources	10-15%



About this Course: Course Outline

- Module 01: Identity
- Module 02: Governance and Compliance
- Module 03: Azure Administration
- Module 04: Virtual Networking
- Module 05: Intersite Connectivity
- Module 06: Network Traffic Management
- Module 07: Azure Storage
- Module 08: Azure Virtual Machines
- Module 09: Serverless Computing
- Module 10: Data Protection
- Module 11: Monitoring



40-60 questions

- Some questions worth more than 1 point
- Answer all the questions
 - *No penalty for guessing*
 - *Some questions cannot be skipped!*
- Mark items for review if you're not sure of your answer



Plan for 180 minutes

- 150 minutes to answer questions
- 30 minutes for instructions, comments, score reporting, etc.



More than just multiple-choice questions!

- Build list, hot area, active screen, drag and drop, etc.



Case Studies

- Detailed information on business and technical requirements; existing environment and other background you need to solve problems
- Requires you to understand and integrate information across multiple sources, determine what's important, and make the best decision



Microsoft Certifications (Optional)

Exam AZ-900: Microsoft Azure Fundamentals



Designed for candidates looking to demonstrate foundational level knowledge of cloud services and how those services are provided.



Microsoft Certified: Azure Administrator Associate



Designed for Azure Administrators who implement, monitor, and maintain compute, storage, network, and security.



Microsoft Certified: Azure Solutions



Architect Expert

Designed for Azure Solutions Architects who create solutions for compute, network, storage, and security.



Cloud Administrator Role

- Cloud Administrators manage the cloud services that span storage, networking and compute cloud capabilities, with a deep understanding of each service across the full IT lifecycle.
- They take end-user requests for new cloud applications and make recommendations on services to use for optimal performance and scale, as well as provision, capacity, monitor and adjust as appropriate. This role requires communicating and coordinating with vendors.
- Cloud Administrators use the Azure Portal and as they become more proficient, they use PowerShell and the Command Line Interface.
- Successful Cloud Administrators start this role with experience on operating systems, virtualization, cloud infrastructure, storage structures, and networking.



About this Course: Prerequisites

- Successful Azure Administrators start this role with experience on operating systems, virtualization, cloud infrastructure, storage structures, and networking
- Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding of network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding of Active Directory concepts, such as users, groups, and role-based access control.
- Understanding of resilience and disaster recovery, including backup and restore operations.



Azure Administrator Associate

EXAM: AZ-104



Module 01: Identity

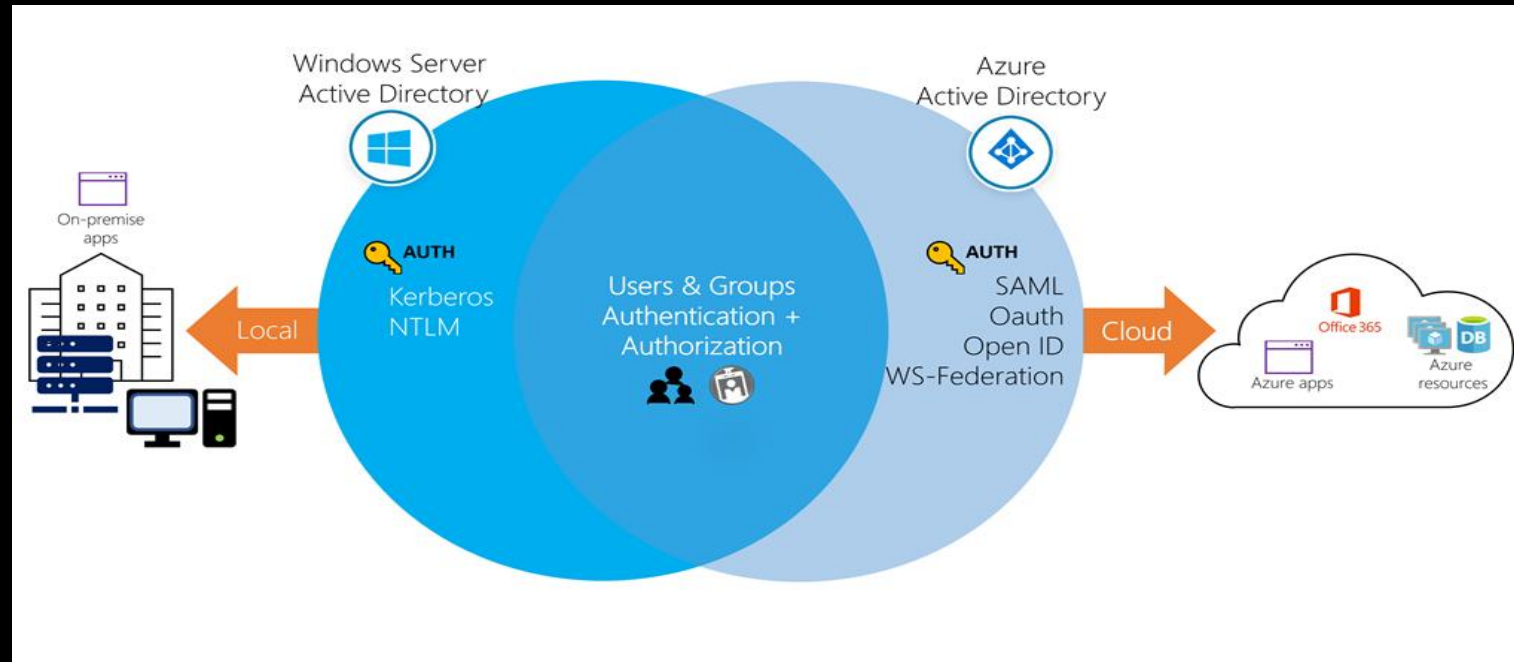
#2: Azure Active Directory



Azure Active Directory Overview

- Azure Active Directory
- Azure AD Concepts
- AD DS vs. Azure Active Directory
- Azure Active Directory Editions
- Azure AD Join
- Multi-Factor Authentication
- Self-Service Password Reset

Azure Active Directory



- A cloud-based suite of identity management capabilities that enables you to securely manage access to Azure services and resources for your users
- Provides application management, authentication, device management, and hybrid identity

Azure AD Concepts



Concept	Description
Identity	An object that can be authenticated.
Account	An identity that has data associated with it.
Azure AD Account	An identity created through Azure AD or another Microsoft cloud service.
Azure tenant	A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription.
Azure AD directory	Each Azure tenant has a dedicated and trusted Azure AD directory.
User subscription	Used to pay for Azure cloud services.

AD DS vs Azure Active Directory



- Identity Solution
- REST API Querying
- Communication Protocols
- Federation Services
- Flat structure

Azure Active Directory Editions

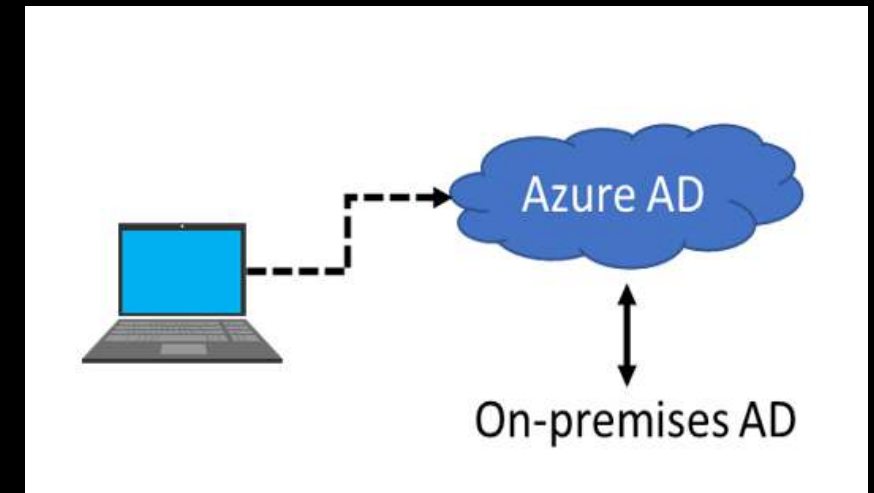


Feature	Free	Office 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Up to 10 apps	Up to 10 apps	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X



Azure AD Join

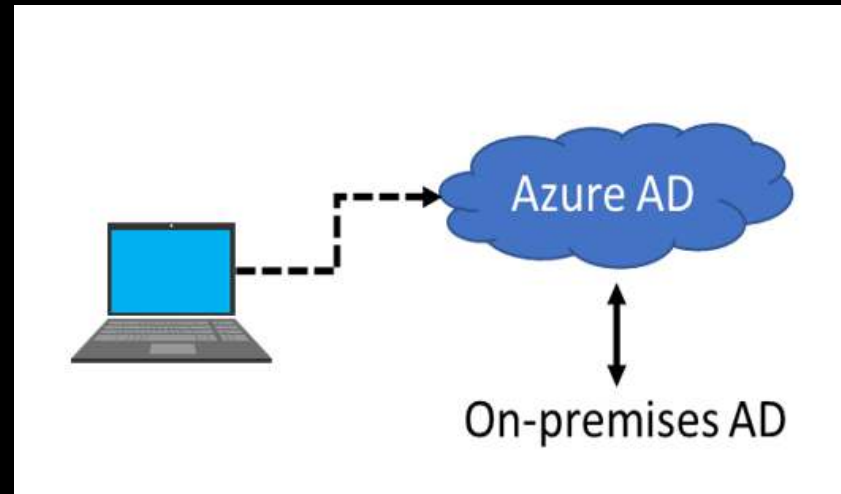
- Single-Sign-On to your Azure managed SaaS apps and services
- Enterprise compliant roaming of user settings across joined devices
- Access to Microsoft Store for Business
- Windows Hello support
- Restriction of access to apps from only compliant devices
- Seamless access to on-premise resources





Azure AD Join

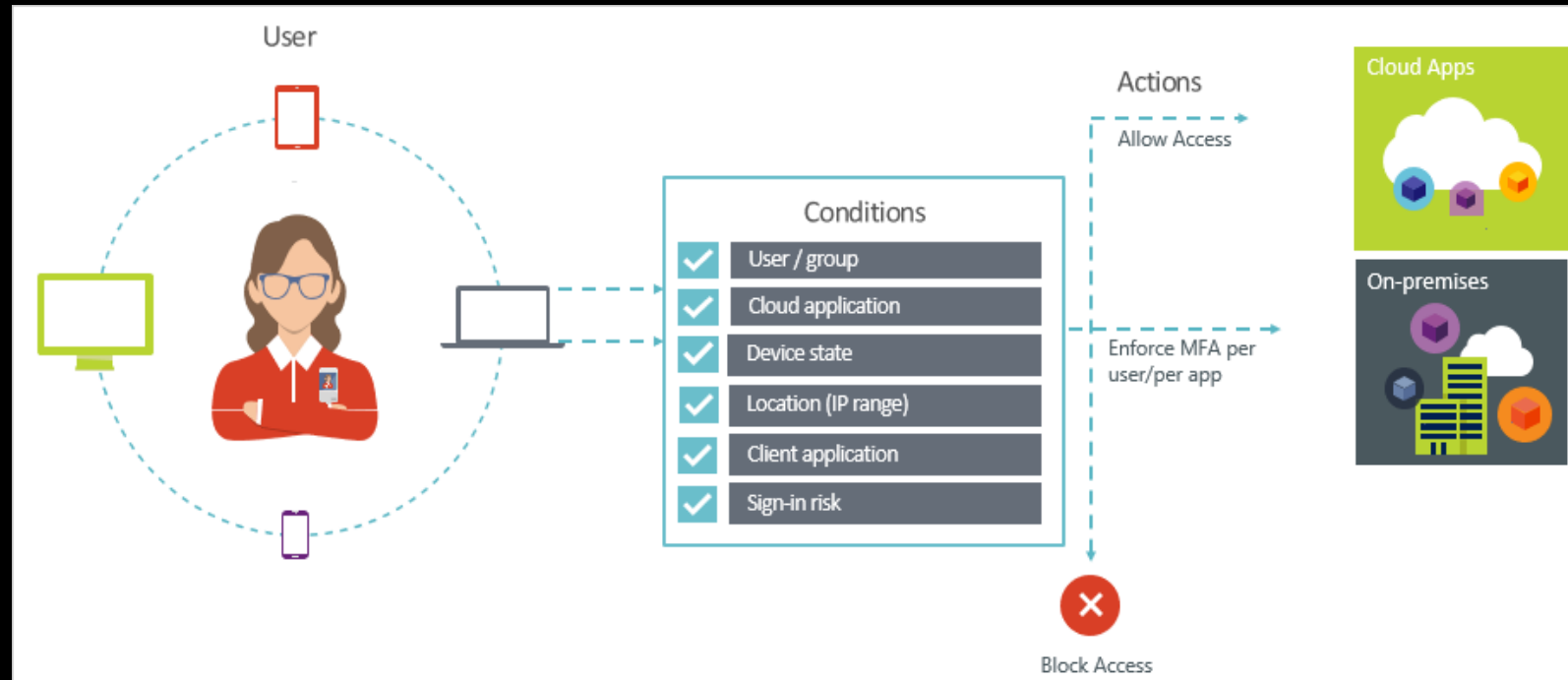
Connection options



- Registering
- Joining



Multi-Factor Authentication



- Conditions – “When this happens”
- Access controls – “Then do this”

- Provides two step authentication verification
- Lets you enforce controls on access to apps based on specific conditions

Self-Service Password Reset



1. Determine who can use self-service password reset
2. Choose the number of authentication methods required and the methods available (email, phone, questions)
3. You can require users to register for SSPR (same process as MFA)

Password reset - Authentication methods
mitaric (Default Directory) - Azure Active Directory

Save Discard

Diagnose and solve problems

Manage

- 1 Properties
- 2 Authentication methods
- 3 Registration

Notifications
Customization
On-premises integration

Activity

Audit logs
Usage & insights

Troubleshooting + Support

New support request

Number of methods required to reset ⓘ
1 2

Methods available to users

Mobile app notification
 Mobile app code
 Email
 Mobile phone
 Office phone
 Security questions

Number of questions required to register ⓘ
3 4 5

Number of questions required to reset ⓘ
3 4 5

Select security questions
5 security questions selected



Azure Administrator Associate

EXAM: AZ-104



Module 01: Identity

#3: Users and Groups








Users and Groups Overview

- User Accounts
- Managing User Accounts
- Bulk User Accounts
- Group Accounts
- Azure AD Connect
- Azure AD Connect Health
- Azure AD B2B and B2C
- Demonstration – Users and Groups

User Accounts



Name	User name	User type	Source
<input type="checkbox"/>  Ziulla	ziaulla@mac...	Guest	External Azure Active Directory
<input type="checkbox"/>  Retail Crisis Notificati	rscrisis@mic...	Member	Windows Server AD
<input type="checkbox"/>  "Planning & Launch Se	plsoem@mi...		Windows Server AD
<input type="checkbox"/>  'amckenziecec	'amckenziec...	Guest	Invited user
<input type="checkbox"/>  'Evento FY20 Colombia	kickcolo@mi...	Member	Windows Server AD

- All users must have an account
- The account is used for authentication and authorization
- Identity Sources: Cloud, Directory-synchronized, and Guest



Managing User Accounts

+ New user + New guest user ↑ Bulk create ↑ Bulk invite ↑ Bulk delete ↓ Download users ↻ Refresh 🔑 Reset password ↗ Multi-Factor Authentication ...

- Must be Global Administrator or User Administrator to manage users
- User profile (picture, job, contact info) is optional
- Deleted users can be restored for 30 days
- Sign in and audit log information is available

New user

Microsoft

Create user

Create a new user in your organization. This user will have a user name like `alice@Microsoft.onmicrosoft.com`.

[I want to create users in bulk](#)

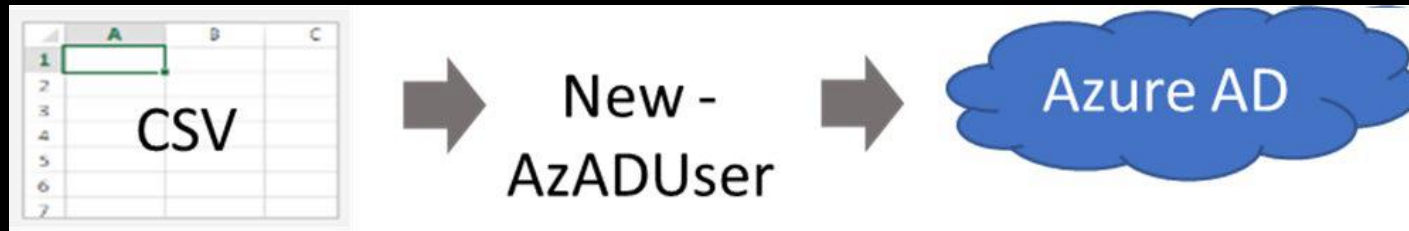
Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

[I want to invite guest users in bulk](#)



Bulk User Accounts



- Create the comma-separated values (CSV) file with the list of all the users and their properties
- Loop through the file processing each user
- Consider error handling, duplicate users, initial password settings, empty properties, and when the account is enabled



Group Accounts

Group Types

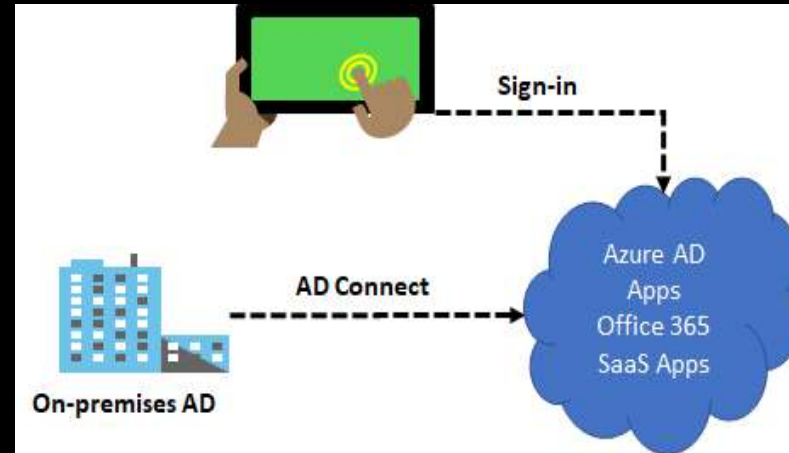
- Security groups
- Office 365 groups

Search groups		+ Add filters		
Name	↑↓	Group Type	Membership Type	
<input type="checkbox"/>	MA	Managers	Security	Assigned
<input type="checkbox"/>	VM	Virtual Machine Administrators	Security	Assigned
<input type="checkbox"/>	VN	Virtual Network Administrators	Security	Assigned

Assignment Types

- Assigned
- Dynamic User
- Dynamic Device (Security groups only)

Azure AD Connect

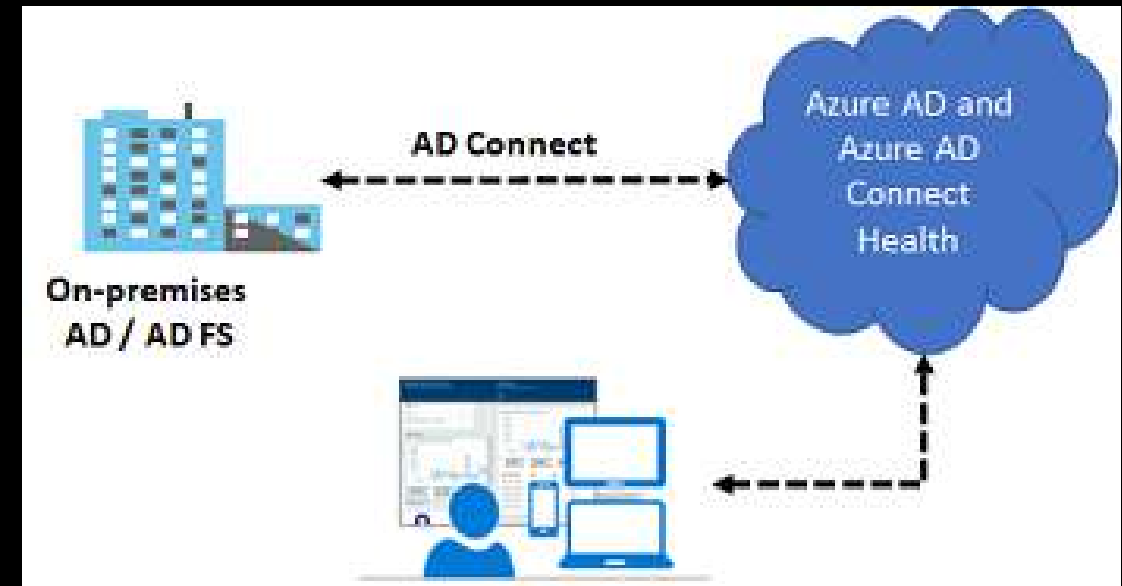


- Integrate your on-premises directories with Azure Active Directory
- Provides a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD
- There are several authentication options – password hash synchronization and pass-through authentication



Azure AD Connect Health

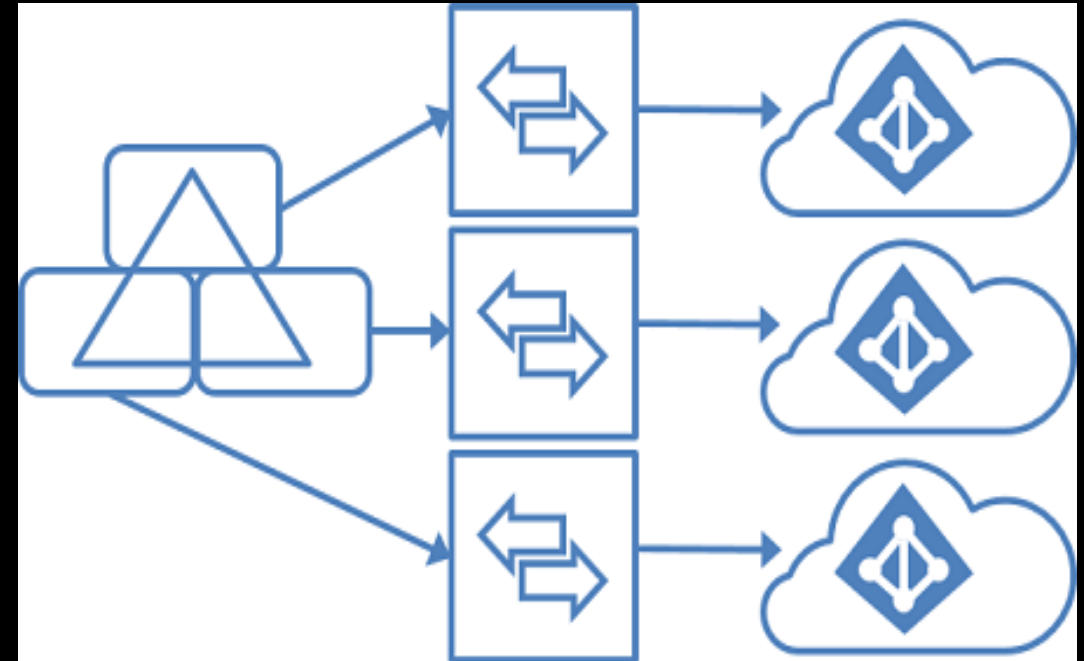
- Monitor and gain insights into AD FS servers, Azure AD Connect, and AD domain controllers
- Monitor and gain insights into the synchronizations that occur between your on-premises AD DS and Azure AD
- Monitor and gain insights into your on-premises identity infrastructure that is used to access Office 365 or other Azure AD applications





Managing Multiple Directories

- In Azure Active Directory (Azure AD), each tenant is a fully independent resource
- There is no parent-child relationship between tenants
- This independence between tenants includes resource, administrative, and synchronization



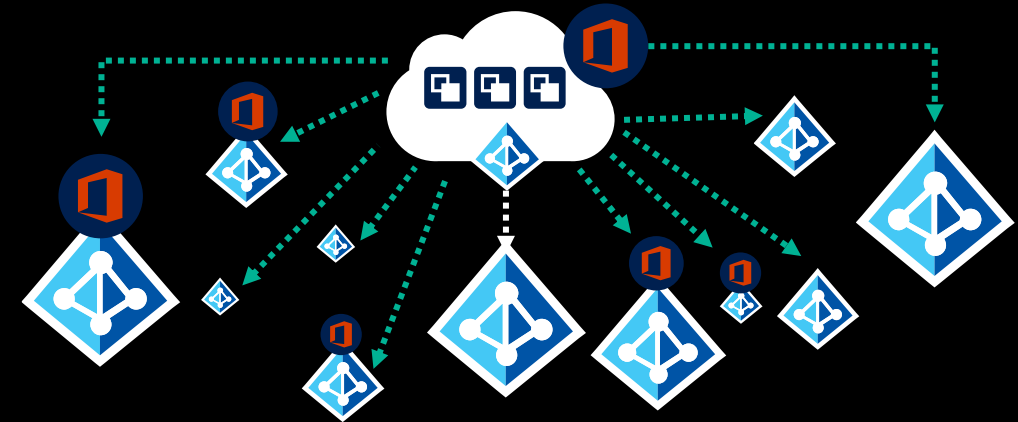
✓ It is recommended to use a supported synchronization configuration



Azure AD B2B and B2C

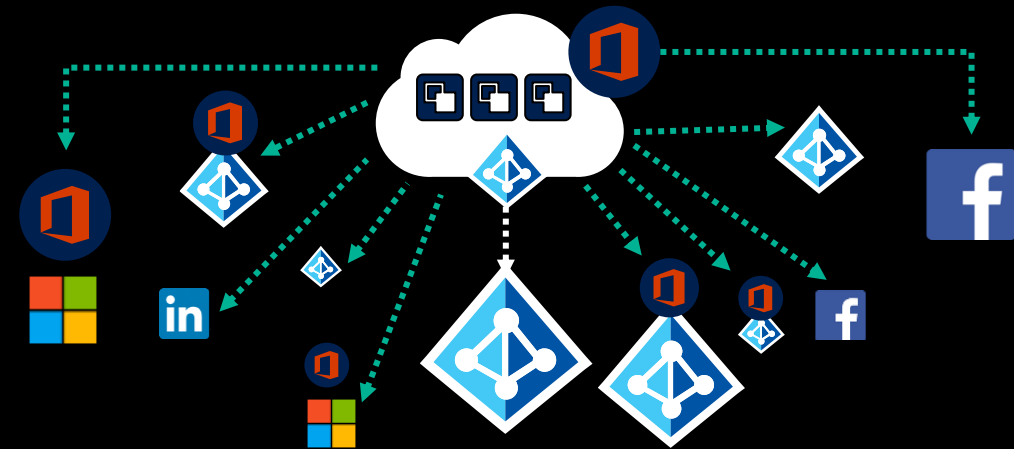
Business to Business (B2B)

- Inviting users from other Azure AD Tenants into your own organization tenant
- User provisioning is done by the invited party



Business to Customer (B2C)

- Inviting users from other social media Identity Tenants into your own organization tenant
- User provisioning is done by the invited party; you are in control to invite the other side's users





Azure Administrator Associate

EXAM: AZ-104



Module 01: Identity

#4: Review Questions



Review Question 1

Your users want to sign-in to devices, apps, and services from anywhere. They want to sign-in using an organizational work or school account instead of a personal account. You must ensure corporate assets are protected and that devices meet standards for security and compliance. Specifically, you need to be able to enable or disable a device. What should you do? Select one.

- Enable the device in Azure AD.
- Join the device to Azure AD.
- Connect the device to Azure AD.
- Register the device with Azure AD.



Review Question 2

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com and an Azure Active Directory (Azure AD) domain named contoso.onmicrosoft.com. Azure AD Connect is installed and Active Directory Federation Services (AD FS) is configured. Password-writeback is enabled. You need to monitor synchronization events generated by Azure AD Connect. Select one

- Install Azure AD Connect Health.
- Deploy a domain controller for contoso.com on a virtual machine in the contoso.onmicrosoft.com tenant.
- Configure Authentication Caching.
- Launch Synchronization Service Manager and edit the properties of the connector.



Review Question 3

Identify three differences from the following list between Azure Active Directory (AD) and Active Directory Domain Services (AD DS). Select three.

- Azure AD uses HTTP and HTTPS communications
- Azure AD uses Kerberos authentication
- There are no Organizational Units (OUs) or Group Policy Objects (GPOs) in Azure AD
- Azure AD includes Federation Services
- Azure AD can be queried through LDAP



Review Question 4

You would like to add a user who has a Microsoft account to your subscription. Which type of user account is this? Select one.

- Cloud identity
- Directory-Synchronized
- Provider identity
- Guest User
- Hosted identity



Review Question 5

You are configuring Self-service Password Reset. Which of the following is not a validation method? Select one.

- An email notification.
- A text or code sent to a user's mobile or office phone.
- A paging service.
- A set of security questions



Review Question 6

You are assigning Azure AD roles. Which role will allow the user to manage all the groups in your Teams tenants and be able to assign other administrator roles? Select one.

- Global administrator
- Password administrator
- Security administrator
- User administrator



Azure Administrator Associate

EXAM: AZ-104



Module 02: Governance and Compliance

#5: Subscriptions and Accounts



Subscriptions and Accounts Overview

- Regions
- Azure Subscriptions
- Getting a Subscription
- Subscription Usage
- Cost Management
- Resource Tags
- Cost Savings

Regions



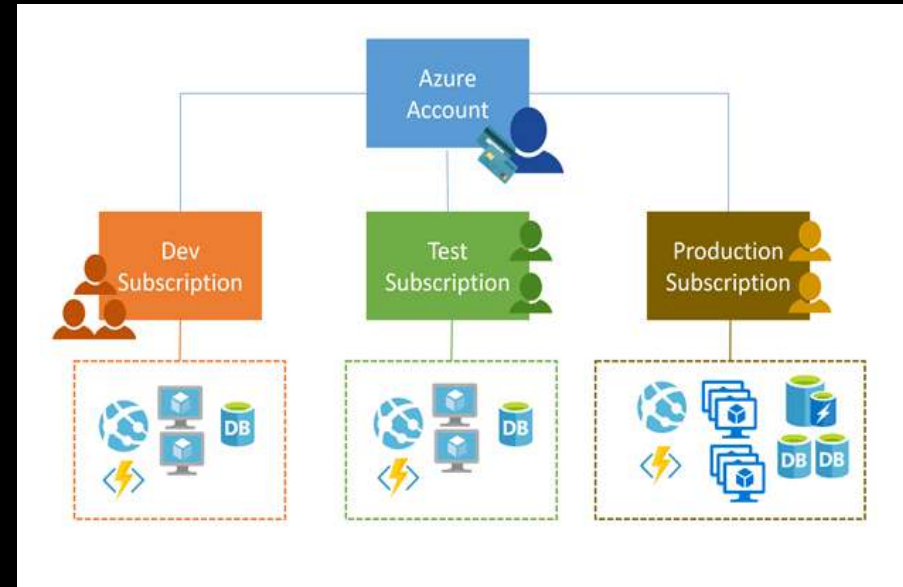
Worldwide there are
50+ regions
representing 140
countries



- A region represents a collection of datacenters
- Provides flexibility and scale
- Preserves data residency
- Select regions close to your users
- Be aware of region deployment availability
- There are global services that are region independent
- Regions are paired for high availability



Azure Subscriptions



- Logical unit of Azure services that is linked to an Azure account
- Security and billing boundary
- Includes accounts - identities in Azure Active Directory (Azure AD) or in a directory that is trusted by Azure AD, such as a work or school organization



Getting a Subscription

- Enterprise Agreement customers make an upfront monetary commitment and consume services throughout the year
- Resellers provide a simple, flexible way to purchase cloud services
- Partners can design and implement your Azure cloud solution
- Personal free account -start right away



Subscription Usage

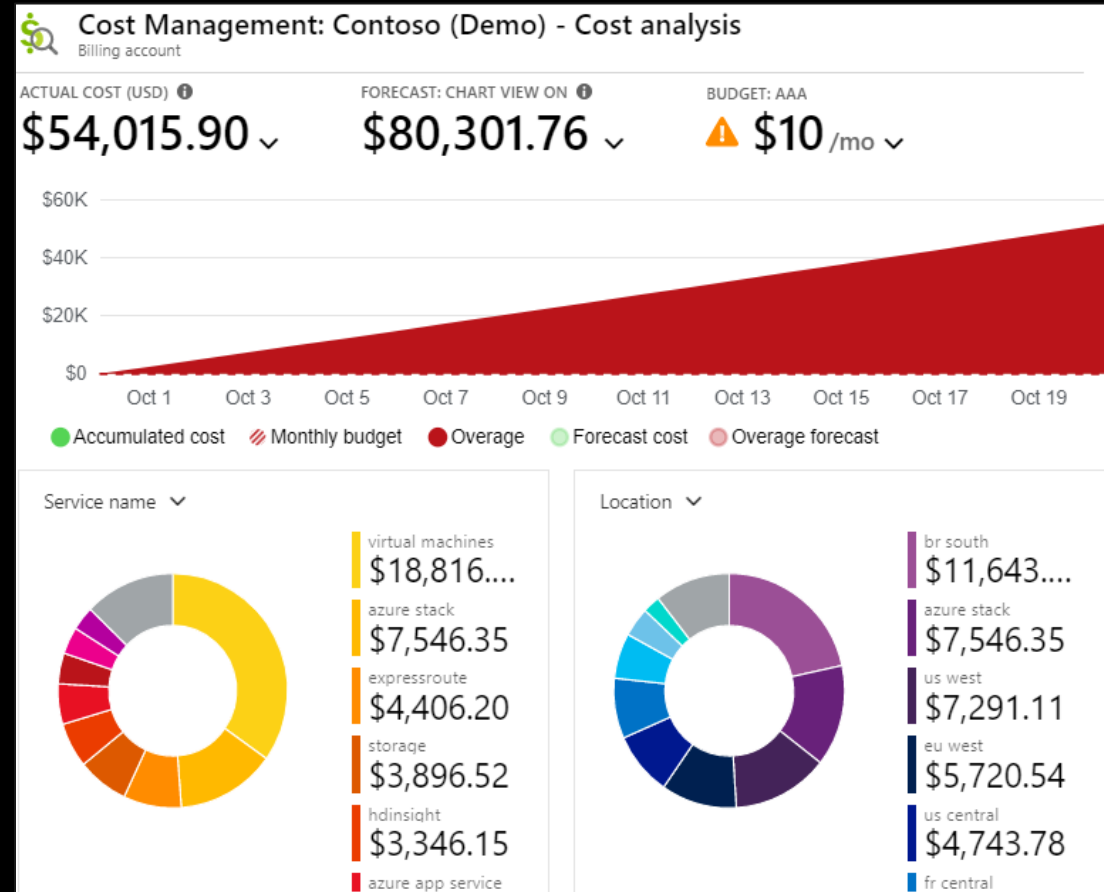


Subscription	Usage
Free	Includes a \$200 credit for the first 30 days, free limited access for 12 months
Pay-As-You-Go	Charges you monthly
Enterprise	One agreement, with discounts for new licenses and Software Assurance - targeted at enterprise-scale organizations.
Student	Includes \$100 for 12 months – must verify student access

Cost Management



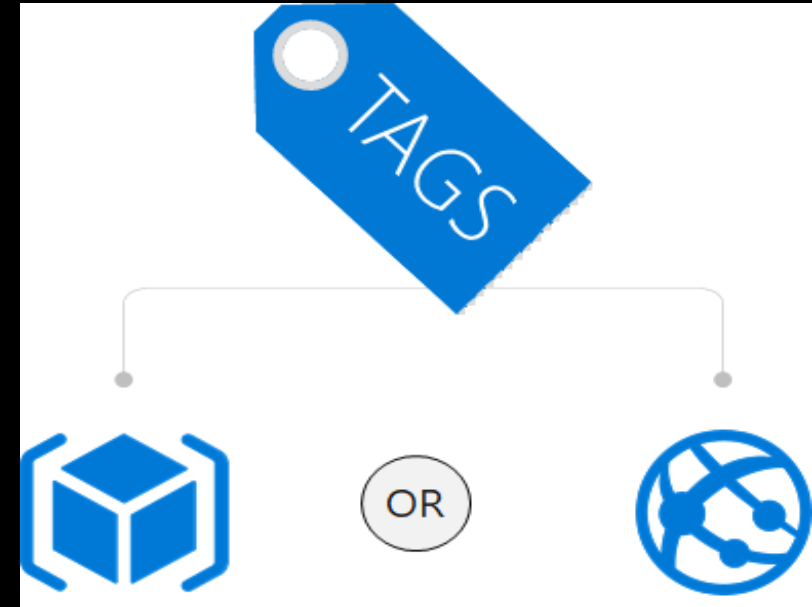
- Conduct cost analysis
- Create a budget
- Review recommendations
- Export the data





Resource Tags

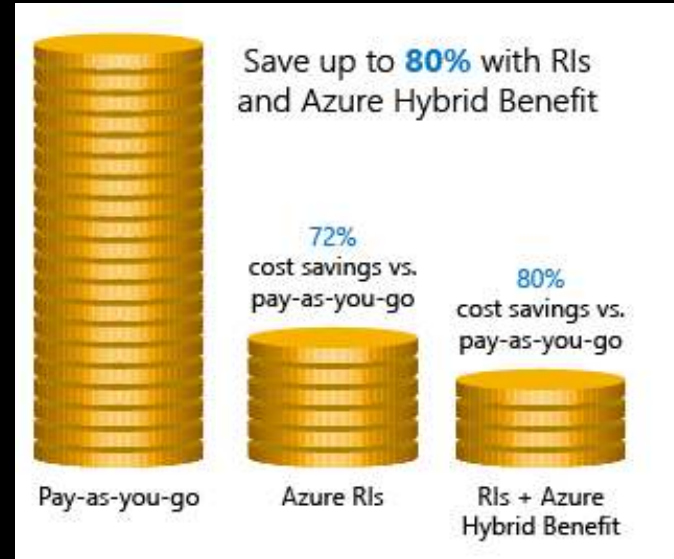
- Provides metadata for your Azure resources
- Logically organizes resources into a taxonomy
- Consists of a name-value pair
- Very useful for rolling up billing information



owner: joe
department: marketing
environment: production

cost-center: marketing

Cost Savings



- Azure Reservations - helps you save money by pre-paying for services
- Azure Hybrid Benefits - use Windows Server and SQL Server on-premises licenses with Software Assurance
- Azure Credits - monthly credit benefit that allows you to experiment with, develop, and test new solutions on Azure
- Regions - Choose low-cost locations and regions



Azure Administrator Associate

EXAM: AZ-104



Module 02: Governance and Compliance

#6: Azure Policy

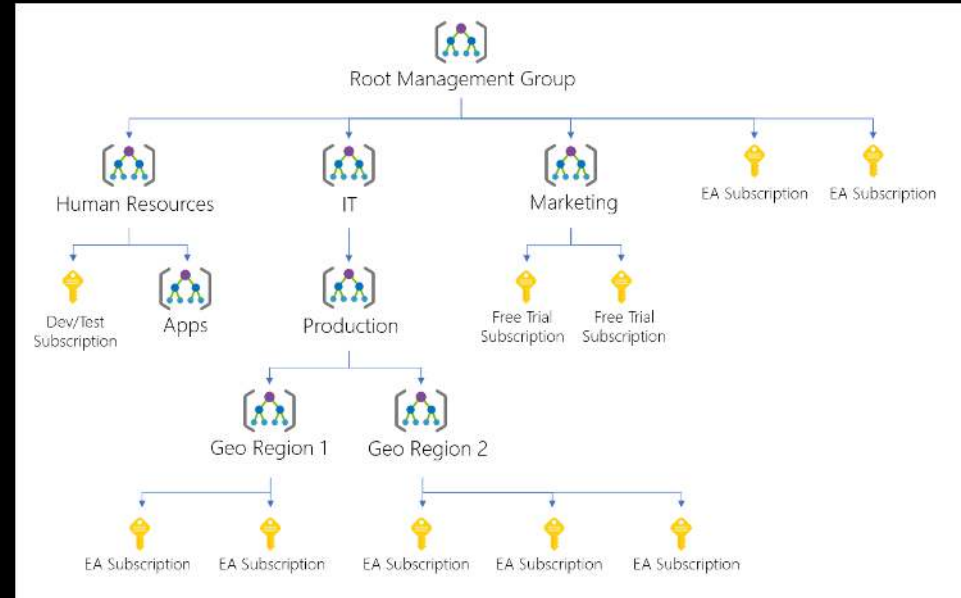


Azure Policy Overview

- Management Groups
- Azure Policy
- Implementing Azure Policy
- Policy Definitions
- Create Initiative Definitions
- Scope the Initiative Definition
- Determine Compliance
- Demonstration – Azure Policy



Management Groups



- Provides a level of scope above subscriptions
- Targeting of policies and spend budgets across subscriptions and inheritance down the hierarchies
- Compliance and cost reporting by organization (business/teams)



Azure Policy

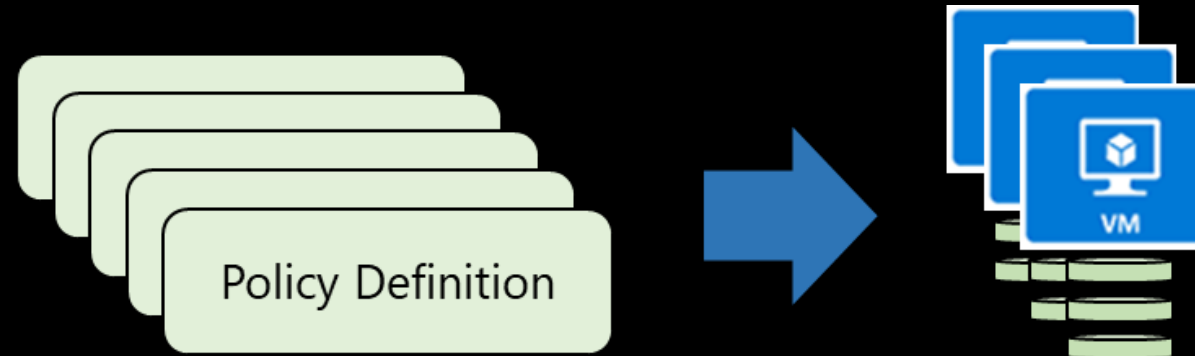
Usage Cases
Allowed resource types
Allowed virtual machine
Allowed locations
Require tag and its value
Azure Backup should be enabled for Virtual Machines

Advantages:

- Enforcement and compliance
- Apply policies at scale
- Remediation

- Azure Policy is a service in Azure that you use to create, assign and, manage policies
- Azure Policy runs evaluations and scans for non-compliant resources

Implementing Azure Policy



1. Browse Policy Definitions
2. Create Initiative Definitions
3. Scope the Initiative Definition
4. View Policy evaluation results



Policy Definitions

- Many policy definitions are available
- You can import policies from GitHub
- Policy Definitions have a specific JSON format
- You can create custom policy definitions

Policy definition
New Policy definition

BASICS

Definition location *
Visual Studio Enterprise

Name * ⓘ
Github Sample Policy

Description
A sample policy from Github.

Category ⓘ
 Create new Use existing
Category

POLICY RULE
[↓ Import sample policy definition from GitHub](#)

Create Initiative Definitions



- Group policy definitions
- Include one or more policies
- Requires planning

Initiative definition
New Initiative definition

BASICS

Definition location *
Visual Studio Enterprise ...

Name * ⓘ
East Region ✓

Description ⓘ
East Region Initiative Definition

Category ⓘ
 Create new Use existing
General ▼

namingPolicyDefinition	Policy to specify allowed naming convention	Custom	Delete
regionPolicyDefinition	Policy to allow resource creation only in certain regions	Custom	Delete



Scope the Initiative Definition

Policy - Assignments

Search (Ctrl+/) << Assign initiative Assign policy Refresh

Scope: Visual Studio Enterprise Definition type: All definition types Search: Filter by name or id... Category: All categories

Total Assignments: 2 Initiative Assignments: 2 Policy Assignments: 0

name	Scope	Type	Policies	Category
East Region	Visual Studio Enterprise	Initiative	2	General
ASC Default (subscription: ...)	Visual Studio Enterprise	Initiative	96	Security Center

- Assign the definition to a scope
- The scope enforces the policy
- Select the subscription, and optionally the resource group

Determine Compliance



Policy - Compliance

Search (Ctrl+/) <<

Assign policy Assign initiative Refresh

Scope: Visual Studio Enterprise Type: All definition types Compliance state: All compliance states Search: Filter by name or id...

Overall resource compliance 98% (159 out of 162) Non-compliant initiatives 1 out of 2 Non-compliant policies 12 out of 98 Non-compliant resources 3 out of 162

Name	Scope	Compliance state	Resource compli...	Non-Compliant Resources	Non-compliant policies
ASC Default (subscription: 957...)	Visual Studio Enterprise	Non-compliant	98% (159 out of 162)	3	12
East Region	Visual Studio Enterprise	Not started	100% (0 out of 0)	0	0

- Non-compliant initiatives
- Non-compliant policies
- Non-compliant resources



Demonstration – Azure Policy

- Assign a policy
- Create and assign an initiative definition
- Check for compliance
- Check for remediation tasks
- Remove your policy and initiative



Azure Administrator Associate

EXAM: AZ-104



Module 02: Governance and Compliance

#7: Role-Based Access Control



Role-Based Access Control Overview

- Role-Based Access Control
- Role Definition
- Role Assignment
- Azure RBAC Roles vs Azure AD Administrator Roles
- RBAC Authentication
- Azure RBAC Roles
- Demonstration – RBAC Roles



Role-Based Access Control

Provides fine-grained access management of resources in Azure

- Built on Azure Resource Manager
- Segregate duties within your team
- Grant only the amount of access to users that they need to perform their jobs

Concepts

- Security principal.
- Role definition.
- Scope.
- Assignment.



Role Definition

Collection of permissions that lists the operations that can be performed

Contributor

Owner
Contributor
 Reader
 ...
 Backup Operator
 Security Reader
 User Access Administrator
 Virtual Machine Contributor

Built-in

Reader Support Tickets
 Virtual Machine Operator

Custom

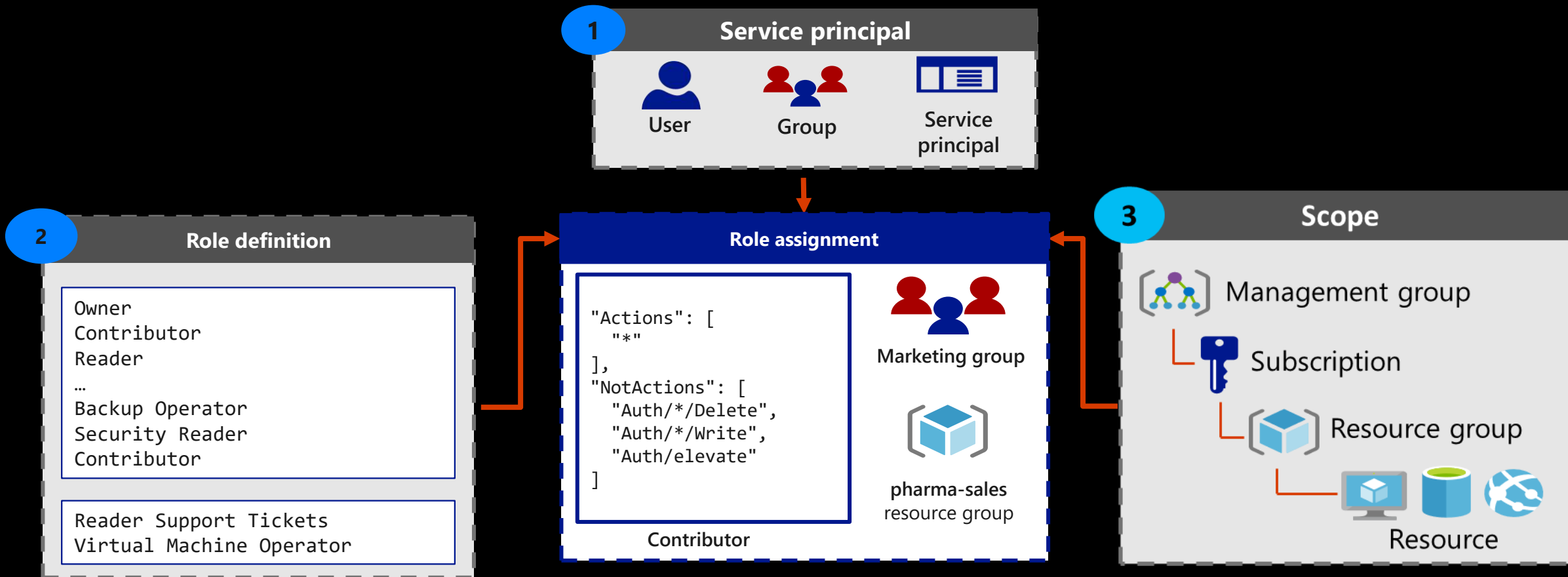
```

Actions": [
  "*"
],
"NotActions" : [
  "Authorization/*/Delete",
  "Authorization/*/Write",
  "Authorization/elevateAccess/Action"
],
"DataActions" : [],
"NotDataActions": [],
"AssignableScopes" : [
  "/"
]
  
```



Role Assignment

Process of binding a role definition to a user, group, or service principal at a scope for the purpose of granting access





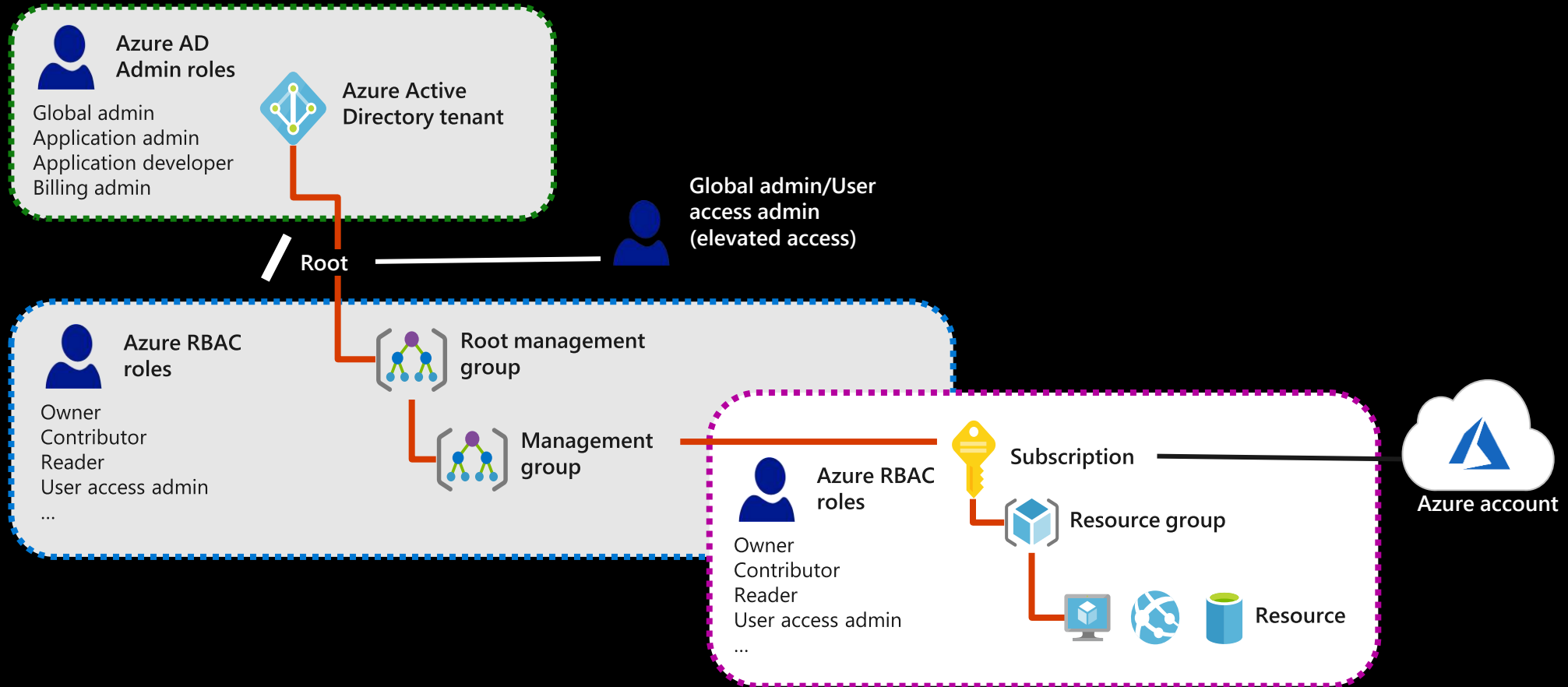
Azure RBAC Roles vs. Azure AD Roles

Azure and Azure AD offer two types of RBAC roles

Azure RBAC roles	Azure AD roles
Manage access to Azure resources	Manage access to Azure AD objects
Scope can be specified at multiple levels	Scope is at the tenant level
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure portal, Office 365 admin portal, Microsoft Graph, Azure Active Directory PowerShell for Graph

- ✓ Classic administrator roles should be avoided if using Azure Resource Manager

RBAC Authentication



Azure RBAC Roles



RBAC role in Azure	Permissions	Notes
Owner	Has full access to all resources and can delegate access to others.	The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope. This applies to all resource types.
Contributor	Creates and manages all types of Azure resources but cannot grant access to others.	This applies to all resource types.
Reader	Views Azure resources.	This applies to all resource types.
User Access Administrator	Manages user access to Azure resources.	This applies to managing access, rather than to managing resources.



Demonstration – Azure RBAC

- Locate the Access Control blade
- Review role permissions
- Add a role assignment
- Explore PowerShell commands



Azure Administrator Associate

EXAM: AZ-104



Module 03: Governance and Compliance

#8: Review Questions



Review Question 1

You need to target policies and review spend budgets across several subscriptions you manage. What should you do? Select one.

- Create resource groups
- Create management groups
- Create billing groups
- Create Azure policies



Review Question 2

You would like to categorize resources and billing for different departments like IT and HR. The billing needs to be consolidated across multiple resource groups and you need to ensure everyone complies with the solution. What should you do? {Choose two to complete a solution}.

- Create tags for each department.
- Create a billing group for each department.
- Create an Azure policy.
- Add the groups into a single resource group.
- Create a subscription account rule.



Review Question 3

Your company financial controller wants to be notified whenever the company is half-way to spending the money allocated for cloud services. What should you do? Select one.

- Create an Azure reservation.
- Create a budget and a spending threshold.
- Create a management group.
- Enter workloads in the Total Cost of Ownership calculator.



Review Question 4

Your organization has several Azure policies that they would like to create and enforce for a new branch office. What should you do? Select one.

- Create a policy initiative
- Create a management group
- Create a resource group
- Create a new subscriptions



Review Question 5

Your manager asks you to explain how Azure uses resource groups. You provide all of the following information, except? Select one.

- Resources can be in only one resource group.
- Resources can be moved from one resource group to another resource group.
- Resource groups can be nested.
- Role-based access control can be applied to the resource group.



Review Question 6

Which of the following would be good example of when to use a resource lock?
Select one.

- An ExpressRoute circuit with connectivity back to your on-premises network.
- A non-production virtual machine used to test occasional application builds.
- A storage account used to temporarily store images processed in a development environment.
- A resource group for a new branch office that is just starting up.



Review Question 7

Your company hires a new IT administrator. She needs to manage a resource group with first-tier web servers including assigning permissions . However, she should not have access to other resource groups inside the subscription. You need to configure role-based access. What should you do? Select one

- Assign her as a Subscription Owner.
- Assign her as a Subscription Contributor.
- Assign her as a Resource Group Owner.
- Assign her as a Resource Group Contributor.



Review Question 8

You have three virtual machines (VM1, VM2, and VM3) in a resource group. The Helpdesk hires a new employee. The new employee must be able to modify the settings on VM3, but not on VM1 and VM2. Your solution must minimize administrative overhead. What should you do? Select one.

- Assign the user to the Contributor role on the resource group.
- Assign the user to the Contributor role on VM3.
- Move VM3 to a new resource group and assign the user to the Contributor role on VM3.
- Assign the user to the Contributor role on the resource group, then assign the user to the Owner role on VM3.



Azure Administrator Associate

EXAM: AZ-104



Module 03: Azure Administration

#9: Resource Manager



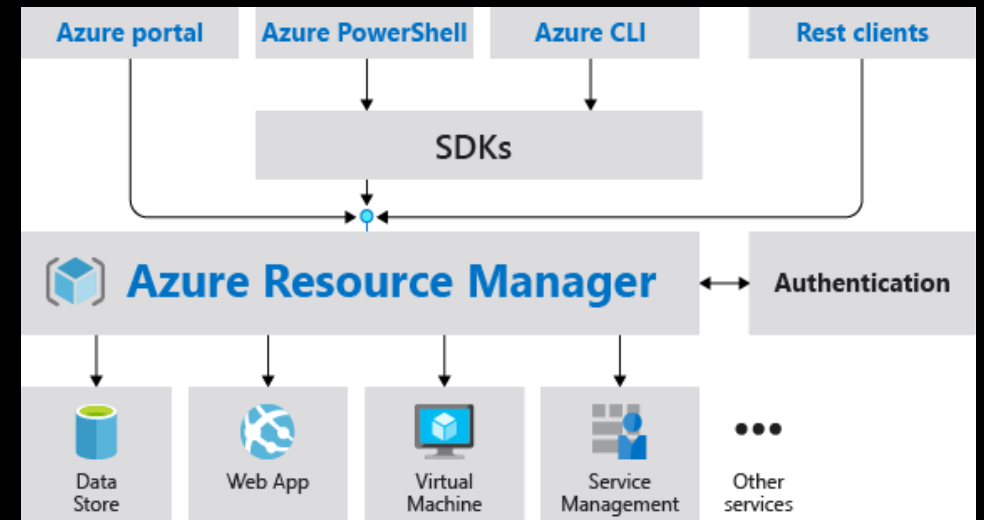
Resource Manager Overview

- Resource Manager
- Terminology
- Resource Group Deployments
- Resource Manager Locks
- Moving Resources
- Removing Resources and Resource Groups
- Resource Limits
- Demonstration- Resource Groups



Resource Manager

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





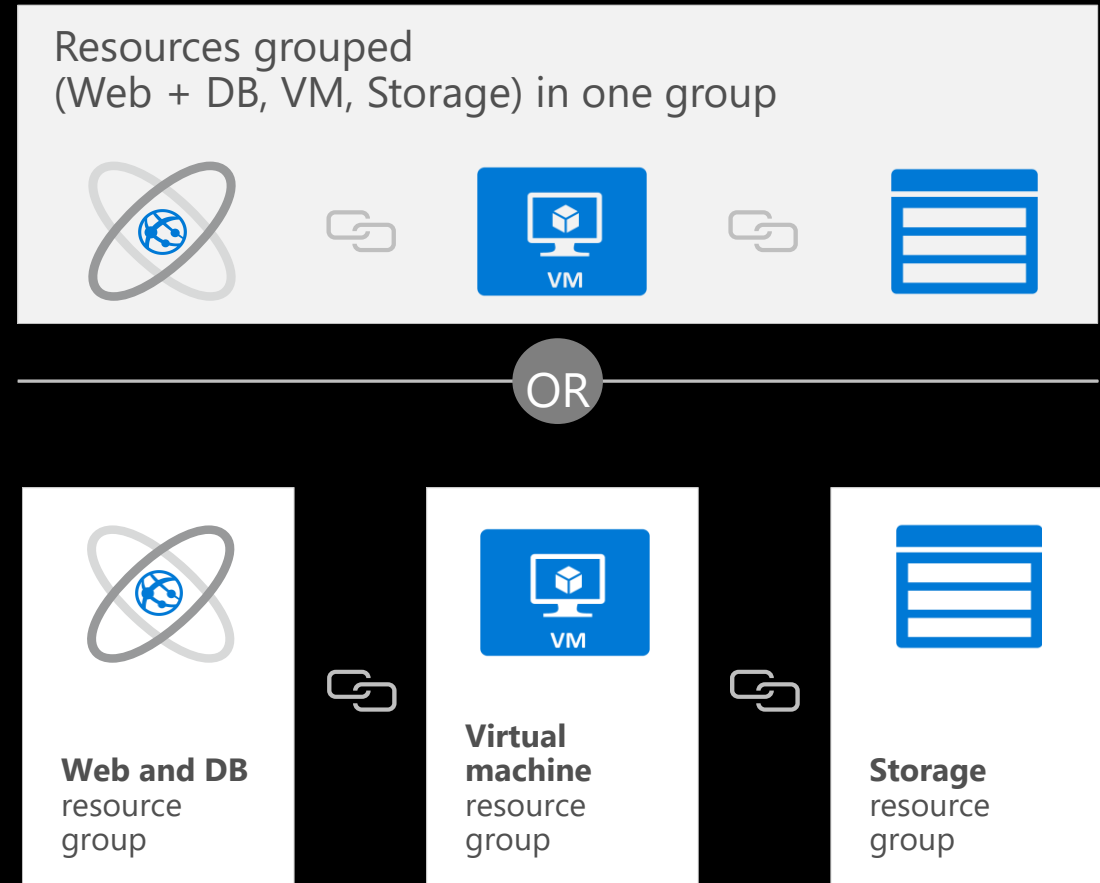
Terminology

- **Resource**
- **Resource Group**
- **Resource Provider**
- **ARM template**
- **Declarative syntax**



Resource Group Deployments

- 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
- Deployments are incremental
 - ✓ By scoping permissions to a resource group, you can add/remove and modify resources easily





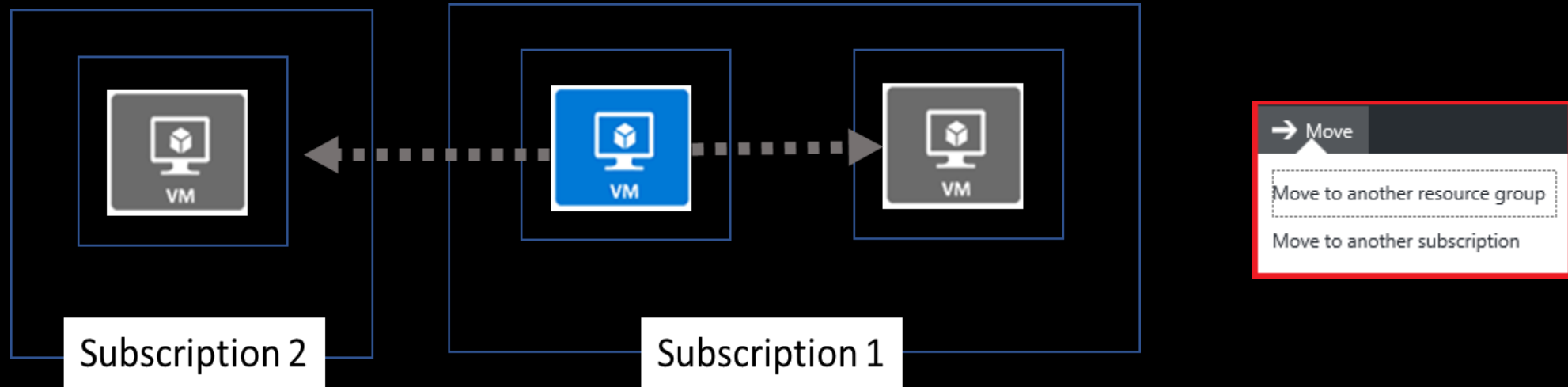
Resource Manager Locks

- 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

The screenshot shows the 'Add lock' dialog in the Azure portal for a Resource Group named 'NetworkRG'. The dialog is titled 'NetworkRG - Locks' and includes a search bar and buttons for '+ Add', 'Subscription', and 'Refresh'. The 'Add lock' section contains a 'Lock name' field with the value 'NetworkLock', a 'Lock type' dropdown menu with 'Read-only' and 'Delete' options, and a 'Notes' field. At the bottom, there are 'OK' and 'Cancel' buttons.



Moving Resources



- When moving resources, both the source group and the target group are locked during the operation
- Services that cannot be moved: AD Domain Services, ExpressRoute, and Site Recovery. Other restrictions apply.



Removing Resources and Resource Groups

- Remove Azure resources that you no longer use
- Ensures you will not see unexpected charges
- Remove individual resources or remove the resource group

The screenshot shows the Azure portal interface. On the left, a resource group is displayed with the title "Resource groups (web + DB, VM, Storage) in one group". Below the title, there are three icons: a globe, a VM icon, and a server rack icon. A red dashed arrow points from the VM icon to a context menu on the right. The context menu has three buttons: "Refresh", "Move", and "Delete". The "Delete" button is highlighted with a red box. Below the buttons, the context menu shows the following information: "Resource group (change) : ASH", "Location : West Central US", and "Subscription (change) : Visual Studio Enterprise".

```
Get-AzResourceGroup -Name 'az104-03*' | Remove-AzResourceGroup -Force -AsJob
```



Resource Limits

ASC DEMO | Usage + quotas
Subscription

Settings

- Programmatic deployment
- Resource groups
- Resources
- Usage + quotas
- Policies
- Security
- Events

You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. [Learn more](#) [Request Increase](#)

Quota	Provider	Location	Usage		
Total Regional vCPUs	Microsoft.Compute	East US		25 %	25 of 100
Total Regional vCPUs	Microsoft.Compute	West Europe		21 %	21 of 100
Total Regional vCPUs	Microsoft.Compute	Central US		17 %	17 of 100
Standard Dv2 Family vCPUs	Microsoft.Compute	West Europe		16 %	16 of 100
Standard DSv2 Family vCPUs	Microsoft.Compute	Central US		14 %	14 of 100

- Resources have a default limit also known as quota
- Helpful to track current usage, and plan for future use
- You can open a free support case to increase limits to published maximums



Azure Administrator Associate

EXAM: AZ-104



Module 03: Azure Administration

#10: Azure Portal and Cloud Shell



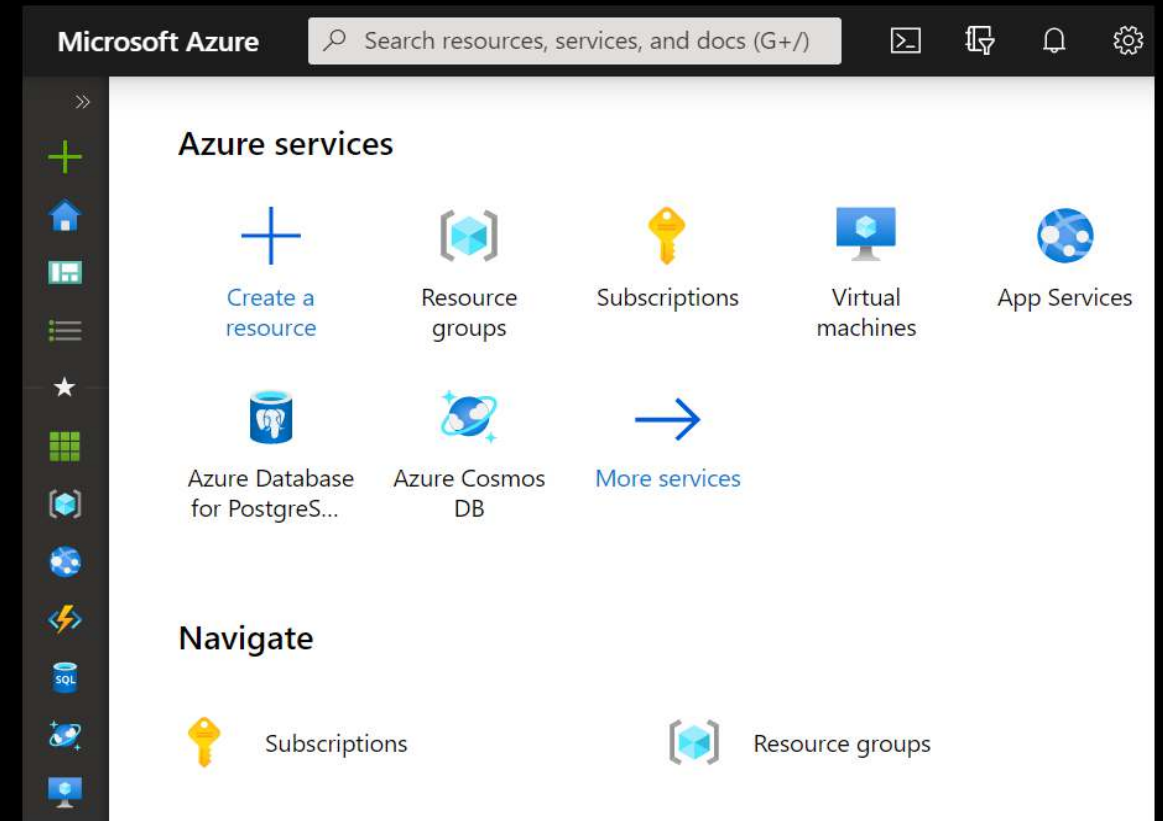
Azure Portal and Cloud Shell Overview

- Azure Portal
- Azure Mobile App
- Demonstration – Azure Portal
- Azure Cloud Shell
- Demonstration – Cloud Shell

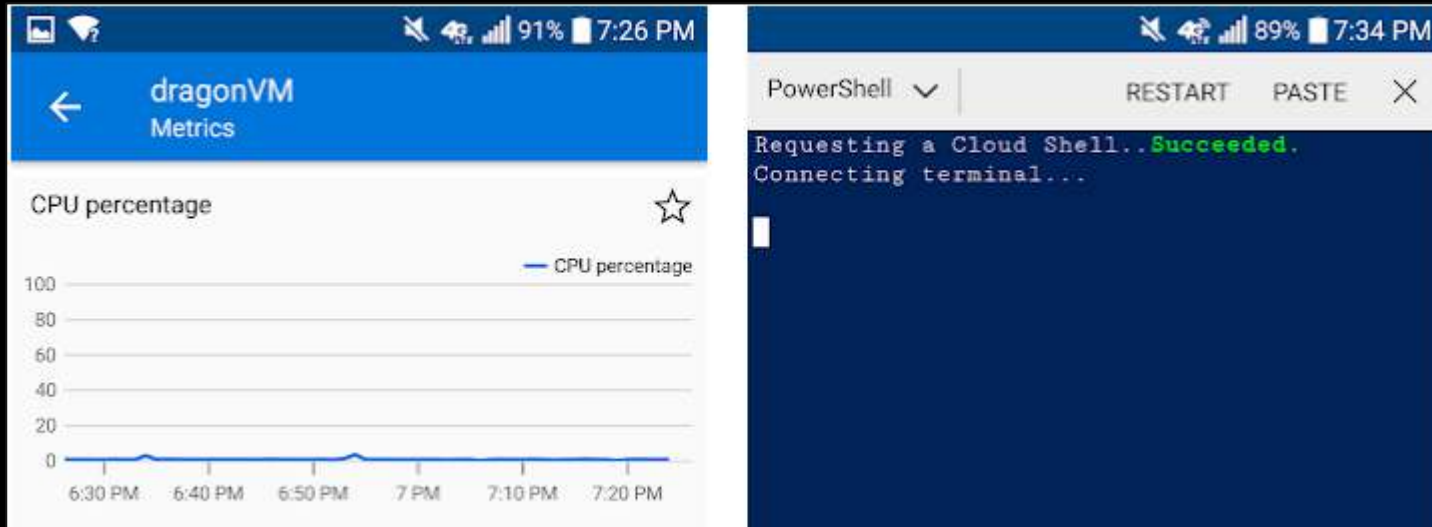
Azure Portal



- Search resources, services, and docs
- Manage resources
- Create customized dashboards and favorites
- Access the Cloud Shell
- Receive notifications



Azure Mobile App



- Stay connected to the cloud
- Check status and critical metrics anytime, anywhere
- Diagnose and fix issues quickly
- Run commands to manage your Azure resources



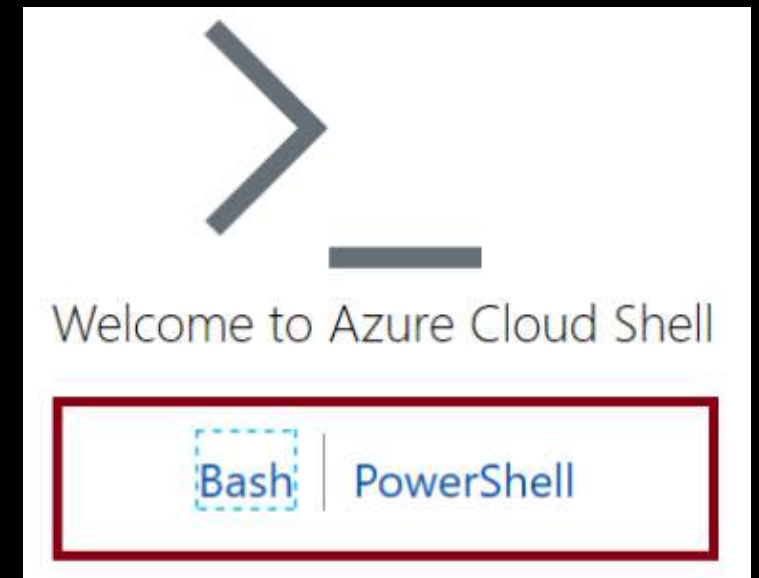
Demonstration – Azure Portal

- Help and keyboard shortcuts
- Customizing your experience



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
- Integrated graphical text editor
- Is assigned one machine per user account
- Times out after 20 minutes





Demonstration – Cloud Shell

- Configure the Cloud Shell
- Experiment with Azure PowerShell
- Experiment with Bash shell
- Experiment with the Cloud Editor



Azure Administrator Associate

EXAM: AZ-104



Module 03: Azure Administration

#11: Azure PowerShell and CLI



Azure PowerShell and CLI Overview

- Azure PowerShell
- PowerShell Cmdlets and Modules
- Demonstration – Working with PowerShell Locally
- Azure CLI
- Demonstration – Working with Azure CLI Locally



Azure PowerShell

```
New-AzVm `
  -ResourceGroupName "CrmTestingResourceGroup" `
  -Name "CrmUnitTests" `
  -Image "UbuntuLTS" `
  ...
```

- Lets you connect to your Azure subscription and manage resources
- Adds the Azure-specific commands – new **Az** module
- Available inside a browser via the Azure Cloud Shell
- Available as a local installation on Linux, macOS, or Windows
- Has an interactive and a scripting mode



PowerShell Cmdlets and Modules

```
Get-Module
# Output
ModuleType Version      Name
-----
Manifest    3.1.0.0    Microsoft.PowerShell.Management
Manifest    3.1.0.0    Microsoft.PowerShell.Utility
Binary      1.0.0.1    PackageManagement
Script      1.0.0.1    PowerShellGet
Script      2.0.0      PSReadline
```

- Cmdlets follow a verb-noun naming convention; shipped in modules
- Modules are a DLL file with the code to process each cmdlet
- Load cmdlets by loading the module containing them
- Use **Get-Modules** to see a list of loaded modules



Demonstration – Working with PowerShell

- Install the Az module
- Install NuGet (if needed)
- Trust the repository
- Connect to Azure and view your subscription information
- Create resources



Azure CLI

```
az vm restart -g MyResourceGroup -n MyVm
```

- Cross-platform command-line program
- Runs on Linux, macOS, and Windows
- Can be used interactively or through scripts
- Commands are structured in *__groups__* and *__subgroups__*
- Use *find* to locate commands
- Use *--help* for more detailed information



Demonstration – Working with the CLI

- Install the CLI
- Verify the CLI installation
- Login to Azure
- Create a resource group
- Verify the resource group



Azure Administrator Associate

EXAM: AZ-104



Module 03: Azure Administration

#12: ARM Templates



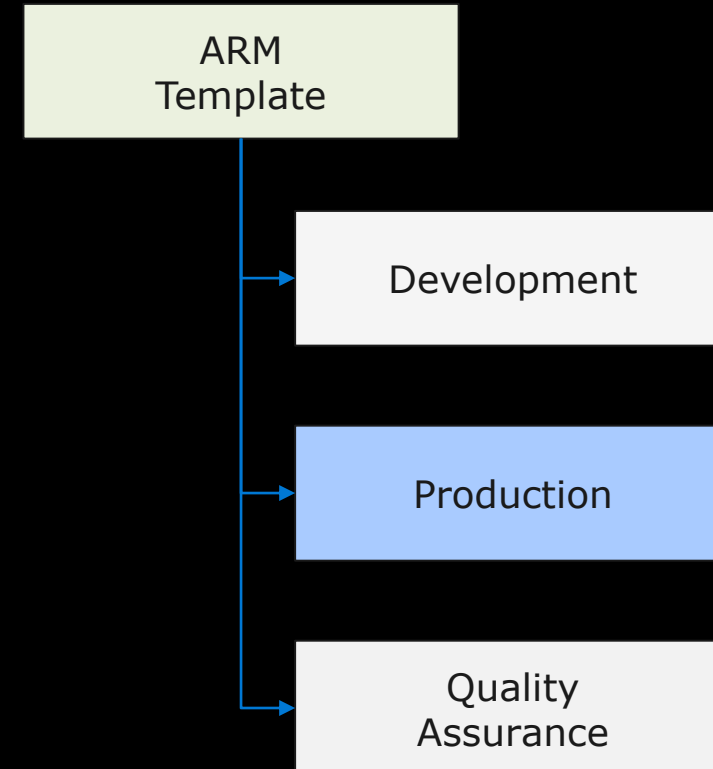
ARM Templates Overview

- Template Advantages
- Template Schema
- Template Parameters
- Template Variables
- Template Functions
- Template Resources
- Template Outputs
- QuickStart Templates
- Demonstration – QuickStart Templates
- Demonstration – Run Templates with PowerShell



Template Advantages

- Improves consistency
- Express complex deployments
- Reduce manual, error prone tasks
- Express requirements through code
- Promotes reuse
- Modular and can be linked
- Simplifies orchestration





Template Schema

```
{
  "$schema": "http://schema.management.
    azure.com/schemas/2019-04-
    01/deploymentTemplate.json#",
  "contentVersion": "",
  "parameters": {},
  "variables": {},
  "functions": [],
  "resources": [],
  "outputs": {}
}
```

- Defines all the Resource Manager resources in a deployment
- Written in JSON
- A collection of key-value pairs
- Each key is a string
- Each values can be a string, number, Boolean expression, list of values, object



Template Parameters

- Specify which values are configurable when the template runs
- This example has two parameters: one for a VM's username (adminUsername), and one for its password (adminPassword)

```
"parameters": {
  "adminUsername": {
    "type": "string",
    "metadata": {
      "description": "Username for the VM."
    }
  },
  "adminPassword": {
    "type": "securestring",
    "metadata": {
      "description": "Password for the VM."
    }
  }
}
```



Template Variables

```
"variables": {  
  "nicName": "myVMNic",  
  "addressPrefix": "10.0.0.0/16",  
  "subnetName": "Subnet",  
  "subnetPrefix": "10.0.0.0/24",  
  "publicIPAddressName": "myPublicIP",  
  "virtualNetworkName": "MyVNET"  
}
```

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



Template Functions

- Reusable procedures
- Makes the template easier to maintain
- This function creates a unique name - use when creating resources that have globally unique naming requirements

```
"functions": [  
  {  
    "namespace": "contoso",  
    "members": {  
      "uniqueName": {  
        "parameters": [  
          {  
            "name": "namePrefix",  
            "type": "string"  
          } ],  
        "output": {  
          "type": "string",  
          "value":  
            "[concat(toLower(parameters('namePrefix')),  
uniqueString(resourceGroup().id))]"  
        }  
      }  
    }  
  } ],
```



Template Resources

```
{
  "type": "Microsoft.Network/publicIPAddresses",
  "name": "[variables('publicIPaddressName')]",
  "location": "[parameters('location')]",
  "apiVersion": "2018-08-01",
  "properties": {
    "publicIPAllocationMethod": "Dynamic",
    "dnsSettings": {
      "domainNameLabel": "[parameters('dnsLabelPrefix')]"
    }
  }
}
```

- Define the Azure resources that make up your deployment
- This example that creates a public IP address resource
- Name is a variable
- Location is a parameter



Template Outputs

```
"outputs": {  
  "hostname": {  
    "type": "string",  
    "value": "[reference(variables(  
      'publicIPAddressName'))].  
      dnsSettings.fqdn]"  
  }  
}
```

- Define any information you'd like to receive when the template runs
- This example receives a VM's IP address or FQDN
- **Hostname** is the output
- The FQDN value is read from the virtual machines public IP address settings



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

757 Quickstart templates are currently in the gallery.

Create Configuration Manager Tech Preview Lab in Azure

This template creates a new System Center Configuration Manager Technical Preview Lab environment. It creates 4 new Azure VMs, configuring a new AD Domain Contr...

 by [Yizhong Wu](#),
Last updated: 12/10/2018

Create a Standard Storage Account

This template creates a Standard Storage Account

 by [Brian Moore](#),
Last updated: 12/4/2018

Deploy a Django app

This template uses the Azure Linux CustomScript extension to deploy an application. This example creates an Ubuntu VM, does a silent install of Python, Django...

 by [Madhan Arumugam Ramakrishnan](#),
Last updated: 7/19/2018

Create an new AD Domain with 2 Domain Controllers

This template creates 2 new VMs to be AD DCs (primary and backup) for a new Forest and Domain

 by [Simon Davies](#),
Last updated: 7/5/2018

<https://azure.microsoft.com/en-us/resources/templates/>



Demonstration – QuickStart Templates

- Explore the QuickStart gallery
- Explore a template



Demonstration – Run Templates with PowerShell

- Connect to your subscription
- Create the resource group
- Deploy the template into the resource group
- Verify the template deployed



Azure Administrator Associate

EXAM: AZ-104



Module 03: Azure Administration

#13: Review Questions



Review Question 1

You are creating a new resource group to use for testing. Which two of the following parameters are required when you create a resource group with PowerShell or the CLI? Select two.

- Location
- Name
- Region
- Subscription
- Tag



Review Question 2

Which of the following is not true about the Cloud Shell? Select one.

- Authenticates automatically for instant access to your resources.
- Each user account can be assigned multiple machines.
- Provides both Bash and PowerShell sessions.
- Provides an editor.
- Requires an Azure file share.



Review Question 3

You are managing Azure locally using PowerShell. You have launched the app as an Administrator. Which of the following commands would you do first? Select one.

- Connect-AzAccount
- Get-AzResourceGroup
- Get-AzSubscription
- New-AzResourceGroup



Review Question 4

You have a new Azure subscription and need to move resources to that subscription. Which of the following resources cannot be moved? Select one

- Key vault
- Storage account
- Tenant
- Virtual machine



Review Question 5

Which of the following is not an element in the template schema? Select one

- Functions
- Inputs
- Outputs
- Parameters



Review Question 6

Which of the following best describes the format of an Azure Resource Manager template? Select one.

- A Markdown document with a pointer table
- A JSON document with key-value pairs
- A TXT document with key-value pairs
- An XML document with element-value pairs



Review Question 7

You are reviewing your virtual machine usage. You notice that you have reached the limit for virtual machines in the US East region. Which of the following provides the easiest solution? Select one.

- Add another resource group
- Change your subscription plan
- Request support increase your limit
- Resize your virtual machines to handle larger workloads



Azure Administrator Associate

EXAM: AZ-104



Module 04: Virtual Networking

#14: Virtual Networks









Virtual Networks Overview

- Azure Networking Components
- Virtual Networks
- Subnets
- Implementing Virtual Networks
- Demonstration – Creating Virtual Networks



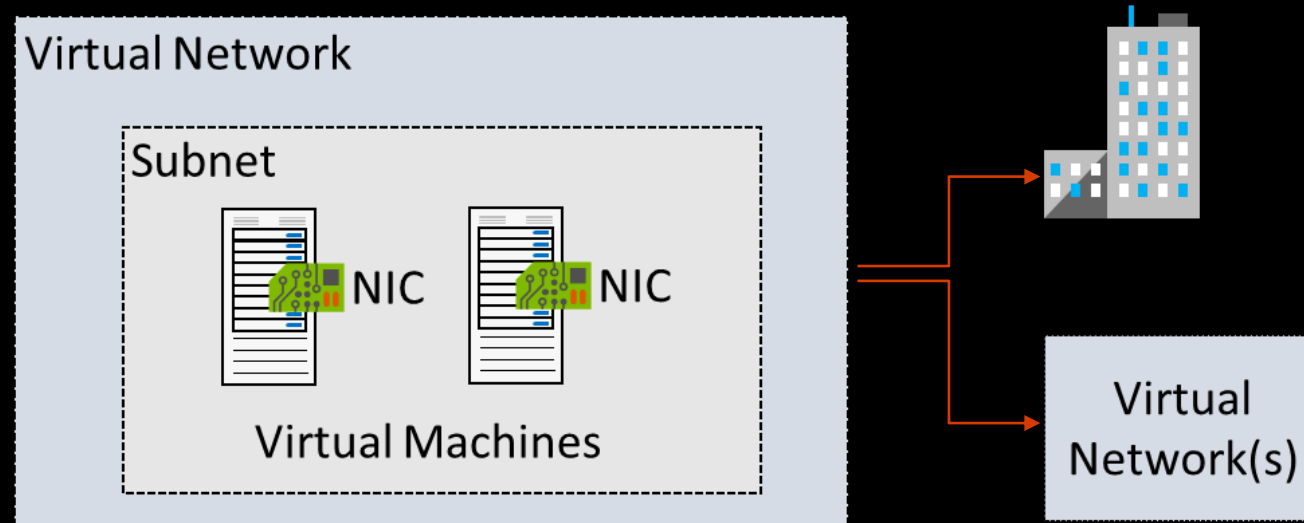
Azure Networking Components

- Adopting cloud solutions can save time and simplify operations
- Azure requires the same types of networking functionality as on-premises infrastructure
- Azure networking offers a wide range of services and products

 Virtual Network Microsoft Create a logically isolated section in Microsoft Azure and securely connect it outward.	 Load Balancer Microsoft A load balancer that distributes incoming traffic among backend virtual machine instances.	 Application Gateway Microsoft Scalable layer-7 load balancer offering various traffic routing rules and SSL termination for backend
 Traffic Manager profile Microsoft Create a Microsoft Azure Traffic Manager Profile that allows you to control the distribution of user	 Virtual network gateway Microsoft The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN	 Virtual WAN Microsoft Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch



Virtual Networks



- Logical representation of your own network
- Create a dedicated private cloud-only virtual network
- Securely extend your datacenter with virtual networks
- Enable hybrid cloud scenarios



+ Subnet + Gateway subnet Refresh

Search subnets

Name	↑↓	Address range	↑↓	IPv4 available addresses	↑↓	Delegated to	↑↓	Security group
subnet0		10.1.0.0/24		251		-		nsg0
subnet1		10.1.1.0/24		251		-		-
subnet2		10.1.2.0/24		251		-		nsg2
GatewaySubnet		10.1.255.0/24		251		-		-

- A virtual network can be segmented into one or more subnets
- Subnets provide logical divisions within your network
- Subnets can help improve security, increase performance, and make it easier to manage the network
- Each subnet must have a unique address range - cannot overlap with other subnets in the virtual network in the subscription

Subnets



+ Subnet + Gateway subnet Refresh

Search subnets

Name	↑↓	Address range	↑↓	IPv4 available addresses	↑↓	Delegated to	↑↓	Security group
subnet0		10.1.0.0/24		251		-		nsg0
subnet1		10.1.1.0/24		251		-		-
subnet2		10.1.2.0/24		251		-		nsg2
GatewaySubnet		10.1.255.0/24		251		-		-

- Service Requirements
- Virtual Appliances
- Service Endpoints
- Network Security Groups



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

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

Project details

Subscription * ⓘ Visual Studio Enterprise ▾

Resource group * ⓘ Lab04 ▾
[Create new](#)

Instance details

Name * VNet2 ✓

Region * (US) East US 2 ▾



Demonstration – Creating Virtual Networks

- Create a virtual network in the portal
- Create a virtual network with PowerShell



Azure Administrator Associate

EXAM: AZ-104



Module 04: Virtual Networking

#15: IP Addressing

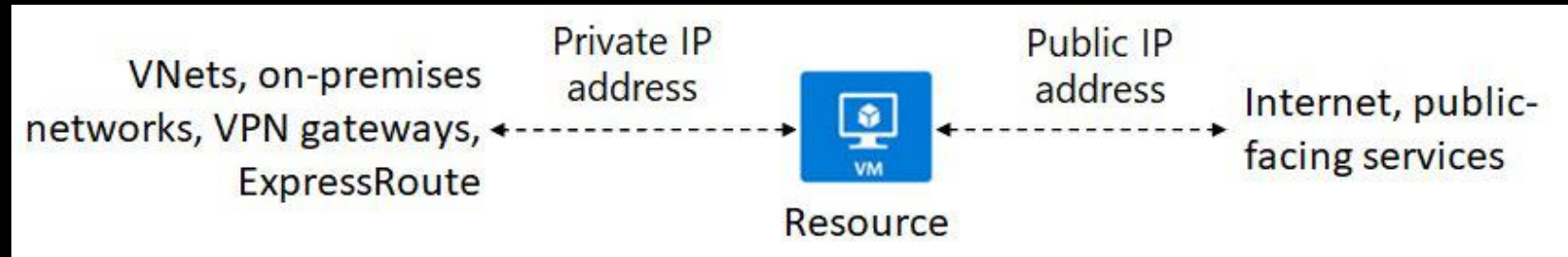


IP Addressing Overview

- IP Addressing
- Creating IP Addresses
- Public IP Addresses
- Private IP Addresses



IP Addressing



- **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



Creating Public IP Addresses

- Available in IPv4 or IPv6 or both
- Basic vs Standard SKU
- Available in Dynamic, Static or both (depending on SKU)
 - Zone redundant
 - Not mixable or immutable
- Range of contiguous addresses available as a prefix

Create public IP address

IP Version * ⓘ
 IPv4 IPv6 Both

SKU * ⓘ
 Basic Standard

IPv4 IP Address Configuration

Name *

IP address assignment *
 Dynamic Static

Public IP Addresses



Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	Yes*
Application Gateway	Front-end configuration	Yes	Yes*

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

* Static IP addresses only available on certain SKUs.



Private IP Addresses

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	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



Azure Administrator Associate

EXAM: AZ-104



Module 04: Virtual Networking

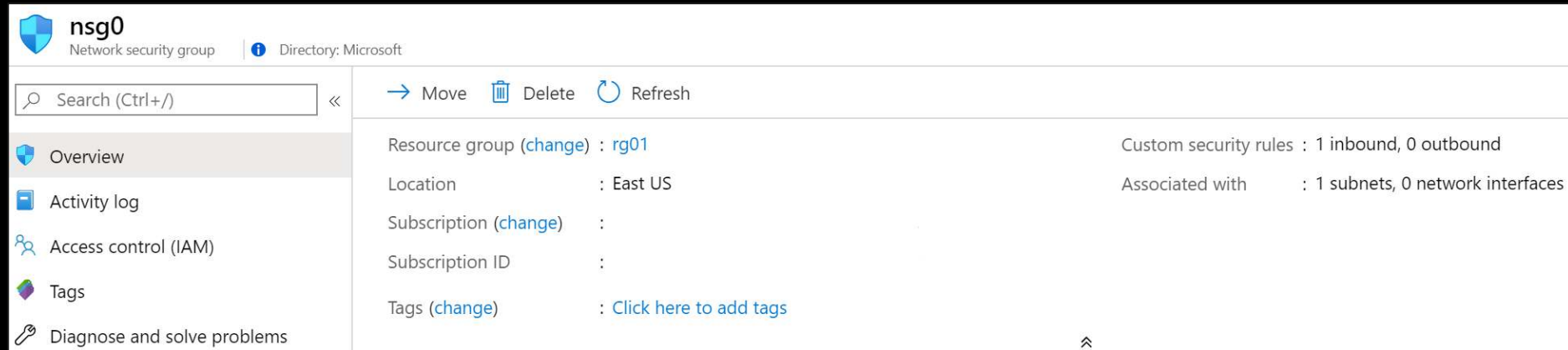
#16: Network Security Group



Network Security Groups Overview

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

Network Security Groups



- Limit network traffic to resources in a virtual network
- Contains a list of security rules that allow or deny inbound or outbound network traffic
- Can be associated to a subnet or a network interface



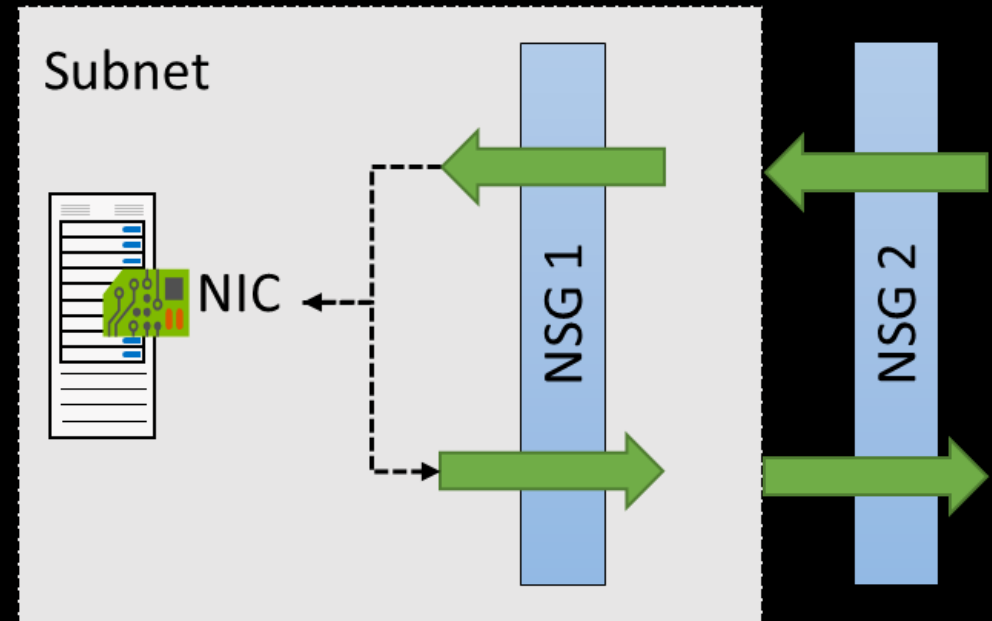
Inbound security rules							
Priority	Name	Port	Protocol	Source	Destination	Action	
100	⚠ RDP_Inbound	3389	Any	Any	Any	✔ Allow	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow	
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✔ Allow	
65500	DenyAllInBound	Any	Any	Any	Any	✘ Deny	
Outbound security rules							
Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow	
65001	AllowInternetOutBound	Any	Any	Any	Internet	✔ Allow	
65500	DenyAllOutBound	Any	Any	Any	Any	✘ Deny	


- 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.



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:** [vm01990](#) [Effective security rules](#) [Topology](#)
Virtual network/subnet: [vnet01/subnet0](#) NIC Public IP: - NIC Private IP: **10.1.0.4** 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

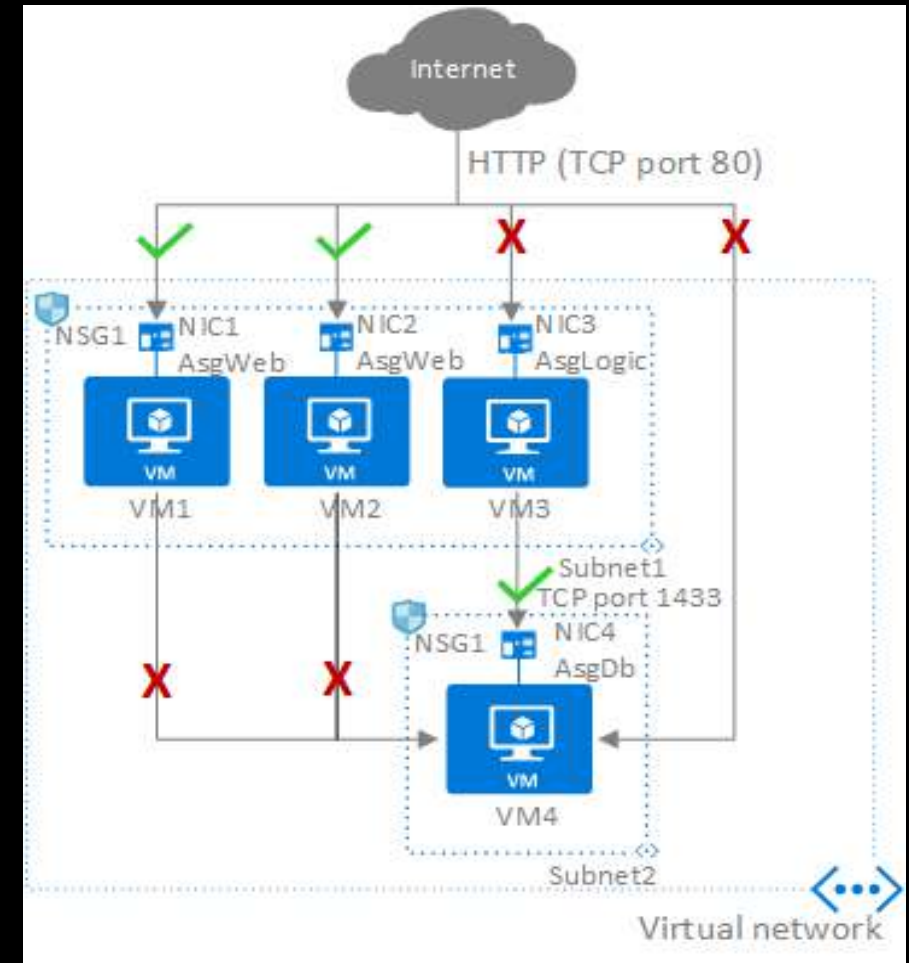
The screenshot shows the 'Add inbound security rule' dialog box for a network security group named 'nsg1'. The dialog is in 'Advanced' mode. The 'Service' dropdown is set to 'Custom'. The 'Port ranges' field contains '8080'. The 'Priority' field contains '100'. The 'Name' field contains 'Port_8080'. The 'Description' field is empty.



Application Security Groups

Provides for the grouping of servers with similar port filtering requirements, and group together servers with similar functions, such as web servers.

- Allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses.
- Handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.





Demonstration – Network Security Rules

- Access the NSGs blade
- Add a new NSG
- Explore inbound and outbound rules



Azure Administrator Associate

EXAM: AZ-104



Module 04: Virtual Networking

#17: Azure Firewall



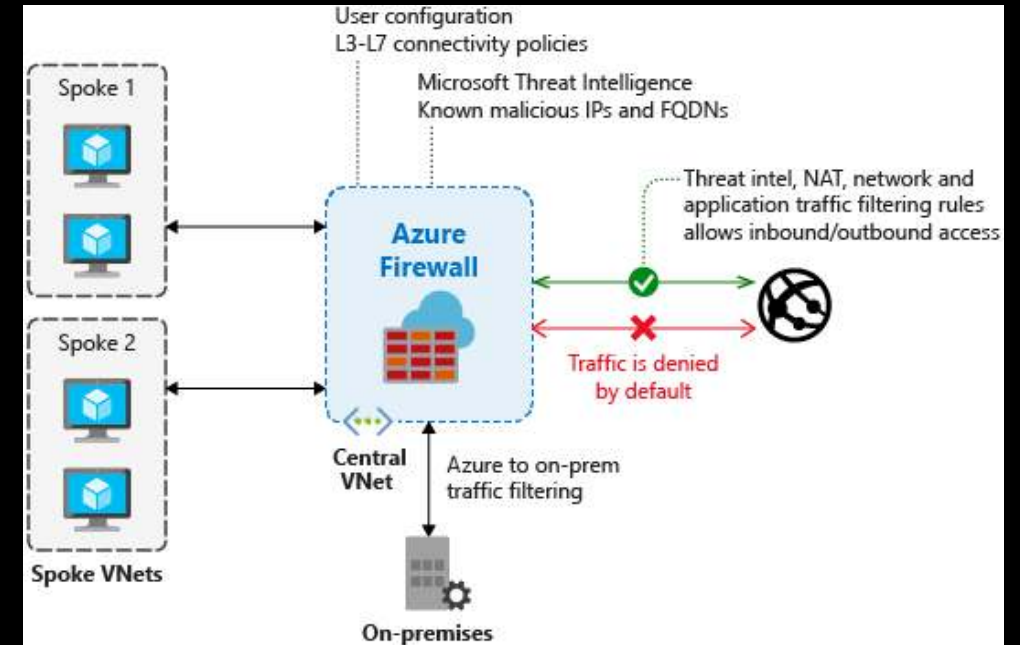
Azure Firewall Overview

- Azure Firewall
- Implementing Firewalls
- Firewall Rules



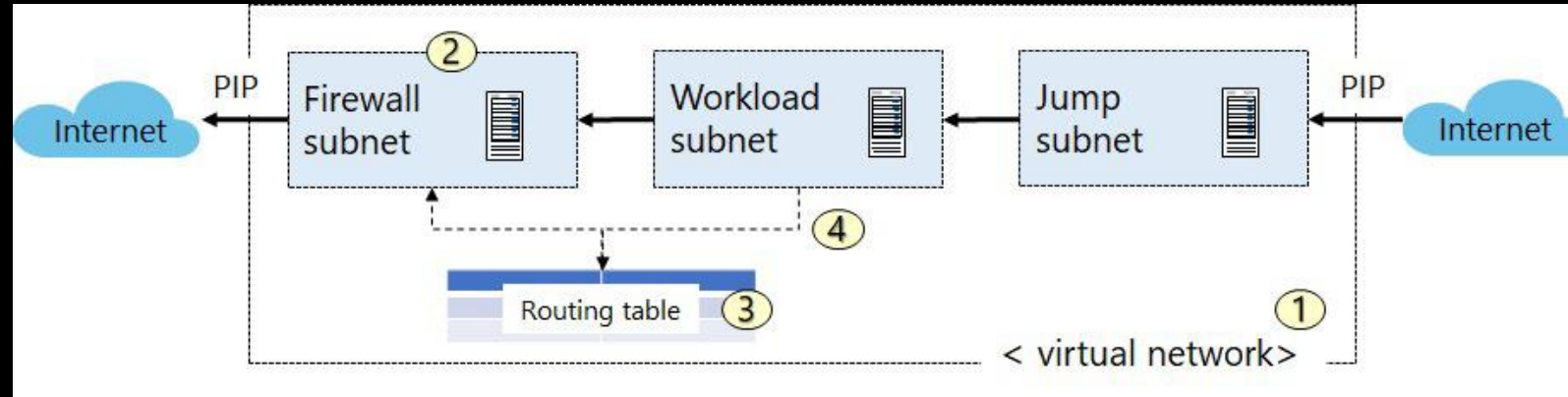
Azure Firewall

- Stateful firewall as a service
- Built-in high availability with unrestricted cloud scalability
- Create, enforce, and log application and network connectivity policies
- Threat intelligence-based filtering
- Fully integrated with Azure Monitor for logging and analytics
- Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways





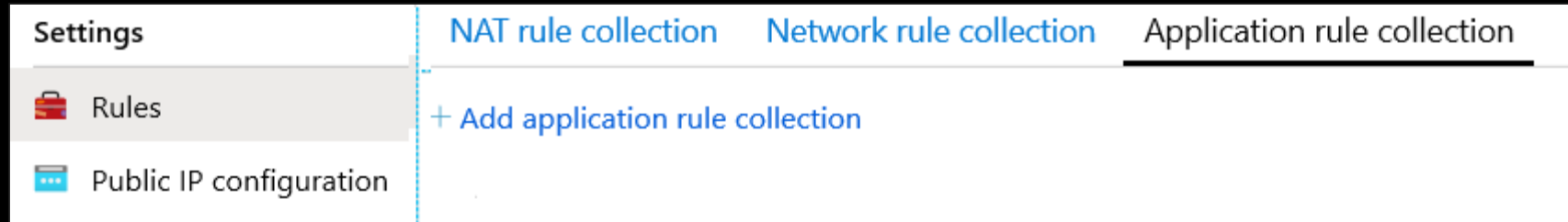
Implementing Firewalls



1. Create the network infrastructure.
2. Deploy the firewall.
3. Create a default route.
4. Configure rules.

✓ In production deployments, a Hub and Spoke model is recommended.

Firewall Rules



NAT rules

Configure DNAT rules to allow incoming connections

Network rules

Configure rules that contain source addresses, protocols, destination ports, and destination addresses

Application rules

Configure fully qualified domain names (FQDNs) that can be accessed from a subnet



Azure Administrator Associate

EXAM: AZ-104



Module 04: Virtual Networking

#18: Azure DNS



Azure DNS Overview

- Domains and Custom Domains
- Verifying Custom Domain Names
- Azure DNS Zones
- DNS Delegation
- DNS Record Sets
- 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 a directory
Azure Active Directory

Basics * **Configuration *** Review + create

Directory details
Configure your new directory

Organization name * ⓘ
Azure Administrator Incorporated ✓

Initial domain name * ⓘ
azureadminincorg ✓
azureadminincorg.onmicrosoft.com

Country/Region ⓘ
United States

Review + create < Previous Next : Review + create >

Custom domain name ✕
Azure Administrator Incorporated

Custom domain name * ⓘ
azureadmininc.org ✓

Add domain



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 hours

azureadmininc.org
Custom domain name

Delete | Got feedback?

i To use azureadmininc.org 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=ms79094380

TTL

3600

[Share these settings via email](#)

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



Azure DNS Zones

- 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

Create DNS zone

Basics Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more.](#)

Project details

Subscription * MSDN Platforms Subscription

Resource group * rg-dns [Create new](#)

Instance details

Name * azureadmininc.org ✓

Resource group location ⓘ East US

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)



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

azureadmininc.org

Name
helloworld ✓
.azureadmininc.org

Type
A

Alias record set ⓘ
 Yes No

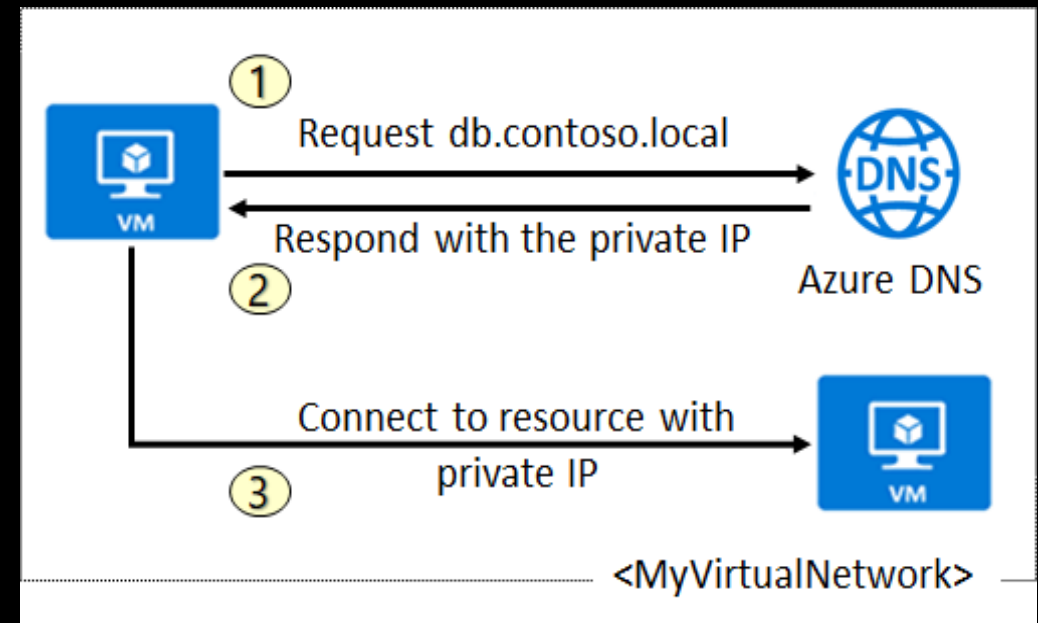
TTL * 1
TTL unit Hours

IP address
0.0.0.0 ...



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



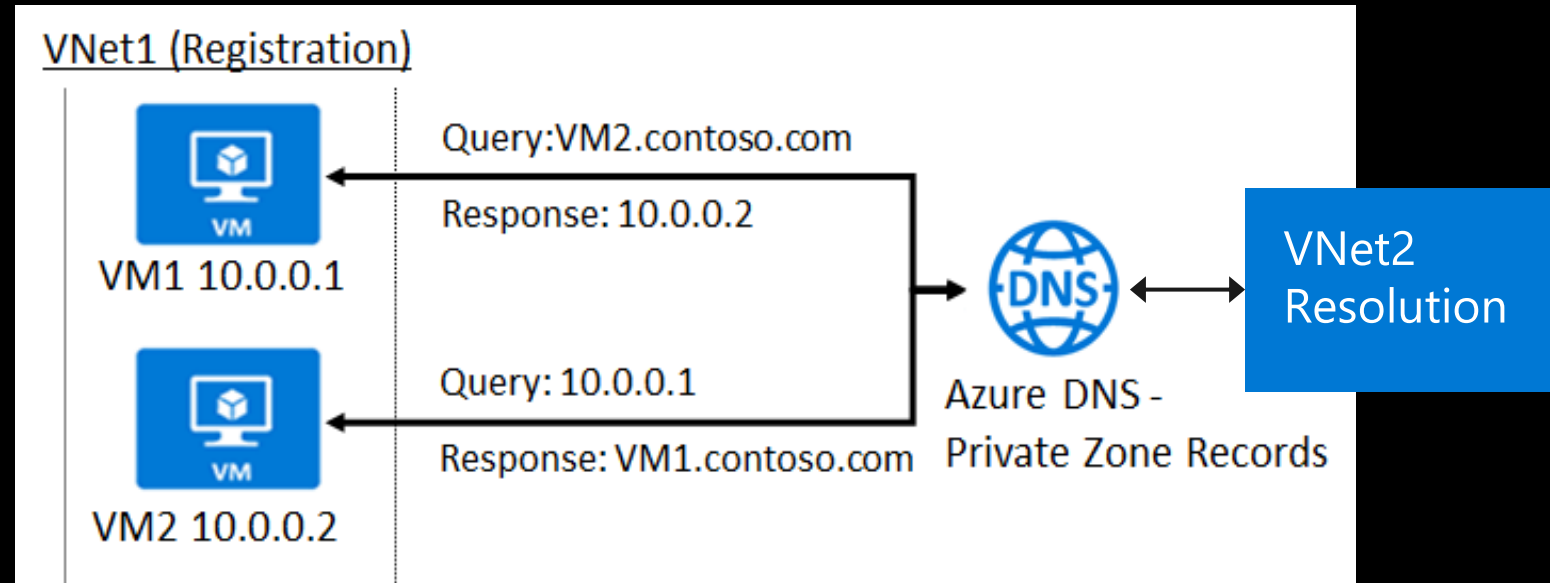


Benefits of Azure DNS

- Removes the need for custom DNS solutions
- Use all common DNS records types
 - Automatic hostname record management
- Hostname resolution between virtual networks
- Familiar tools and user experience
- Split-horizon DNS support
- Available in all Azure regions



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



Demonstration – DNS Name Resolution

- Create a DNS zone
- Add a DNS record set
- Use PowerShell to view DNS information
- View your name servers
- Test the resolution
- Explore DNS metrics



Azure Administrator Associate

EXAM: AZ-104



Module 04: Virtual Networking

#19: Review Questions



Review Question 1

Your company has an existing Azure tenant named `alpineskihouse.onmicrosoft.com`. The company wants to start using `alpineskihouse.com` for their Azure resources. You add a custom domain to Azure. Now, you need to add a DNS record to prepare for verifying the custom domain. Which two of the following record types could you create? Select two.

- Add an PTR record to the DNS zone.
- Add a TXT record to the DNS zone.
- Add an MX record to the DNS zone.
- Add an SRV record to the DNS zone.
- Add a CNAME record to the DNS zone.



Review Question 2

You are planning to configure networking in Microsoft Azure.

Your company has a new Microsoft Azure presence with the following network characteristics:

- 1 Virtual Network.
- 1 subnet using 192.168.0.0/23 (does not have existing resources).

Your on-premises data center has the following network characteristics:

- 10 subnets using 192.168.1.0/24 through 192.168.10.0/24.

The company intends to use 192.168.1.0/24 on-premises and 192.168.0.0/24 in Azure. You need to update your company's environment to enable the needed functionality. What should you do? (Each answer represents part of the solution. Choose two.)

- Delete 192.168.0.0/23 from Azure.
- Delete 192.168.1.0/24 in the on-premises environment.
- Create a matching public subnet in Azure and in the on-premises environment.
- Create a subnet for 192.168.0.0/23 in the on-premises environment.
- Create a subnet for 192.168.0.0/24 in Azure.



Review Question 3

- You are planning your Azure network implementation to support your company's migration to Azure. Your first task is to prepare for the deployment of the first set of VMs. The first set of VMs that you are deploying have the following requirements:
 - **Consumers on the internet must be able to communicate directly with the web application on the VMs.**
 - **The IP configuration must be zone redundant.**

You need to configure the environment to prepare for the first VM. Additionally, you need to minimize costs, whenever possible, while still meeting the requirements. What should you do? Select one.

- Create a standard public IP address. During the creation of the first VM, associate the public IP address with the VM's NIC.
- Create a standard public IP address. After the first VM is created, remove the private IP address and assign the public IP address to the NIC.
- Create a basic public IP address. During the creation of the first VM, associate the public IP address with the VM.
- Create a basic public IP address. After the first VM is created, remove the private IP address and assign the public IP address to the NIC.



Review Question 4

You deploy a new domain named contoso.com to domain controllers in Azure. You have the following domain-joined VMs in Azure:

- **VM1 at 10.20.30.10**
- **VM2 at 10.20.30.11**
- **VM3 at 10.20.30.12**
- **VM99 at 10.20.40.101**

You need to add DNS records so that the hostnames resolve to their respective IP addresses. Additionally, you need to add a DNS record so that intranet.contoso.com resolves to VM99. What should you do? (Each answer presents part of the solution. Choose two.)

- Add AAAA records for each VM.
- Add A records for each VM.
- Add a TXT record for intranet.contoso.com with the text of VM99.contoso.com.
- Add an SRV record for intranet.contoso.com with the target pointing at VM99.contoso.com
- Add a CNAME record for intranet.contoso.com with a value of VM99.contoso.com.



Review Question 5

Your company is preparing to move some services and VMs to Microsoft Azure. The company has opted to use Azure DNS to provide name resolution. A project begins to configure the name resolution. The project identifies the following requirements

- **A new domain will be used.**
- **The domain will have DNS records for internal and external resources.**
- **Minimize ongoing administrative overhead.**

You need to prepare and configure the environment with a new domain name and a test hostname of WWW. Which of the following steps should you perform? (Each answer presents part of the solution. Choose three.)

- Register a domain name with a domain registrar.
- Register a domain name with Microsoft Azure.
- Delegate the new domain name to Azure DNS.
- Add an Address (A) record for Azure name servers in the zone.
- Add DNS glue records to point to the Azure name servers.
- Add a record for WWW.



Review Question 6

You have a VM with two NICs named NIC1 and NIC2. NIC1 is connected to the 10.10.8.0/24 subnet. NIC2 is connected to the 10.20.8.0/24 subnet. You plan to update the VM configuration to provide the following functionality:

- **Enable direct communication from the internet to TCP port 443.**
- **Maintain existing communication across the 10.10.8.0/24 and 10.20.8.0/24 subnets.**
- **Maintain a simple configuration whenever possible.**

You need to update the VM configuration to support the new functionality. What should you do? Select one.

- Remove the private IP address from NIC2 and then assign a public IP address to it. Then, create an inbound security rule.
- Add a third NIC and associate a public IP address to it. Then, create an inbound security rule.
- Associate a public IP address to NIC2 and create an inbound security rule.
- Create an inbound security rule for TCP port 443.



Review Question 7

You're currently using network security groups (NSGs) to control how your network traffic flows in and out of your virtual network subnets and network interfaces. You want to customize how your NSGs work. For all incoming traffic, you need to apply your security rules to both the virtual machine and subnet level. Which of the following options will let you accomplish this? (Choose two)

- Configure the AllowVNetInBound security rule for all new NSGs.
- Create rules for both NICs and subnets with an allow action.
- Delete the default rules.
- Add rules with a higher priority than the default rules.



Review Question 8

You need to ensure that Azure DNS can resolve names for your registered domain. What should you implement? Select one.

- zone delegation
- a CNAME record
- an MX record
- a secondary zone
- a primary zone with a NS record



Review Question 9

You are configuring the Azure Firewall. You need to allow Windows Update network traffic through the firewall. Which of the following should you use? Select one.

- Application rules
- Destination inbound rules
- NAT rules
- Network rules



Azure Administrator Associate

EXAM: AZ-104



Module 05: Intersite Connectivity

#20: VNet Peering

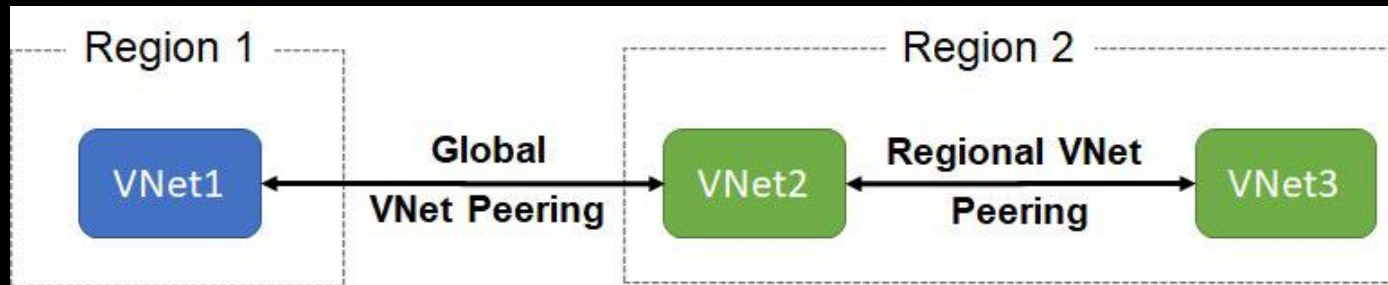


VNet Peering Overview

- VNet Peering
- Gateway Transit and Connectivity
- Configure VNet Peering
- Service Chaining
- Demonstration – VNet Peering



VNet Peering



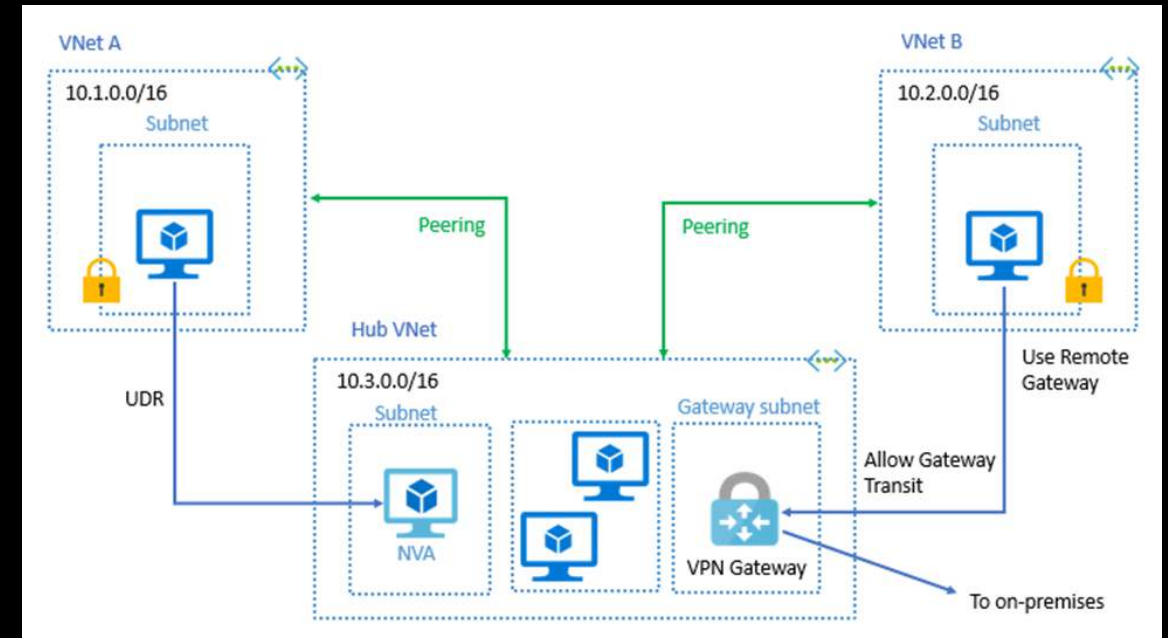
- VNet peering connects two Azure virtual networks
- Two types of peering: Regional and Global
- Peered networks use the Azure backbone for privacy and isolation
- You can peer across subscriptions
- Easy to setup, seamless data transfer, and great performance

- Private
- Performance
- Communication
- Seamless
- No disruption



Gateway Transit and Connectivity

- 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



✓ IP address spaces of connected networks can't overlap



Configure VNet Peering

- **Allow forwarded traffic** - from within the peer virtual network into your virtual network
- **Allow gateway transit** - Allows the peer virtual network to use your virtual network gateway
- **Use remote gateways** - only one virtual network can have this enabled

Configuration

Configure virtual network access settings

Allow virtual network access from vnet1 to vnet2 ⓘ

Disabled Enabled

Configure forwarded traffic settings

Allow forwarded traffic from vnet2 to vnet1 ⓘ

Disabled Enabled

Configure gateway transit settings

Allow gateway transit ⓘ

Configure Remote Gateways settings

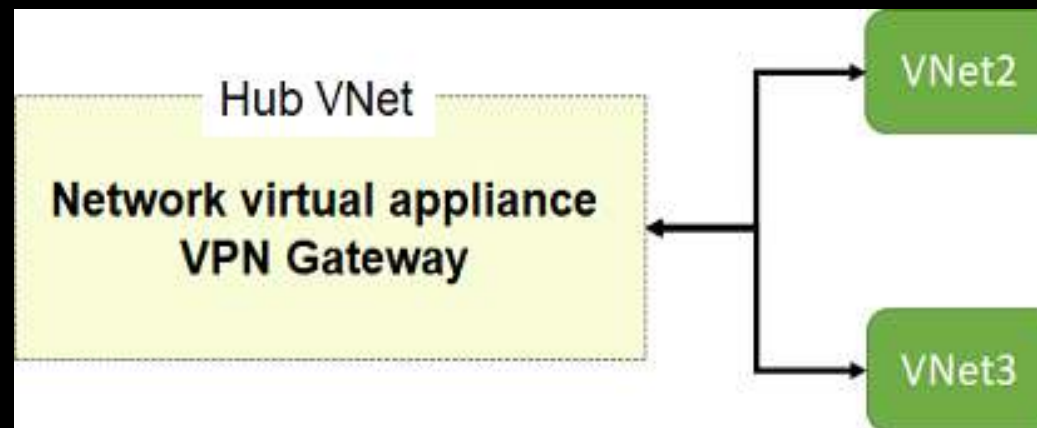
Use remote gateways ⓘ

✓ If you select 'Allow gateway transit' on one virtual network; then you should select 'Use remote gateways' on the other virtual network.



Service Chaining

- Leverage user-defined routes and service chaining to implement custom routing
- Implement a VNet hub with a network virtual appliance or a VPN gateway
- Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes





Demonstration – VNet Peering

- Configure VNet peering on the first virtual network
- Configure a VPN gateway
- Allow gateway transit
- Confirm VNet peering on the second virtual network



Azure Administrator Associate

EXAM: AZ-104



Module 05: Intersite Connectivity

#21: VPN Gateway Connections

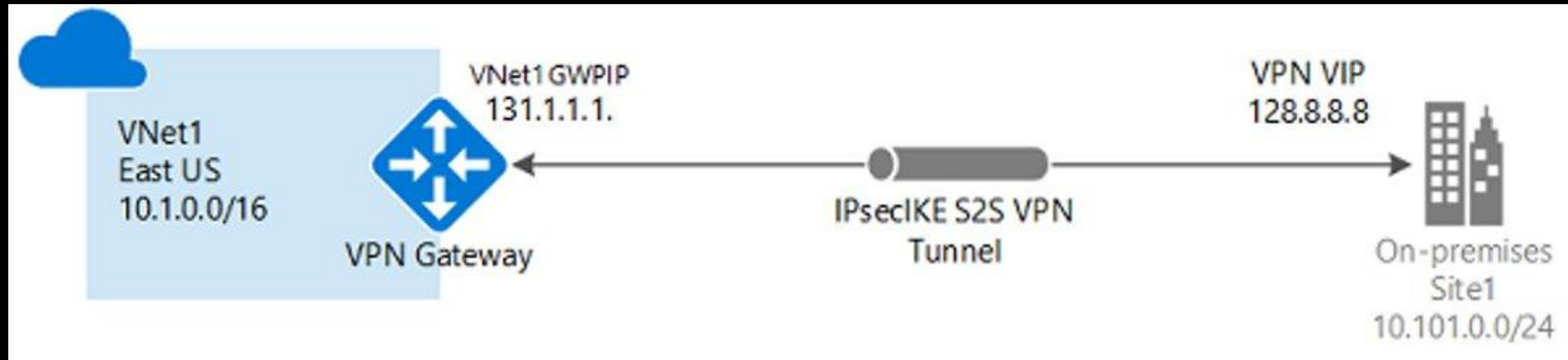


VPN Gateway Connections Overview

- VPN Gateways
- Implement Site-to-Site VPN Connections
- Create the Gateway Subnet
- VPN Gateway Configuration
- VPN Gateway Types
- VPN Gateway SKU and Generation
- Create the Local Network Gateway
- Configure the On-Premises VPN Device
- Create the VPN Connection
- High Availability Scenarios
- Demonstration – VPN Gateway



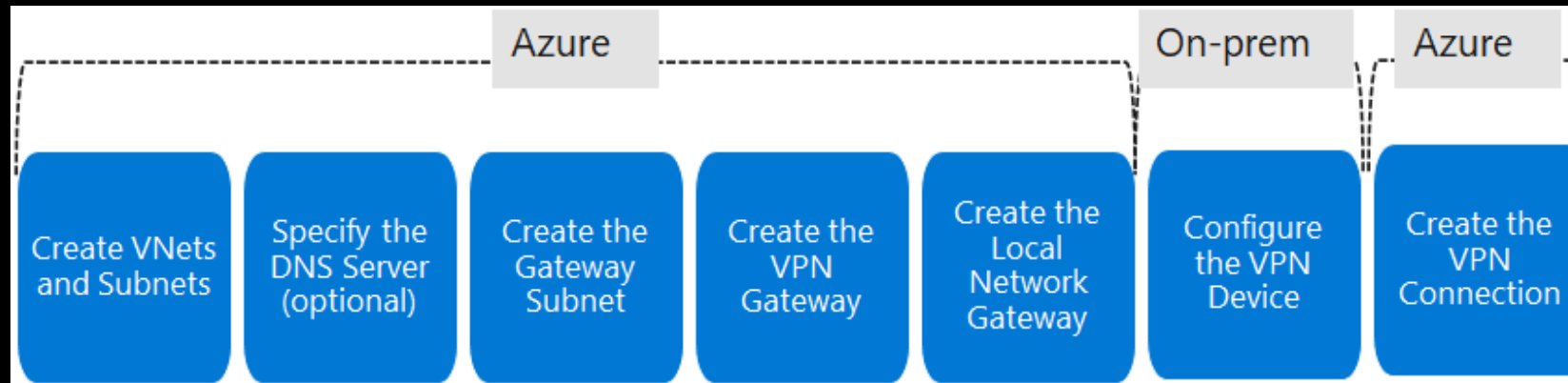
VPN Gateways



- **Site-to-site connections** connect on-premises datacenters to Azure virtual networks
- **Network-to-network connections** connect Azure virtual networks (custom)
- **Point-to-site (User VPN) connections** connect individual devices to Azure virtual networks



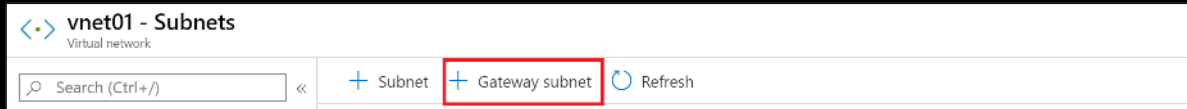
Implement Site-to-Site VPN Connections



- Take time to carefully plan your network configuration
- The on-premises part is necessary only if you are configuring Site-to-Site
- Always verify and test your connections



Create the Gateway Subnet



- The gateway subnet contains the IP addresses; if possible, use a CIDR block of /28 or /27.
- When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings.
- Never deploy other resources (for example, additional VMs) to the gateway subnet.
- Avoid associating a NSG with the gateway subnet.

Add subnet
vnet01

Name
GatewaySubnet

Address range (CIDR block) * ⓘ
10.1.255.0/27 ✓
10.1.255.0 - 10.1.255.31 (27 + 5 Azure reserved addresses)

NAT gateway ⓘ
None

Add IPv6 address space

Network security group
None

Route table
None

Service endpoints
Services ⓘ
0 selected

Subnet delegation
Delegate subnet to a service ⓘ
None



VPN Gateway Configuration

- Most VPN types are Route-based
- Your choice of gateway SKU affects the number of connections you can have and the aggregate throughput benchmark
- Associate a virtual network that includes the gateway subnet
- The gateway needs a public IP address

Create virtual network gateway

Instance details

Name *

Region *

Gateway type * ⓘ VPN ExpressRoute

VPN type * ⓘ Route-based Policy-based

SKU * ⓘ

Generation ⓘ

VIRTUAL NETWORK

Virtual network * ⓘ

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Enable active-active mode * ⓘ Enabled Disabled

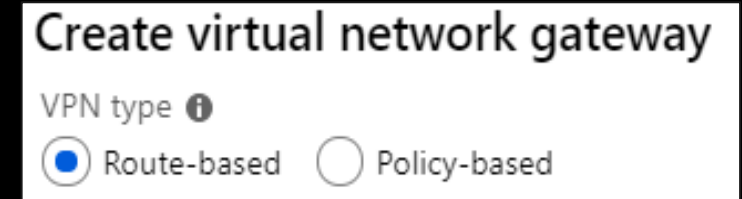
Configure BGP ASN * ⓘ Enabled Disabled

- ✓ It can take up to 45 minutes to provision the VPN gateway



VPN Gateway Types

- **Route-based VPNs** use *routes* in the IP forwarding or routing table to direct packets
 - Supports for IKEv2
 - Can use dynamic routing protocols
- **Policy-based VPNs** encrypt and direct packets through IPsec tunnels based on the IPsec policies.
 - Support for IKEv1 only
 - Legacy on-premises VPN devices



Most VPN Gateway configurations require a Route-based VPN



Gateway SKU and Generation

Sampling of available SKUs

SKU * ⓘ ▼

Generation ⓘ ▼

Gen	SKU	S2S/VNet-to-VNet Tunnels	P2S IKEv2 Connections	Throughput Benchmark
1	VpnGw1/Az	Max. 30	Max. 250	650 Mbps
1	VpnGw2/Az	Max. 30	Max. 500	1.0 Gbps
2	VpnGw2/Az	Max. 30	Max. 500	1.25 Gbps
1	VpnGw3/Az	Max. 30	Max. 1000	1.25 Gbps
2	VpnGw3/Az	Max. 30	Max. 1000	2.5 Gbps
2	VpnGw4/Az	Max. 30	Max. 5000	5.0 Gbps

- The Gateway SKU affects the connections and the throughput
- Resizing is allowed within the generation
- The Basic SKU (not shown) is legacy and should not be used



Create the Local Network Gateway

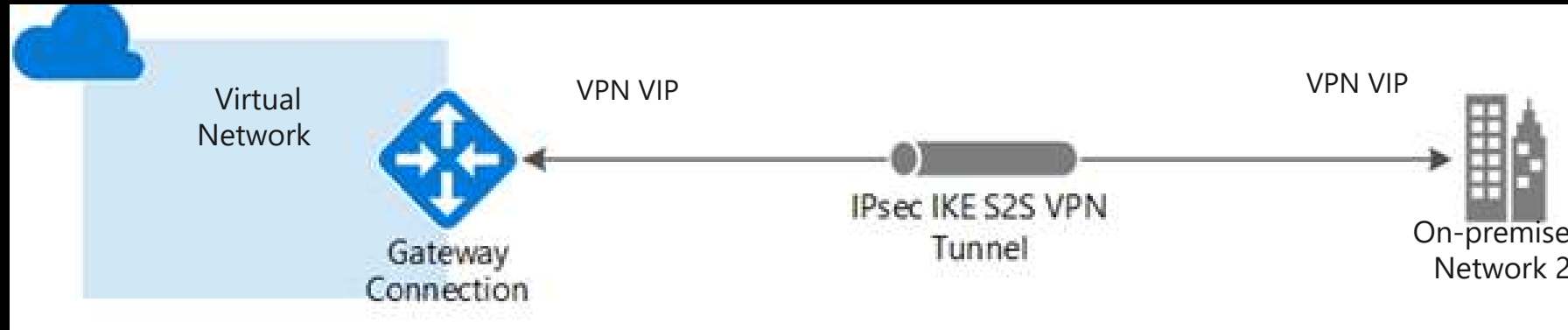
- Defines the on-premises network configuration
- Give the site a name by which Azure can refer to it
- The local gateway needs a public IP address
- Specify the IP address prefixes that will be routed through the gateway to the VPN device

The screenshot shows the 'Create local network gateway' form with the following fields and values:

- Name ***: VNet1LocalNet (with a green checkmark)
- IP address ***: 33.2.1.5 (with a green checkmark)
- Address space**: 192.168.3.0/24 (with a dropdown menu icon)
- Add additional address range**: (with a dropdown menu icon)
- Configure BGP settings**: (checkbox is unchecked)



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)



Create the VPN Connection

- Once your VPN gateway is created and the on-premises device is configured, create a connection object
- Configure a name for the connection and specify the type as Site-to-site (IPsec)
- Select the VPN Gateway and the Local Network Gateway
- Enter the Shared key for the connection

The screenshot shows the 'Add connection' dialog box in the Azure portal. The dialog is titled 'Add connection' and has a close button (X) in the top right corner. Below the title, there is a sub-header 'vng01'. The dialog is divided into two main sections: the left section for connection configuration and the right section for selecting a local network gateway.

Left Section (Add connection):

- Name ***: A text input field containing 'Azure-to-OnPrem' with a green checkmark on the right.
- Connection type ⓘ**: A dropdown menu showing 'Site-to-site (IPsec)' with a downward arrow.
- *Virtual network gateway ⓘ**: A field containing 'vng01' with a lock icon on the right.
- *Local network gateway ⓘ**: A field containing 'Azure-to-OnPrem' with a right-pointing arrow on the right.
- Shared key (PSK) * ⓘ**: A text input field containing 'abc123' with a green checkmark on the right.

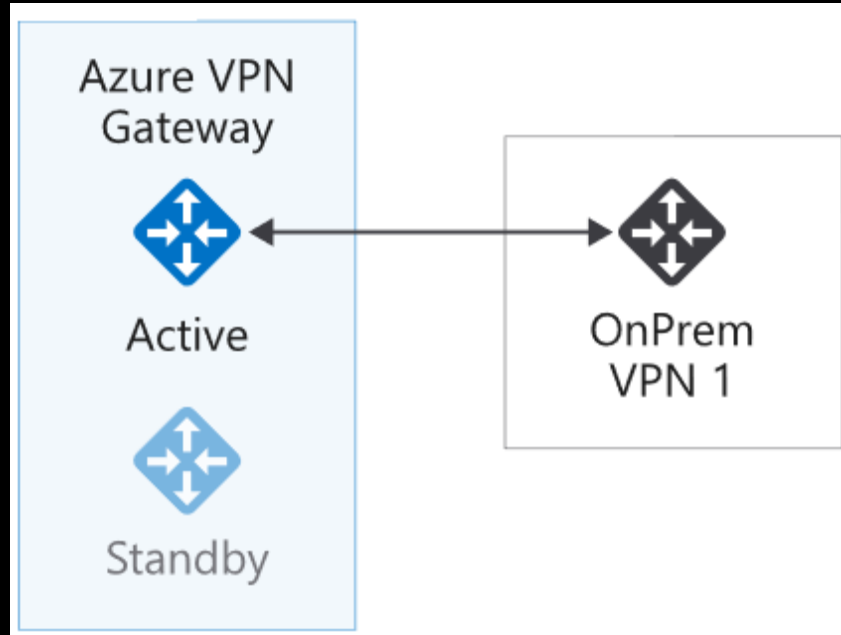
Right Section (Choose local network gat...):

- A 'Create new' button with a plus sign icon.
- A list item for 'Azure-to-OnPrem NetworkRG' with a green plus icon and a right-pointing arrow.

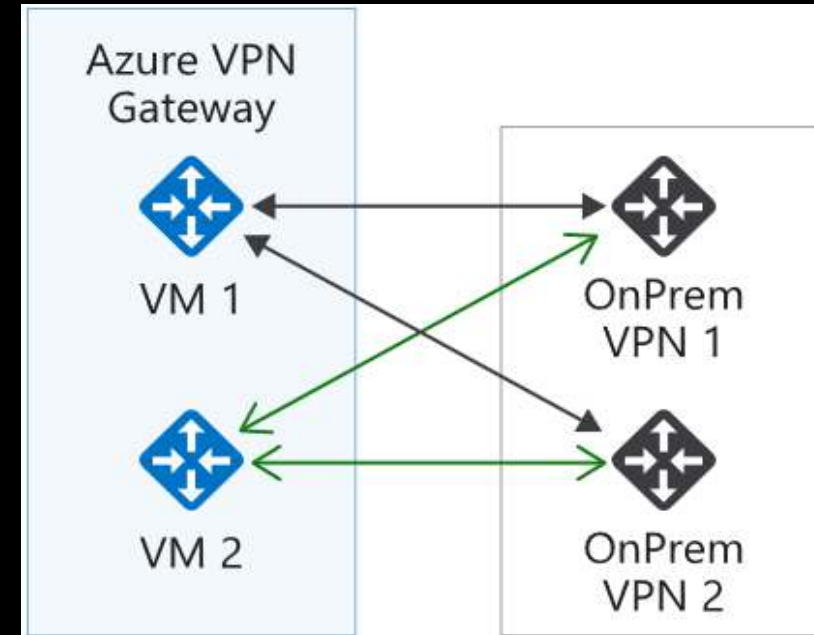


High Availability Scenarios

Active/standby (default)



Active/active



- VPN gateways are deployed as two instances
- Enable **active/active mode** for higher availability



Demonstration – VPN Gateways

- Explore the Gateway subnet blade
- Explore the Connected Devices blade
- Explore adding a virtual network gateway
- Explore adding a connection between the virtual networks



Azure Administrator Associate

EXAM: AZ-104



Module 05: Intersite Connectivity

#22: ExpressRoute and Virtual WAN

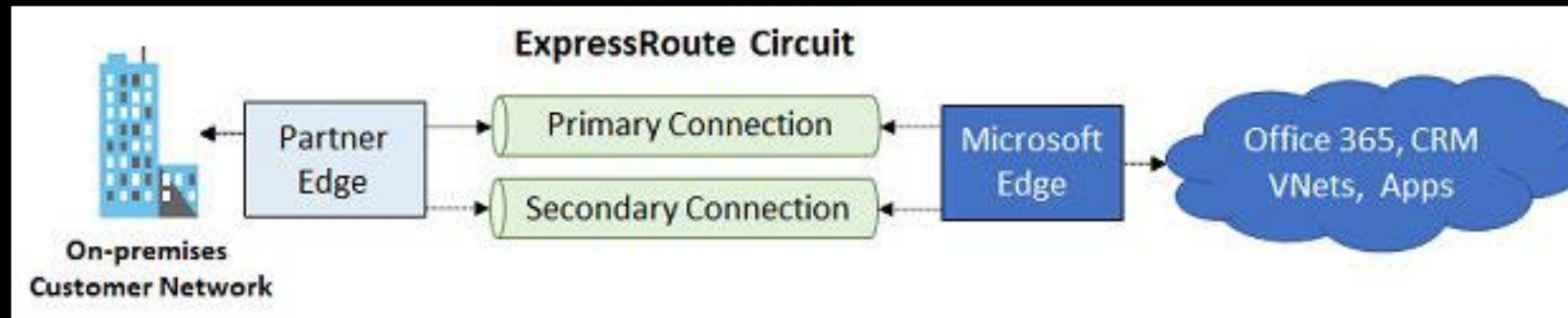


ExpressRoute and Virtual WAN Overview

- ExpressRoute
- ExpressRoute Capabilities
- Coexisting Site-to-Site and ExpressRoute
- Intersite Connection Comparisons
- Virtual WANs



ExpressRoute



- Private connections between your on-premises network and Microsoft datacenters
- Connections do not go over the public Internet – partner network
- Secure, reliable, low latency, high speed connections



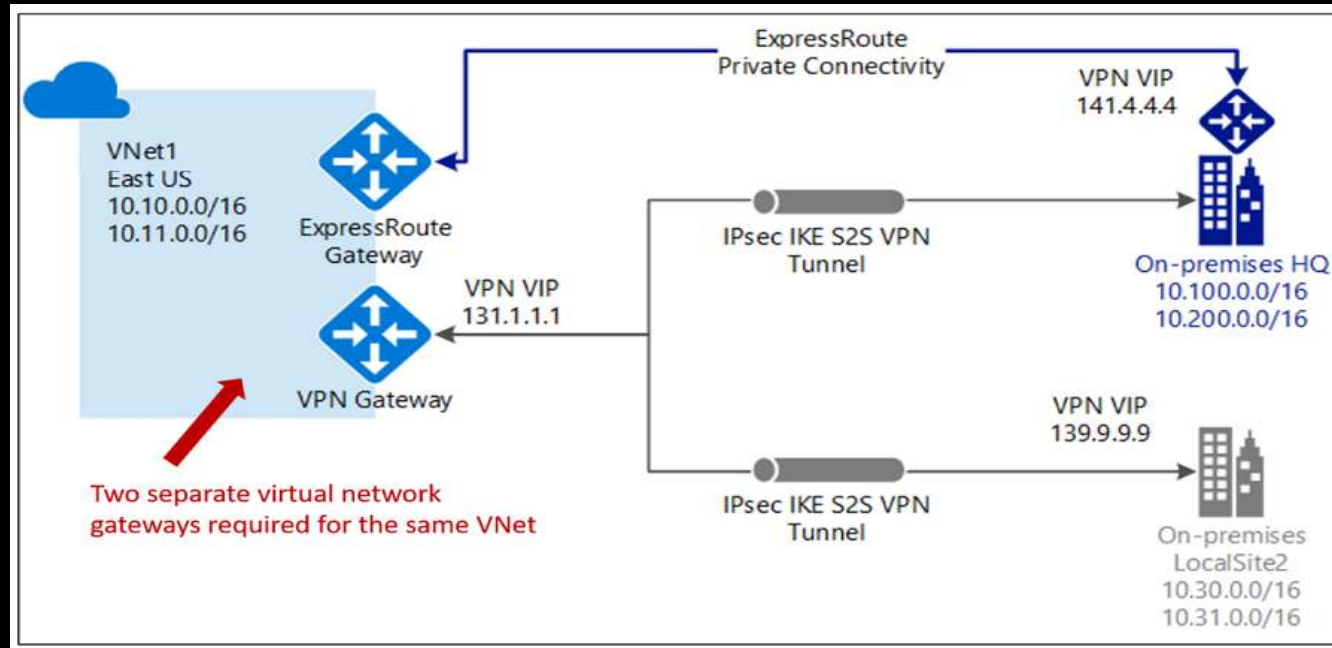
ExpressRoute Capabilities

- Layer 3 connectivity with redundancy
- Connectivity to all regions within a geography
- Global connectivity with ExpressRoute premium add-on
- Across on-premises connectivity with ExpressRoute Global Reach
- Bandwidth options – 50 Mbps to 100 Gbps
- Billing models – unlimited, metered, premium





Coexisting Site-to-Site and ExpressRoute



- Use S2S VPN as a secure failover path for ExpressRoute
- Use S2S VPNs to connect to sites that are not connected with ExpressRoute
- Notice two VNet gateways for the same virtual network

Intersite Connections Comparison

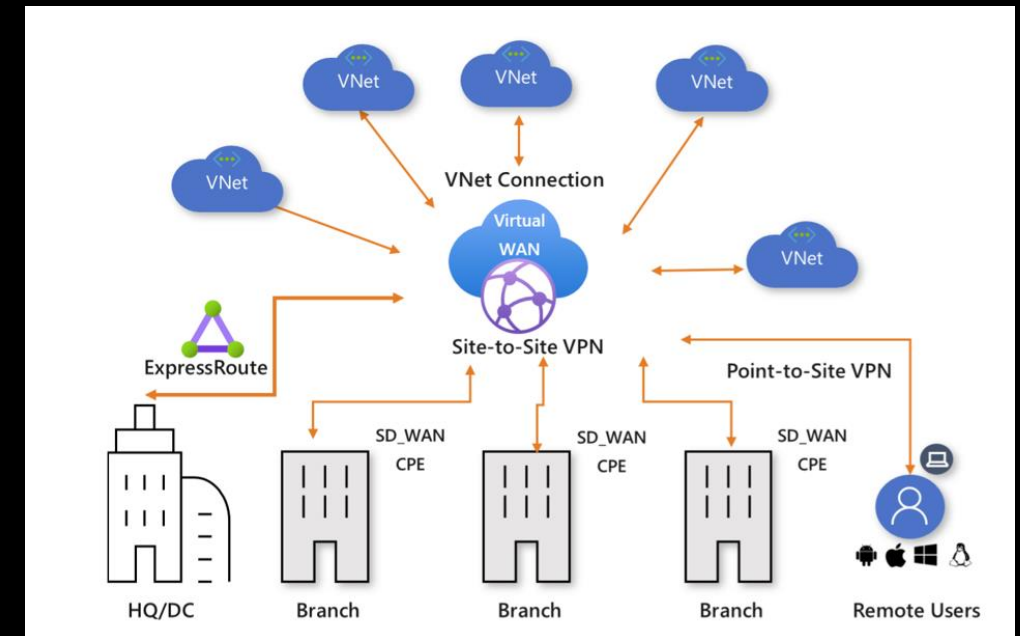


Connection	Azure services supported	Bandwidth	Protocols	Typical use case
Virtual network, point-to-site	Azure IaaS services, Azure Virtual Machines	Based on the gateway SKU	Active/passive	Dev, test, and lab environments for cloud services and virtual machines.
Virtual network, site-to-site	Azure IaaS services, Azure Virtual Machines	Typically < 1 Gbps aggregate	Active/passive Active/active	Dev, test, and lab environments. Small-scale production workloads and virtual machines.
ExpressRoute	Azure IaaS and PaaS services, Microsoft Office 365 services	50 Mbps up to 100 Gbps	Active/active	Enterprise-class and mission-critical workloads. Big data solutions.



Virtual WANs

- Brings together S2S, P2S, and ExpressRoute
- Integrated connectivity using a hub-and-spoke connectivity model
- Connect virtual networks and workloads to the Azure hub automatically
- Visualize the end-to-end flow within Azure
- Two types: Basic and Standard





Azure Administrator Associate

EXAM: AZ-104



Module 05: Intersite Connectivity

#23: Review Questions



Review Question 1

You want to connect different VNets in the same region as well as different regions and decide to use VNet peering to accomplish this. Which of the following statements are true benefits of VNet peering? Select two.

- The virtual networks can exist in any Azure cloud region.
- Network traffic between peered virtual networks is private.
- Peering is easy to configure and manage, requiring little to no downtime.
- Gateway transit can be configured regionally or globally.



Review Question 2

Your company is preparing to implement a Site-to-Site VPN to Microsoft Azure. You are selected to plan and implement the VPN. Currently, you have an Azure subscription, an Azure virtual network, and an Azure gateway subnet. You need to prepare the on-premises environment and Microsoft Azure to meet the prerequisites of the Site-to-Site VPN. Later, you will create the VPN connection and test it. What should you do? (Each answer presents part of the solution. Select three.)

- Obtain a VPN device for the on-premises environment.
- Obtain a VPN device for the Azure environment.
- Create a virtual network gateway (VPN) and the local network gateway in Azure.
- Create a virtual network gateway (ExpressRoute) in Azure.
- Obtain a public IPv4 IP address without NAT for the VPN device.
- Obtain a public IPv4 IP address behind NAT for the VPN device.



Review Question 3

Your company is preparing to implement persistent connectivity to Microsoft Azure. The company has a single site, headquarters, which has an on-premises data center. The company establishes the following requirements for the connectivity:

- **Connectivity must be persistent.**
- **Connectivity must provide for the entire on-premises site.**

You need to implement a connectivity solution to meet the requirements. What should you do? Select one.

- Implement a Site-to-Site VPN.
- Implement a Virtual Private Cloud (VPC).
- Implement a Virtual Private Gateway (VGW).
- Implement a VNet-to-VNet VPN.
- Implement a Point-to-Site VPN.



Review Question 4

You are configuring VNet Peering across two Azure virtual networks, VNET1 and VNET2. You are configuring the VPN Gateways. You want VNET2 to be able to use VNET1's gateway to get to resources outside the peering. What should you do? Select one.

- Select allow gateway transit on VNET1 and use remote gateways on VNET2.
- Select allow gateway transit on VNET2 and use remote gateways on VNET1.
- Select allow gateway transit and use remote gateways on both VNET1 and VNET2.
- Do not select allow gateway transit or use remote gateways on either VNET1 or VNET2.



Review Question 5

You are configuring a site-to-site VPN connection between your on-premises network and your Azure network. The on-premises network uses a Cisco ASA VPN device. You have checked to ensure the device is on the validated list of VPN devices. Before you proceed to configure the device what two pieces of information should you ensure you have? Select two.

- The shared access signature key from the recovery services vault.
- The shared key you provided when you created your site-to-site VPN connection.
- The gateway routing method provided when you created your site-to-site VPN connection.
- The static IP address of your virtual network gateway.
- The public IP address of your virtual network gateway.
- The user and password for the virtual network gateway.



Review Question 6

You manage a large datacenter that is running out of space. You propose extending the datacenter to Azure using a Multi-Protocol Label Switching virtual private network. Which connectivity option would you select? Select one.

- Point-to-Site
- VPN Peering
- Multi-site
- Site-to-Site
- ExpressRoute
- VNet-to-VNet



Review Question 7

You are creating a connection between two virtual networks. Performance is a key concern. Which of the following will most influence performance? Select one.

- Ensuring you select a route-based VPN.
- Ensuring you select a policy-based VPN.
- Ensuring you specify a DNS server.
- Ensuring you select an appropriate Gateway SKU.



Review Question 8

Your manager asks you to verify some information about Azure Virtual WANs. Which of the following statements are true? Select three.

- You must use one of the approved connectivity partner providers.
- You must use a VPN device that provides IKEv2/IKEv1 IPsec support.
- Virtual WAN supports ExpressRoute.
- Virtual WAN supports site-to-site connections.
- Virtual WAN does not support point-to-site connections.
- You can switch between the Basic and Standard plans



Azure Administrator Associate

EXAM: AZ-104



Module 06: Network Traffic Management

#24: Network Routing & Endpoints



Network Routing Overview

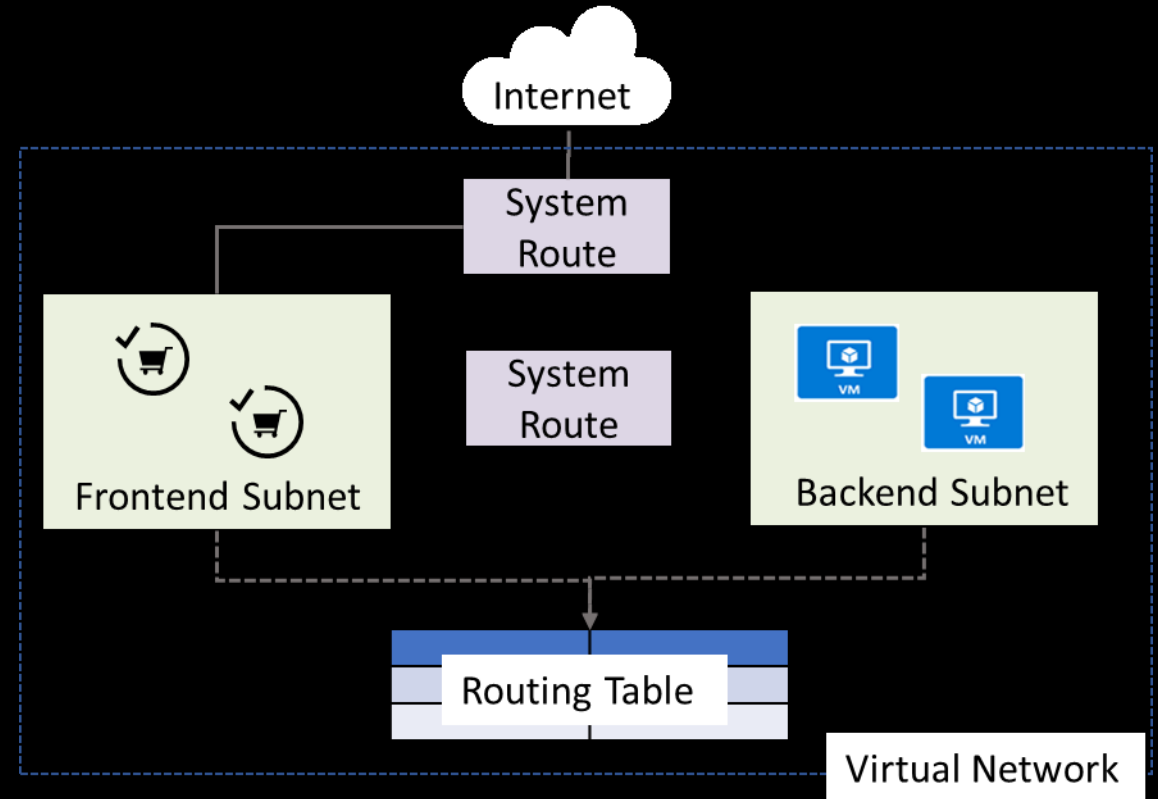
- System Routes
- User Defined Routes
- Routing Example
- Create a Routing Table
- Create a Custom Route
- Associate the Route Table
- Demonstration – Custom Routing Tables
- Service Endpoints
- Service Endpoint Services
- Private Link



System Routes

System routes direct network traffic between virtual machines, on-premises networks, and the Internet

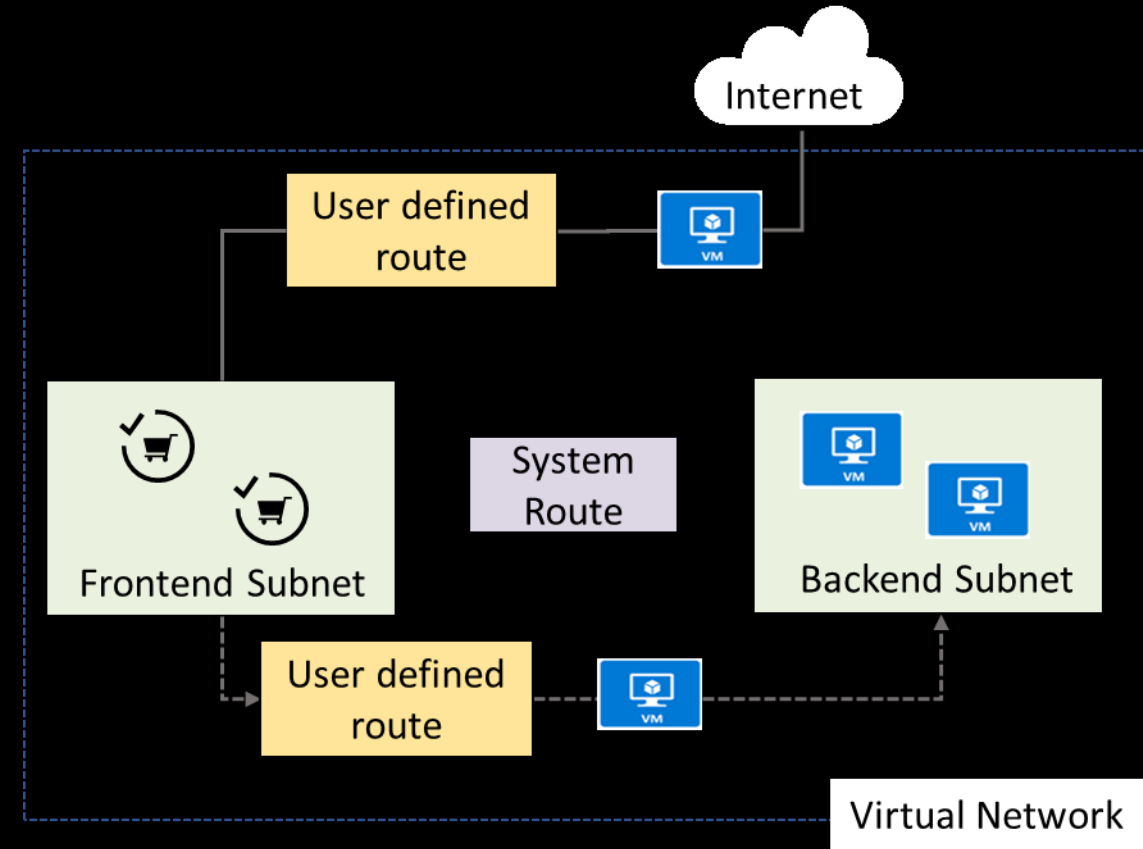
- Traffic between VMs in the same subnet
- Between VMs in different subnets in the same virtual network
- Data flow from VMs to the Internet
- Communication between VMs using a VNet-to-VNet VPN
- Site-to-Site and ExpressRoute communication through the VPN gateway





User Defined Routes

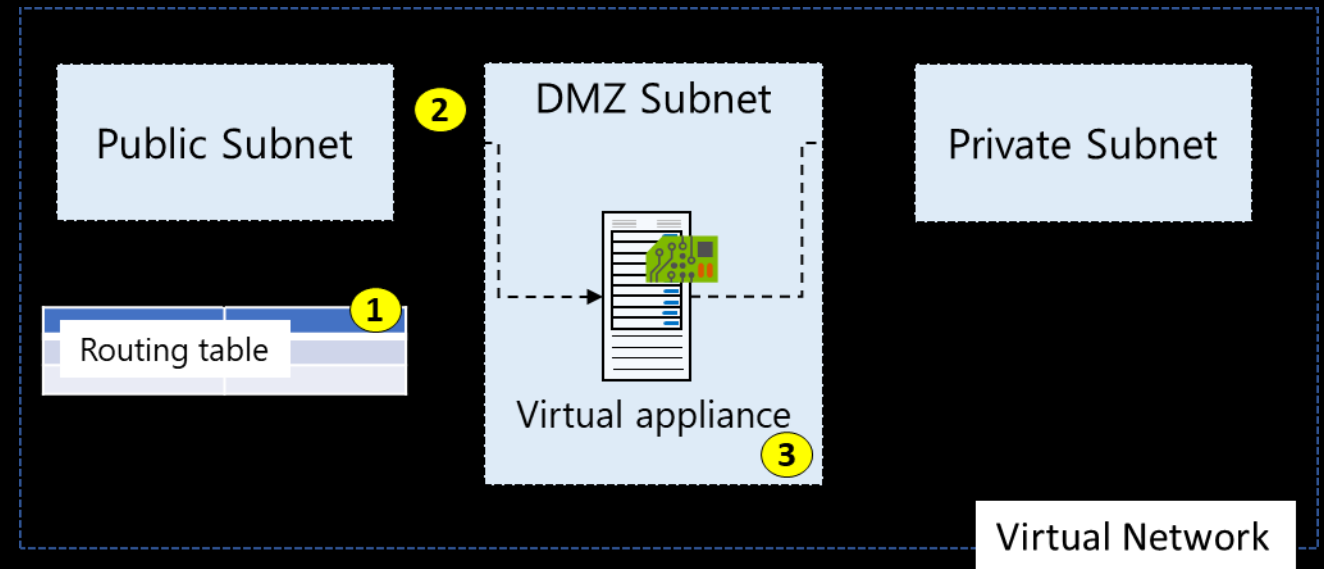
- A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network
- User-defined routes are custom routes that control network traffic by defining routes that specify the next hop of the traffic flow
- The next hop can be a virtual network gateway, virtual network, internet, or virtual appliance





Routing Example

All traffic coming into the public subnet and headed for the private subnet must go through the virtual network appliance



- Create a routing table
- Add a custom route that requires all private subnet traffic be directed to a network appliance
- Associate the new route to the public subnet



Create a Routing Table

- A standard routing protocol is used to exchange routing and reachability information between two or more networks
- Routes are automatically added to the route table of all subnets with virtual network gateway route propagation enabled
- In most situations you will want to enable route propagation

Create route table

You can add routes to this table after it's created.

* Name
myRouteTablePublic ✓

* Subscription
Visual Studio Enterprise ▼

* Resource group
myRGWest ▼
[Create new](#)

* Location
(US) West US ▼

Virtual network gateway route propagation
Disabled **Enabled**

[Create](#) [Automation options](#)



Create a Custom Route

- When you create a route there are several Next hop types
- In this example, any private subnet IP addresses will be sent to the virtual appliance
- Other choices are Virtual network gateway, Virtual network, Internet, and None

Add route
myRouteTablePublic

Route name *
ToPrivateSubnet ✓

Address prefix * ⓘ
10.0.1.0/24 ✓

Next hop type ⓘ

- Virtual network gateway ^
- Virtual network gateway
- Virtual network
- Internet
- Virtual appliance**
- None



Associate the Route Table

- Each subnet can have zero or one route table associated to it
- In our example, the Public subnet will be associated with the routing table

Add subnet ✕

VNet1

Name *

Public ✓

Address range (CIDR block) * ⓘ

10.0.1.0/24 ✓

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

NAT gateway ⓘ

None ▾

Add IPv6 address space

Network security group

None ▾

Route table

myRouteTablePublic ▾



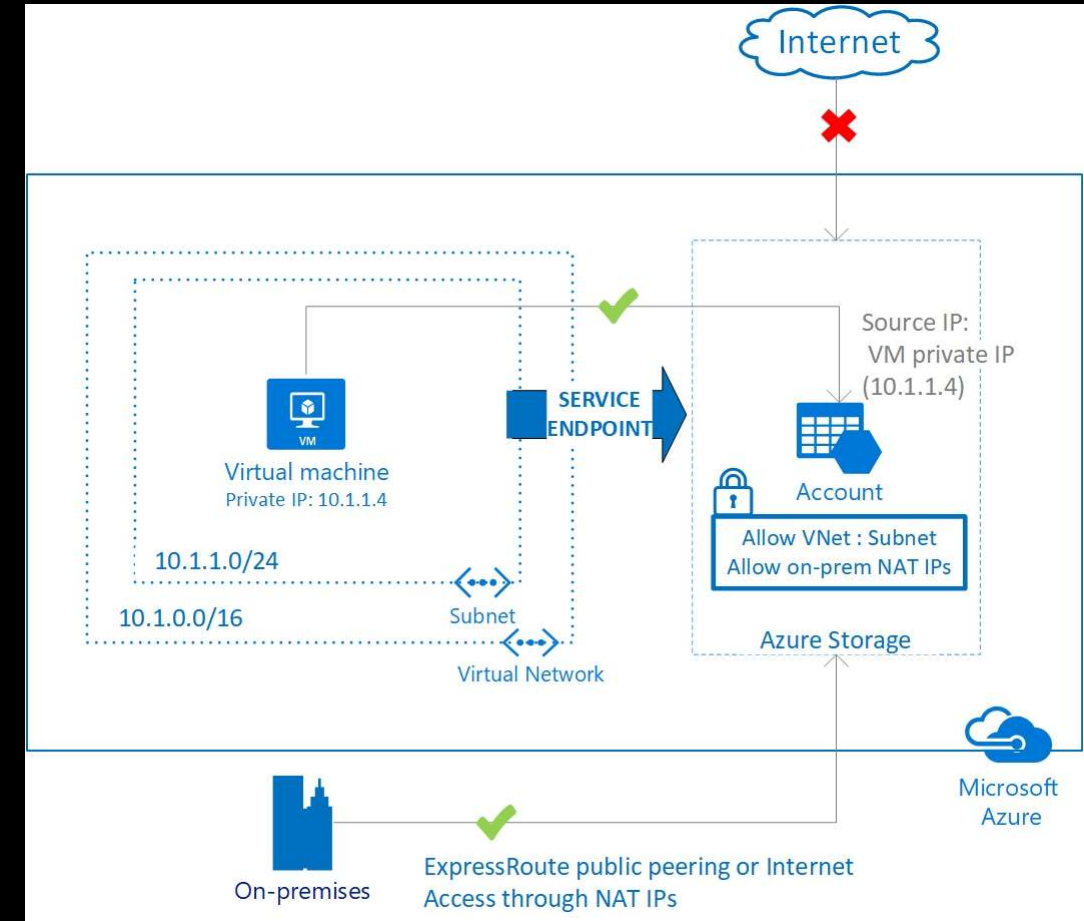
Demonstration – Custom Routing Tables

- Create a route table
- Add a route
- Associate a route table to a subnet
- Use PowerShell to view your routing information



Service Endpoints

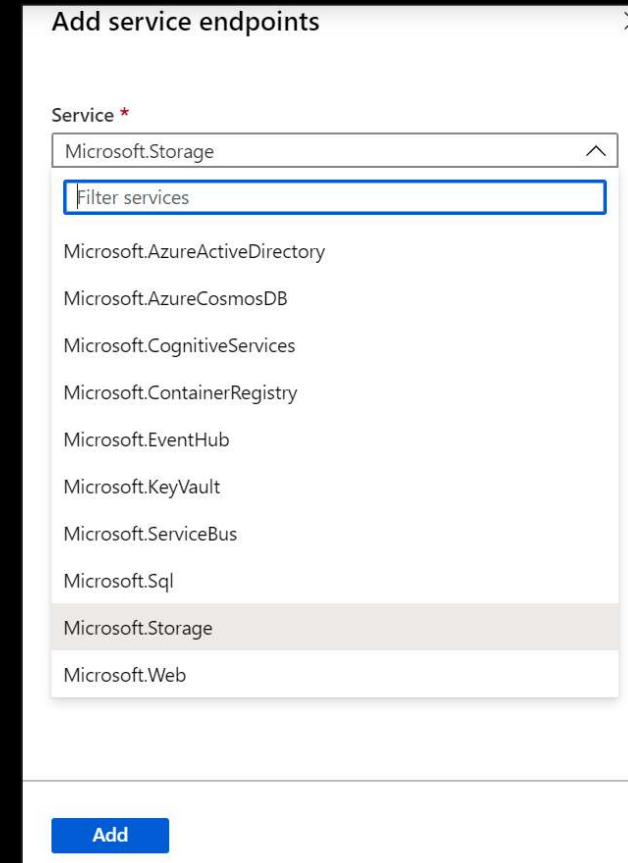
- Endpoints limit network access to specific subnets and IP addresses
- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Endpoints use the Microsoft Azure backbone network
- Simple to set up with less management overhead





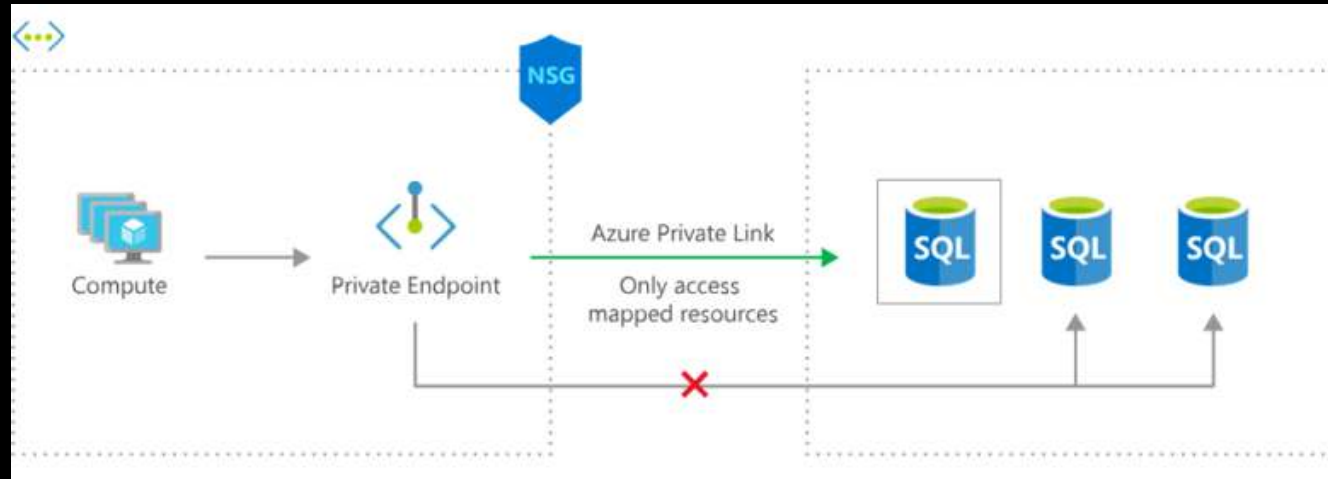
Service Endpoint Services

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





Private Link



- Private connectivity to services on Azure. Traffic remains on the Microsoft network, with no public internet access
- Integration with on-premises and peered networks
- In the event of a security incident within your network, only the mapped resource would be accessible



Azure Administrator Associate

EXAM: AZ-104



Module 06: Network Traffic Management

#25: Azure Load Balancer

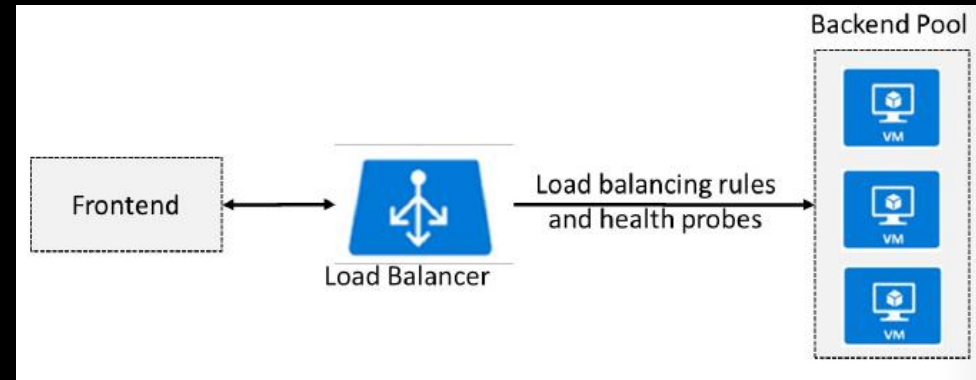


Azure Load Balancer Overview

- Azure Load Balancer
- Public Load Balancer
- Internal Load Balancer
- Load Balancer SKUs
- Backend Pools
- Load Balancer Rules
- Session Persistence
- Health Probes



Azure Load Balancer

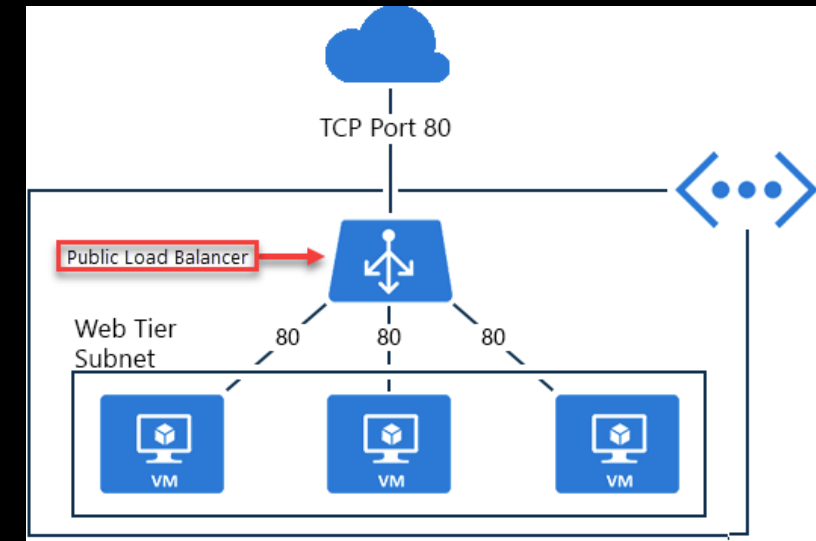


- Distributes inbound traffic to backend resources using load-balancing rules and health probes
- Can be used for both inbound/outbound scenarios
- Two types: Public and Internal



Public Load Balancer

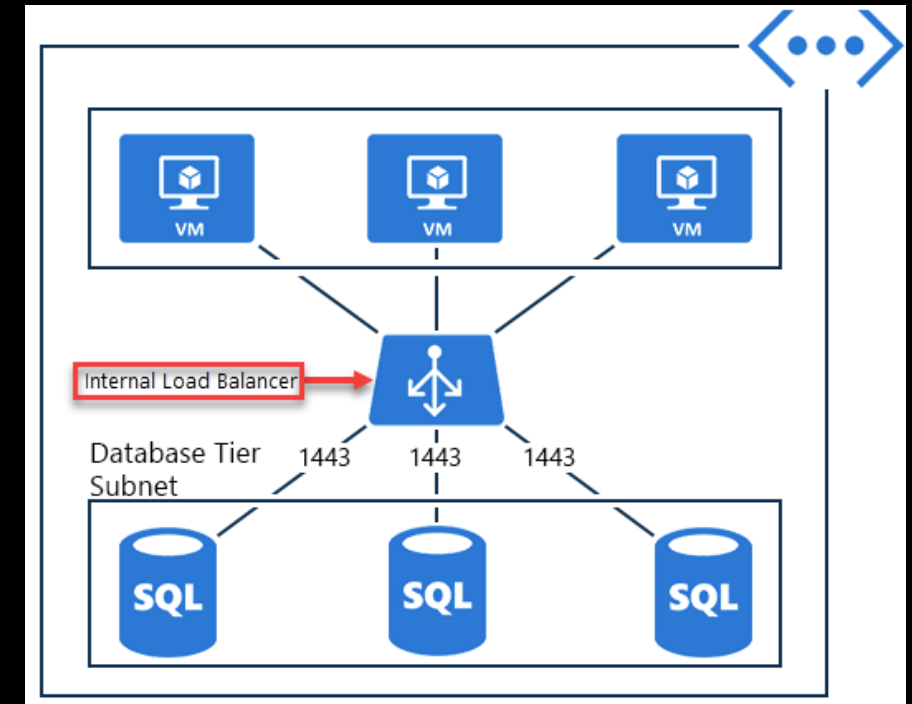
- Maps public IP addresses and port number of incoming traffic to the VM's private IP address and port number, and vice versa.
- Apply load balancing rules to distribute traffic across VMs or services.





Internal Load Balancer

- Directs traffic only to resources inside a virtual network or that use a VPN to access Azure infrastructure.
- Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint.
- Enables load balancing within a virtual network, for cross-premises virtual networks, for multi-tier applications, and for line-of-business applications.

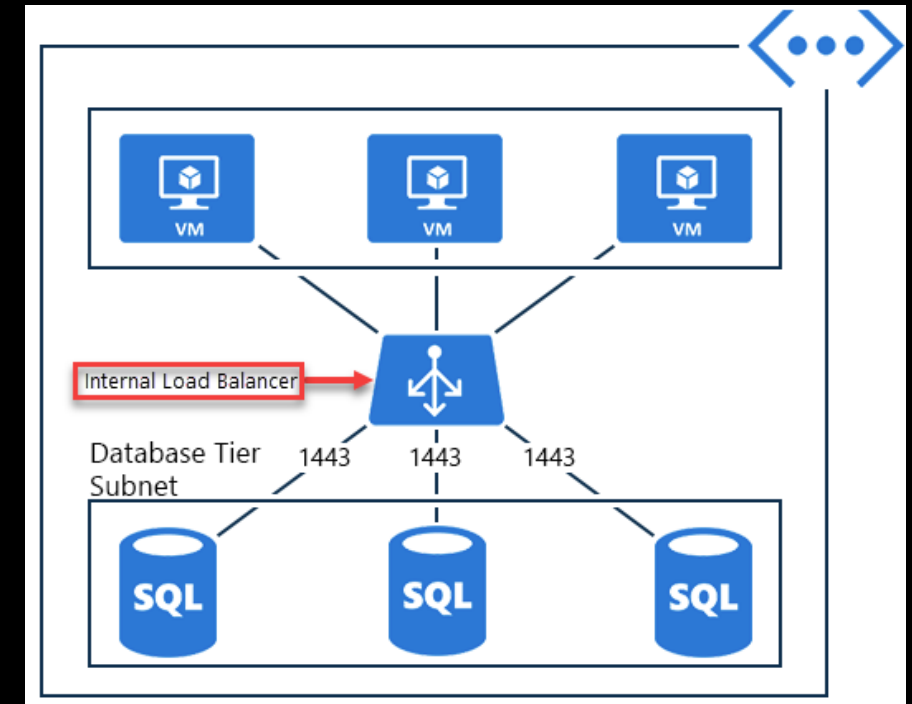




Internal Load Balancer

Types of Load Balancing

- Within a Virtual network
- For a cross-premises virtual network
- For multi-tier applications
- For line-of-business applications





Load Balancer SKUs

- Load balancer supports both Basic and Standard (newer) SKUs
- SKUs are not mutable
- Load Balancer rule cannot span two virtual networks
- No charge for the Basic Load Balancer SKU

Instance details

Name *
lb01 ✓

Region *
(US) East US ✓

Type * ⓘ
 Internal Public

SKU * ⓘ
 Basic Standard

Configure virtual network.

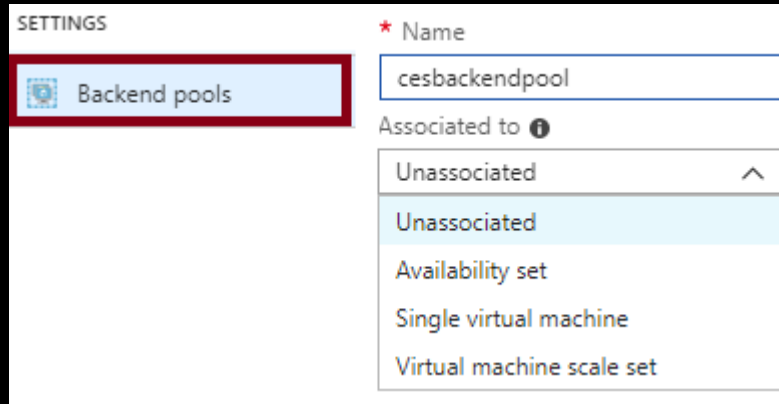
Virtual network * ⓘ
vnet01 ✓

Subnet *
subnet01 (10.1.0.0/24) ✓
[Manage subnet configuration](#)

IP address assignment *
 Static Dynamic



Backend Pools



To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer

SKU	Backend pool endpoints
Basic SKU	VMs in a single availability set or VM scale set.
Standard SKU	Any VM in a single virtual network, including a blend of VMs, availability sets, and VM scale sets.



Load Balancer Rules

- Maps a frontend IP and port combination to a set of backend IP addresses and port combination
- Rules can be used in combination with NAT rules
- A NAT rule is explicitly attached to a VM (or network interface) to complete the path to the target

Add load balancing rule

lb01

Name *
lbr01 ✓

IP Version *
 IPv4 IPv6

Frontend IP address * ⓘ
10.1.0.4 (LoadBalancerFrontEnd) ▾

Protocol
 TCP UDP

Port *
80

Backend port * ⓘ
80

Backend pool ⓘ
bep01 ▾

Health probe ⓘ
hp01 (HTTP:80) ▾

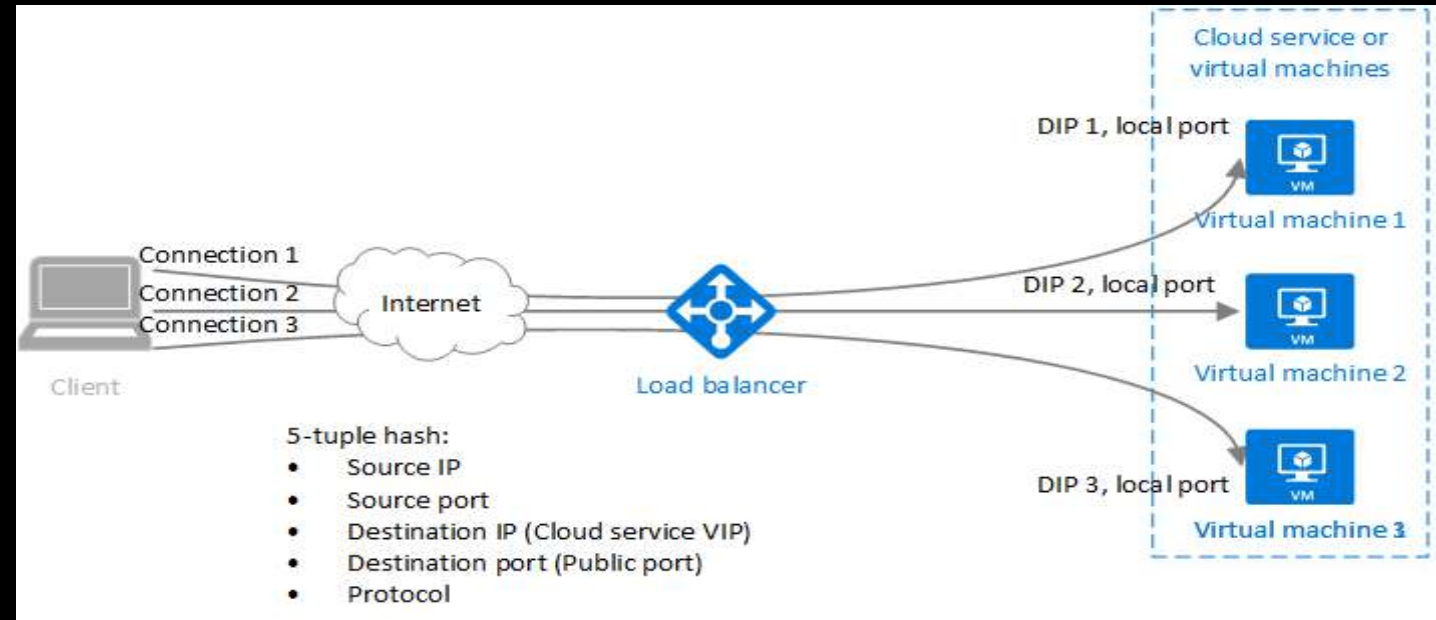
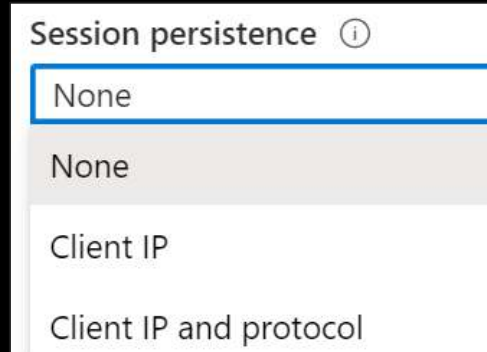
Session persistence ⓘ
None ▾

Idle timeout (minutes) ⓘ
 4

Floating IP (direct server return) ⓘ
 Disabled Enabled



Session Persistence



- Session persistence specifies how client traffic is handled
- **None** (default) requests can be handled by any virtual machine
- **Client IP** requests will be handled by the same virtual machine
- **Client IP and protocol** specifies that successive requests from the same address and protocol will be handled by the same virtual machine



Health Probes

- Allows the load balancer to monitor the status of an app
- Dynamically adds or removes VMs from the load balancer rotation based on their response to health checks
- HTTP custom probe (preferred) pings every 15 seconds
- TCP custom probe tries to establish a successful TCP session

The screenshot shows a configuration window titled "Add health probe" for a load balancer named "lb01". The form contains the following fields:

- Name ***: A text input field containing "hp01" with a green checkmark on the right.
- Protocol ⓘ**: A dropdown menu with "HTTP" selected.
- Port * ⓘ**: A text input field containing "80".
- Path * ⓘ**: A text input field containing "/".
- Interval * ⓘ**: A text input field containing "5", with the unit "seconds" indicated below.
- Unhealthy threshold * ⓘ**: A text input field containing "2", with the unit "consecutive failures" indicated below.



Azure Administrator Associate

EXAM: AZ-104



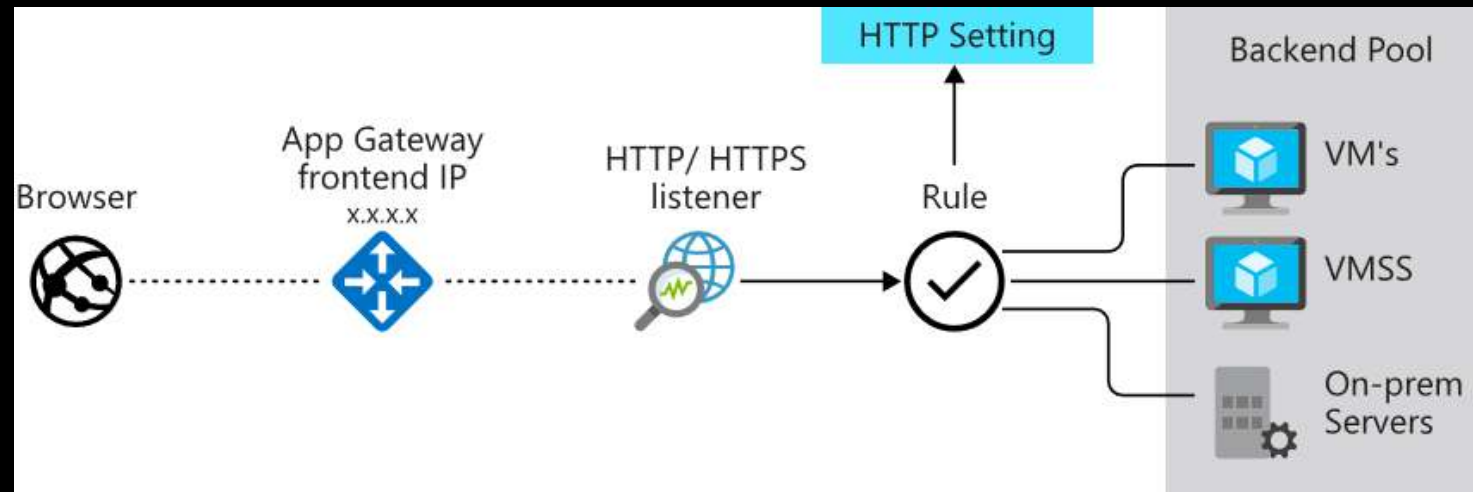
Module 06: Network Traffic Management

#26: Azure Application Gateway



Application Gateway

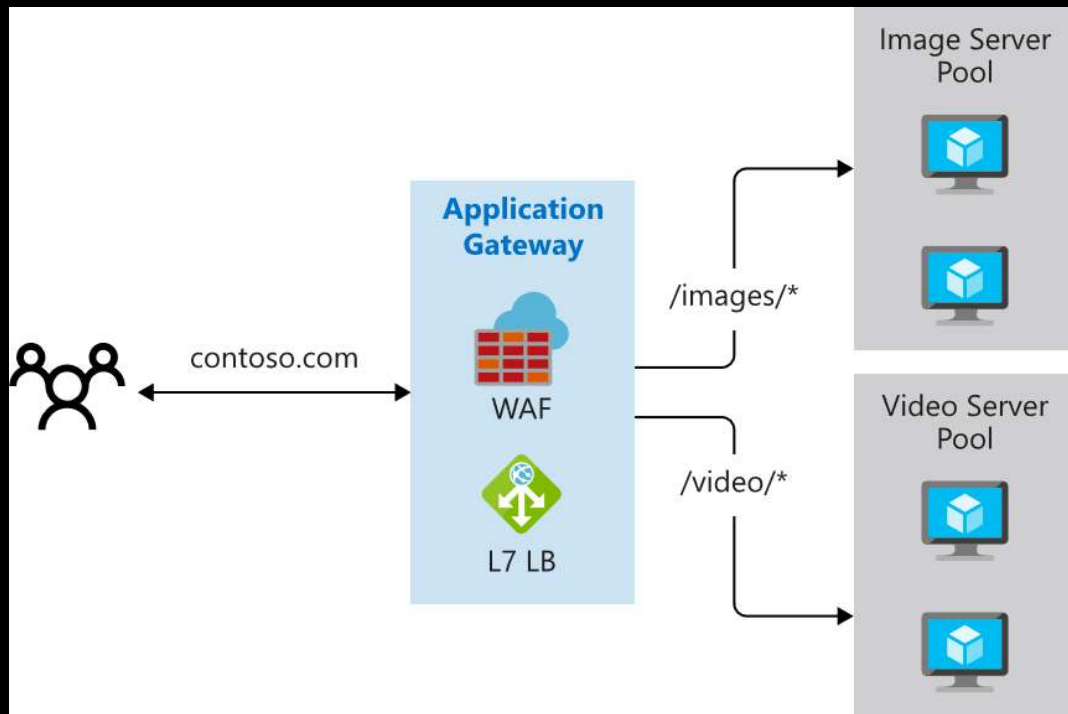
- Manages web app requests
- Routes traffic to a pool of web servers based on the URL of a request
- The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers



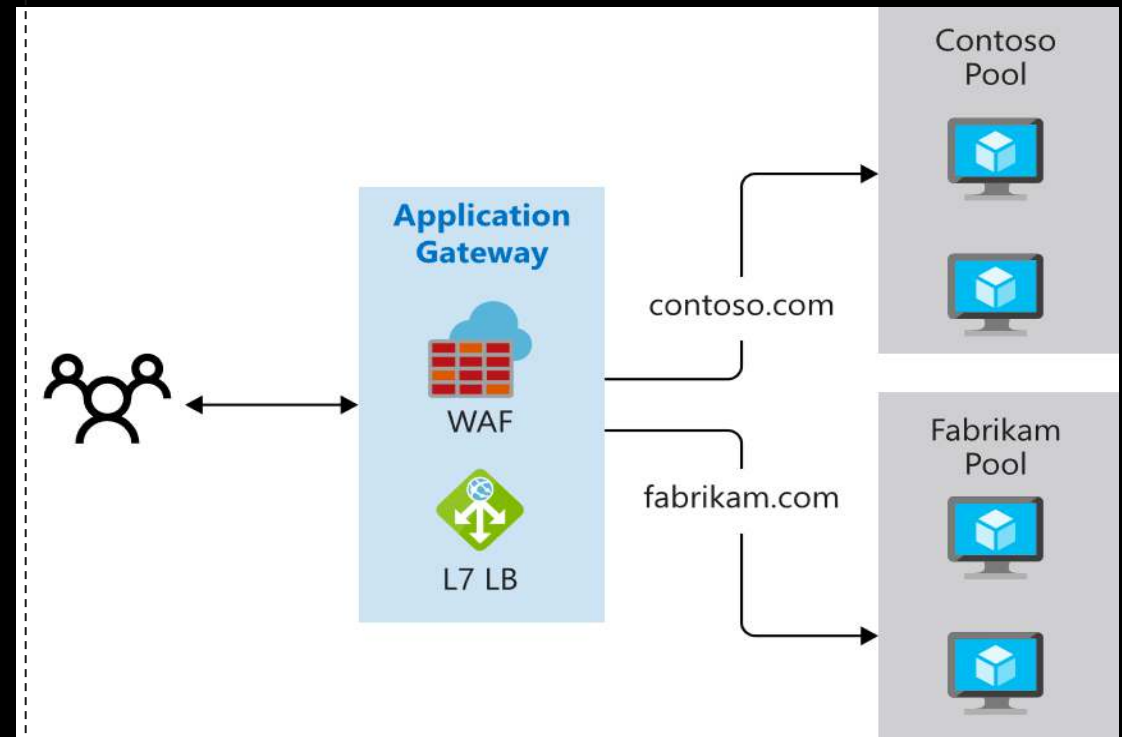
Application Gateway Routing



Path-based routing



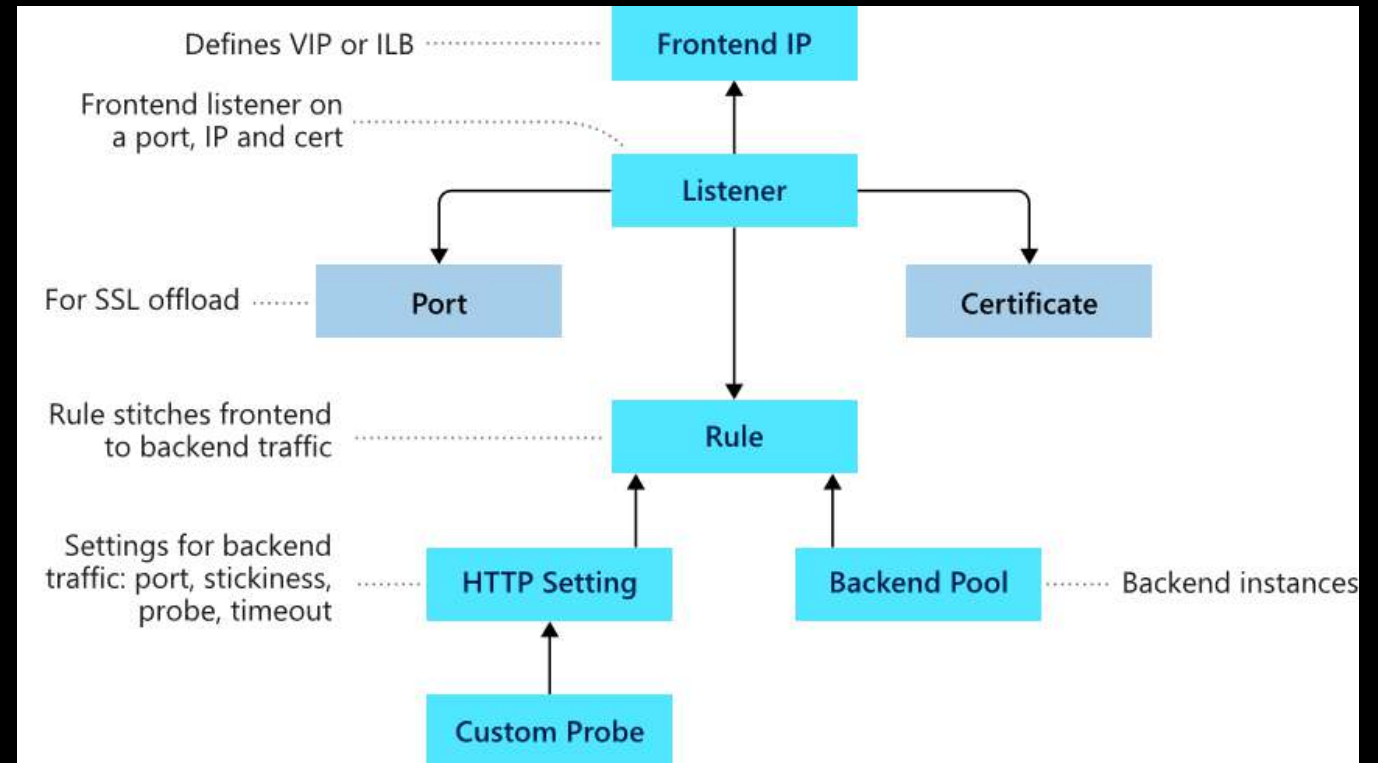
Multiple-site routing





Application Gateway Components

- Frontend IP
- Listeners
- Routing rules
- Backend pools
- Web application firewall (optional)
- Health probes





Azure Administrator Associate

EXAM: AZ-104



Module 06: Network Traffic Management

#27: Azure Traffic Manager



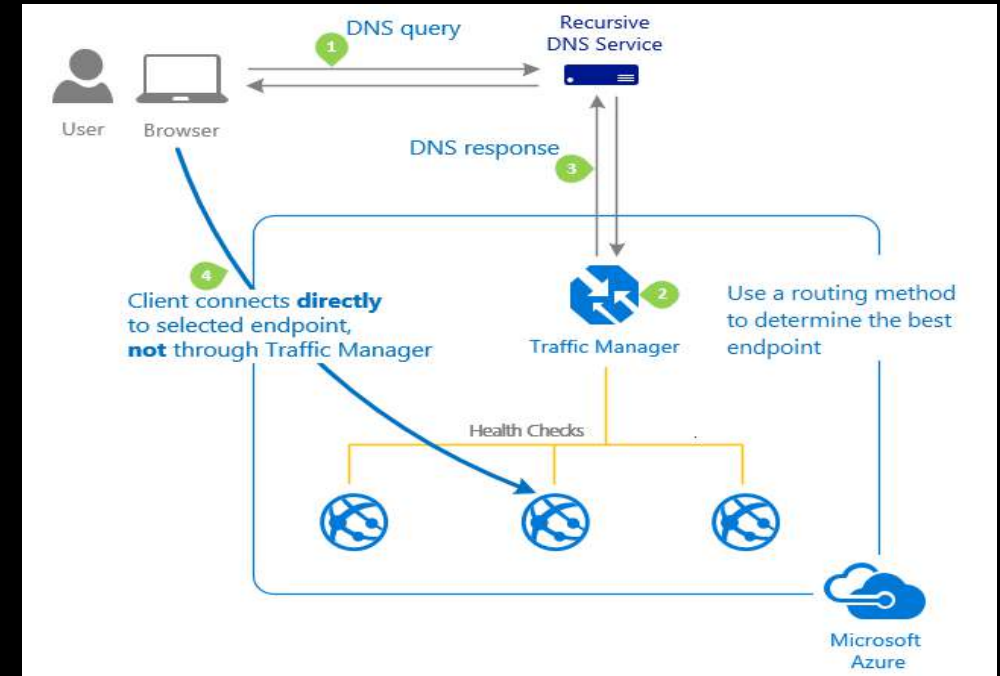
Traffic Manager Overview

- Azure Traffic Manager
- Traffic Manager Routing Methods
- Distributing Network Traffic



Azure Traffic Manager

- Allows you to control distribution of user traffic to service endpoints around the world
- Uses DNS to direct end-user requests to the most appropriate endpoint
- Selects an endpoint based on the configuring traffic-routing method
- Provides endpoint health checks and automatic endpoint failover

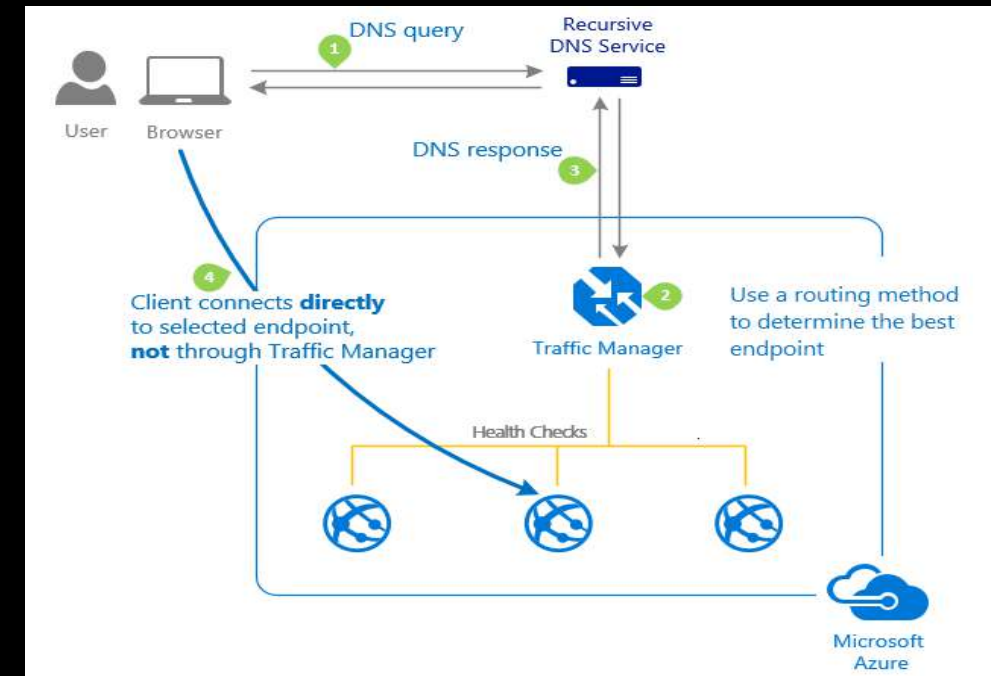




Azure Traffic Manager

Benefits

- Improve availability of critical applications
- Improve responsiveness for high performance applications
- Upgrade and perform service maintenance without downtime
- Combine on-premises and Cloud-based applications
- Distribute traffic for large, complex deployments





Traffic Manager Routing Methods

- **Priority** routing routes traffic to a prioritized list of service endpoints
- **Performance** routing Routes traffic to the location closest to the user
- **Geographic** routing routes traffic to a set of geographic locations
- **Weighted** routing distributes traffic evenly using a pre-defined weighting
- **MultiValue** routing distributes traffic only to IPv4 and IPv6 endpoints
- **Subnet** routing distributes traffic based on source IP ranges

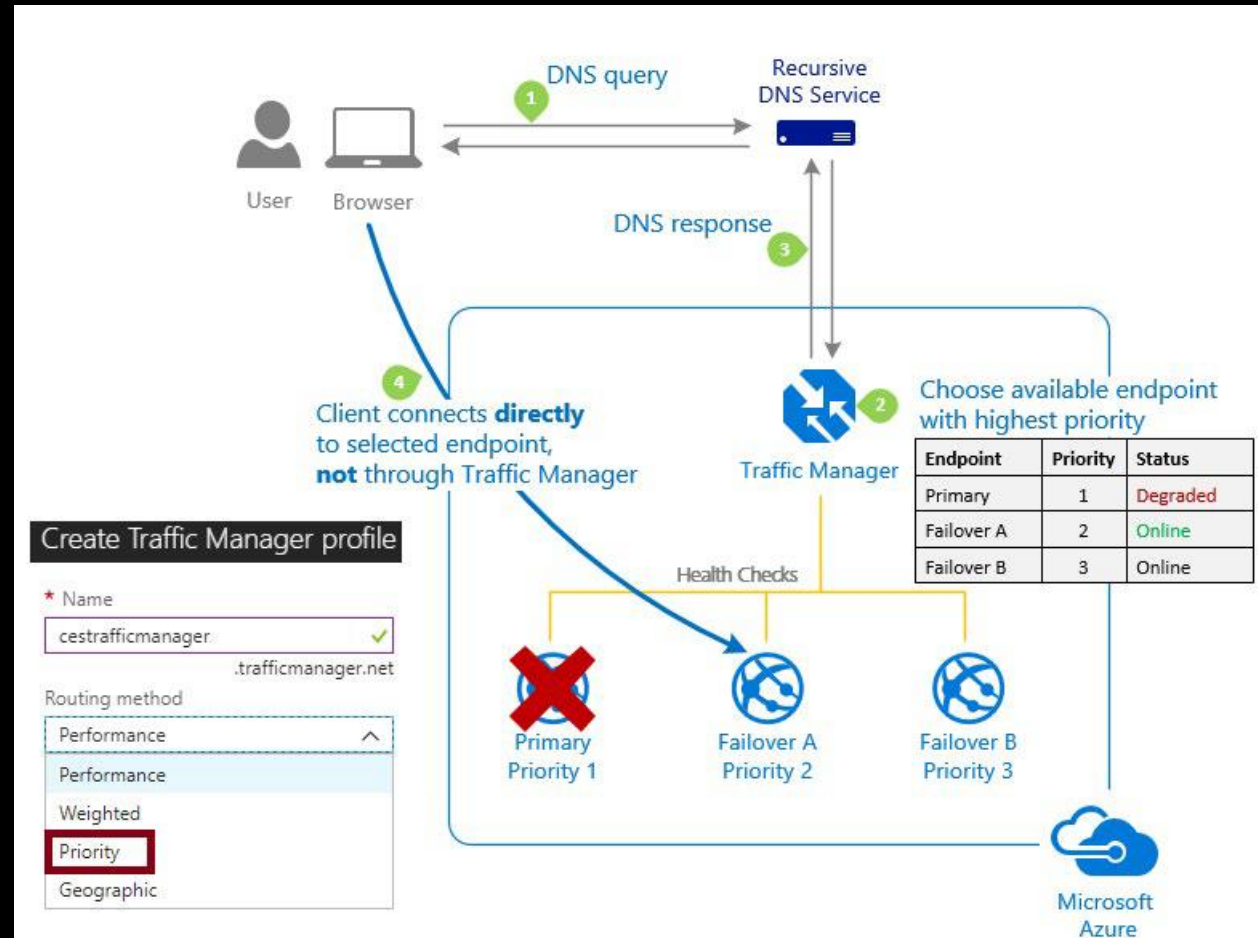
Create Traffic Manager profile

Name *
SouthEastTM3 ✓
.trafficmanager.net

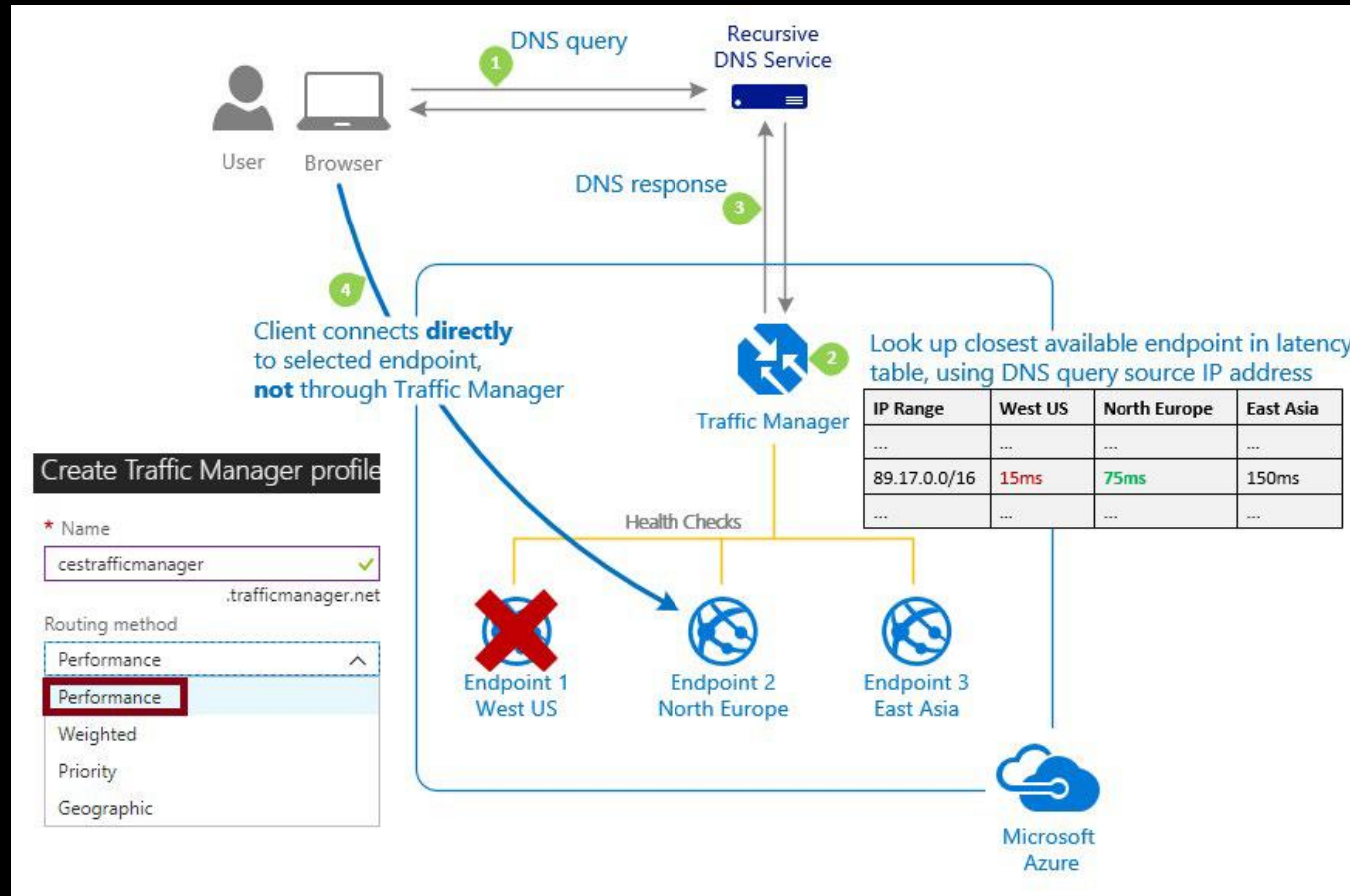
Routing method
Weighted ^
Performance
Weighted
Priority
Geographic
MultiValue
Subnet



Traffic Manager Priority Routing

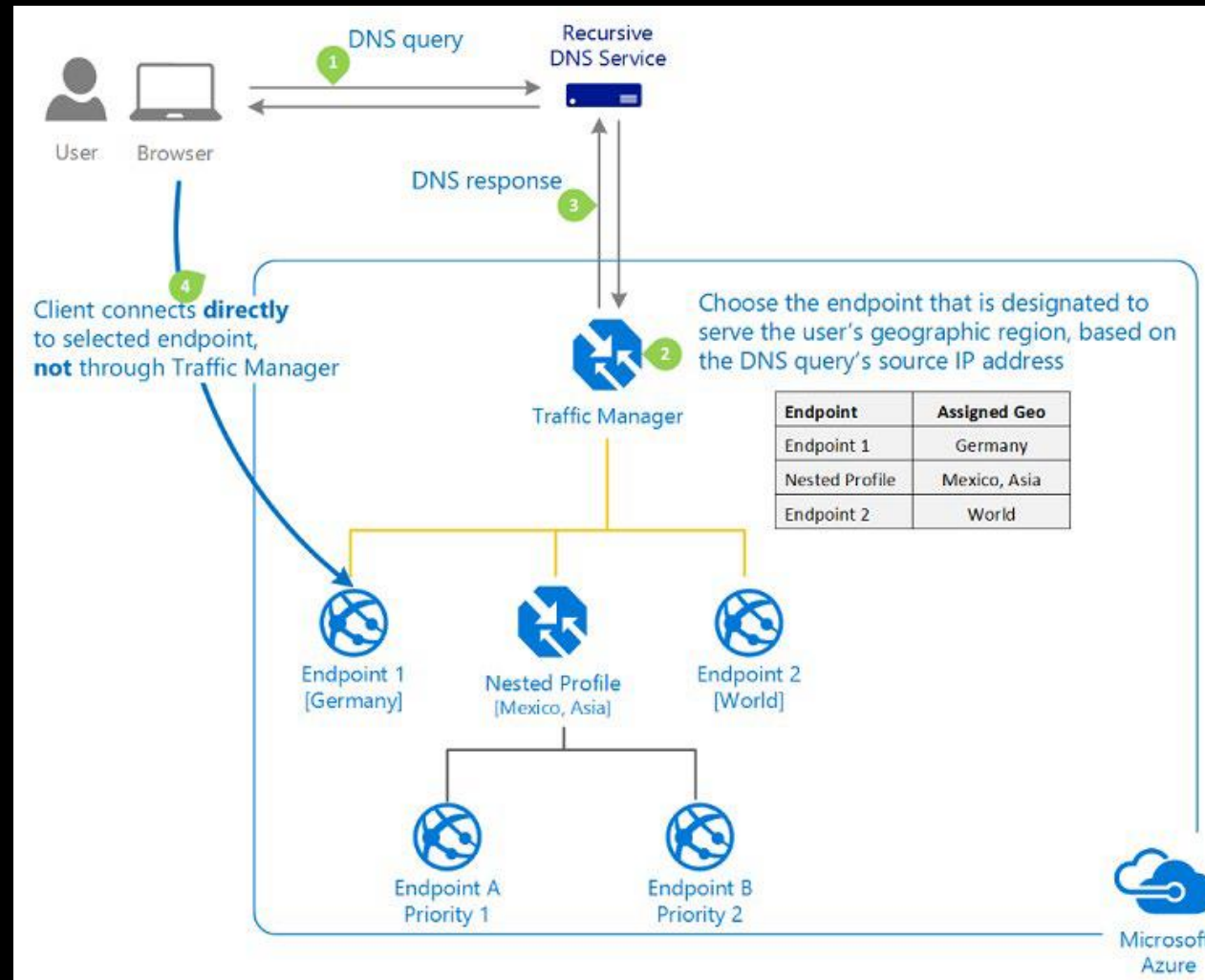


Traffic Manager Performance Routing

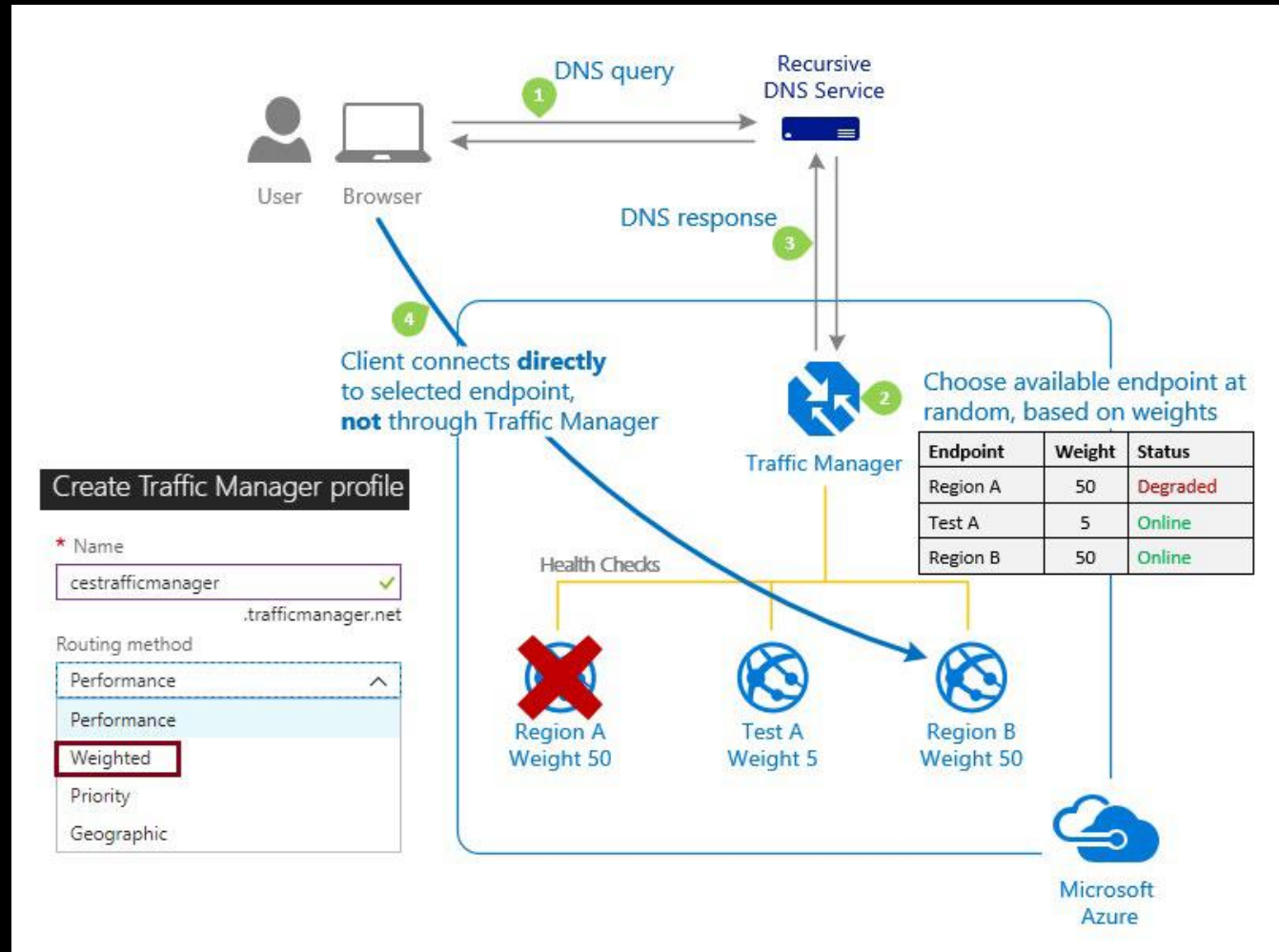




Traffic Manager Geographic Routing



Traffic Manager Weighted Routing





Distributing Network Traffic

Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport Layer (level 4)	Application Layer (level 7)	DNS Resolver
Protocols	Any TCP or UDP Protocol	HTTP, HTTPS, HTTP/2, & WebSockets	DNS Resolution
Backends or Endpoints	Azure Virtual Machines, and Azure Virtual Machine Scale Sets	Azure Virtual Machines, Azure Virtual Machine Scale Sets, Azure App Services, IP Addresses, and Hostnames	Azure Cloud Services, Azure App Services, Azure App Service Slots, and Public IP Addresses
Network Connectivity	External and Internal	External and Internal	External

- Azure has several options to distribute network traffic
- They can each be used in isolation or in combination



Azure Administrator Associate

EXAM: AZ-104



Module 06: Network Traffic Management

#28: Review Questions



Review Question 1

Which of the following two features of Azure networking provide the ability to redirect all Internet traffic back to your company's on-premises servers for packet inspection? Select two.

- User Defined Routes
- Cross-premises network connectivity
- Traffic Manager
- Forced Tunnelling
- System Routes



Review Question 2

Your company provides customers a virtual network in the cloud. You have dozens of Linux virtual machines in another virtual network. You need to install an Azure load balancer to direct traffic between the virtual networks. What should you do? Select one.

- Install a private load balancer.
- Install a public load balancer.
- Install an external load balancer.
- Install an internal load balancer.
- Install a network load balancer.



Review Question 3

Your company has a popular regional web site. The company plans to move it to Microsoft Azure and host it in the Canada East region. The web team has established the following requirements for managing the web traffic:

- **Evenly distribute incoming web requests across a farm of 10 Azure VMs.**
- **Support many incoming requests, including spikes during peak times.**
- **Minimize complexity.**
- **Minimize ongoing costs.**

Which of the following would you select for this scenario? Select one.

- Azure Traffic Manager
- Azure Load Balancer
- Azure Application Gateway
- Azure Cloud Services



Review Question 4

You deploy an internal load balancer between your web tier and app tier servers. You configure a custom HTTP health probe. Which two of the following are not true? Select two.

- The load balancer manages the health probe.
- By default, the health probe checks the endpoint every 30 seconds.
- The instance is healthy if it responds with an HTTP 200 error.
- You can change the amount of time between health probe checks.
- You can change the number of failures within a time period.



Review Question 5

Which criteria does Application Gateway use to route requests to a web server? Select one

- The hostname, port, and path in the URL of the request.
- The IP address of the web server that is the target of the request.
- The region in which the servers hosting the web application are located.
- The users authentication information.



Review Question 6

Which load balancing strategy does the Application Gateway implement?
Select one

- Distributes requests to each available server in a backend pool in turn, round-robin.
- Distributes requests to the server in the backend pool with the lightest load.
- Polls each server in the backend pool in turn, and sends the request to the first server that responds.
- Uses one server in the backend pool until that server reaches 50% load, then moves to the next server.



Review Question 7

You have several websites and are using Traffic Manager to distribute the network traffic. You are bringing a new endpoint online but are not sure that it is ready to accept a full load of requests. Which Traffic Manager routing algorithm should you use? Select one.

- Round robin
- Priority
- Geographic
- **Weighted**
- Performance



Review Question 8

Your company has a website that allows users to customize their experience by downloading an app. Demand for the app has increased so you have added another virtual network with two virtual machines. These machines are dedicated to serving the app downloads. You need to ensure the additional download requests do not affect the website performance. Your solution must route all download requests to the two new servers you have installed. What action will you recommend? Select one

- **Configure Traffic Manager.**
- Add a user-defined route.
- Create a local network gateway.
- Configure a new routing table.
- Add an application gateway.



Review Question 9

You are deploying the Application Gateway and want to ensure incoming requests are checked for common security threats like cross-site scripting and crawlers. To address your concerns what should you do? Select one.

- Install an external load balancer
- Install an internal load balancer
- Install Azure Firewall
- Install the Web Application Firewall



Azure Administrator Associate

EXAM: AZ-104



Module 07: Azure Storage

#29: Storage Accounts



Storage Accounts Overview

- Azure Storage
- Azure Storage Services
- Storage Account Kinds
- Replication Strategies
- Accessing Storage
- Securing Storage Endpoints
- Demonstration – Securing a Storage Endpoint



Azure Storage

A service that you can use to store files, messages, tables, and other types of information

- Durable, secure, scalable, managed, accessible
- Manage data with multiple storage accounts

Three categories of Azure storage:

- Storage for virtual machines – Disks and File Shares
- Unstructured data – Blobs and Data Lake Store
- Structured data - Tables, Cosmos DB, and Azure SQL DB

Standard storage backed by magnetic drives (HDD) is lowest cost

Premium storage backed by solid state drives (SSD)



Azure Storage Services

- **Azure Containers:** A massively scalable object store for text and binary data
- **Azure Files:** Managed file shares for cloud or on-premises deployments
- **Azure Tables:** A NoSQL store for schemaless storage of structured data
- **Azure Queues:** A messaging store for reliable messaging between application components



Containers

Scalable, cost-effective storage for unstructured data

[Learn more](#)



File shares

Serverless SMB file shares

[Learn more](#)



Tables

Tabular data storage

[Learn more](#)



Queues

Effectively scale apps according to traffic

[Learn more](#)



Storage Account Kinds

Storage account type	Supported services	Supported tiers	Replication options
BlobStorage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
Storage (general purpose v1)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
StorageV2 (general purpose v2)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, ZGRS (preview), RA-ZGRS (preview)
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS, ZRS (limited regions)
File Storage	Files only	Premium	LRS, ZRS (limited regions)

- ✓ All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest

Replication Strategies



Data Replication Options	Description
Locally redundant storage (LRS)	Data is replicated three times within a single facility in a single region.
Zone-redundant storage (ZRS)	Data is replicated three times across two to three facilities, either within a single region or across two regions.
Geo-redundant storage (GRS)	Data is replicated three times within the primary region and replicated three times to the regions pair.
Read access geo-redundant storage (RA-GRS)	Data is replicated three times within the primary region and replicated with read-access to the region pair.
Geo-zone-redundant storage (GZRS)	Data is replicated across three Availability Zones and replicated to the region pair.
Read-access Geo-zone-redundant storage (RA-GZRS)	Data is replicated across three Availability Zones and replicated with read-access to the region pair.



Accessing Storage

- Every object has a unique URL address
- The storage account name forms the subdomain of that address

CNAME record	Target
blobs.contoso.com	contosoblobs.blob.core.windows.net

The subdomain and domain name forms an *endpoint*

- Container service: <http://mystorageaccount.blob.core.windows.net>
- Table service: <http://mystorageaccount.table.core.windows.net>
- Queue service: <http://mystorageaccount.queue.core.windows.net>
- File service: <http://mystorageaccount.file.core.windows.net>

Securing Storage Account Endpoints



storage987123 | Firewalls and virtual networks
Storage account

Search (Ctrl+/) << Save Discard Refresh

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
∨ vnet01	1			Demo
	subnet01	10.1.0.0/24	✓ Enabled	Demo

- Firewalls and Virtual Networks allows for restricting access to the Storage Account from specific Subnets on Virtual Networks
- Subnets and Virtual Networks must exist in the same Azure Region or Region Pair as the Storage Account



Demonstration – Securing a Storage Endpoint

- Create a storage account
- Upload a file to the storage account
- Create a subnet service endpoint
- Secure the storage to the service endpoint
- Test the storage endpoint



Azure Administrator Associate

EXAM: AZ-104



Module 07: Azure Storage

#30: Blob Storage



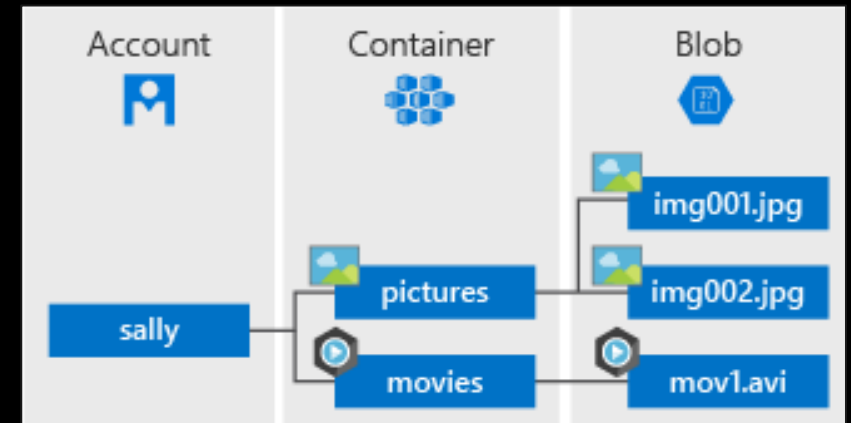
Blob Storage Overview

- Blob Storage
- Blob Containers
- Blob Access Tiers
- Blob Lifecycle Management
- Uploading Blobs
- Storage Pricing
- Demonstration – Blob Storage



Blob Storage

- Stores unstructured data in the cloud
- Can store any type of text or binary data
- Also referred to as *object storage*
- Common uses:
 - Serving images or documents directly to a browser
 - Storing files for distributed access
 - Streaming video and audio
 - Storing data for backup and restore, disaster recovery, archiving
 - Storing data for analysis by an on-premises or Azure-hosted service





Blob Containers

- All blobs must be in a container
- Accounts have unlimited containers
- Containers can have unlimited blobs
- **Private blobs** - no anonymous access
- **Blob access** - anonymous public read access for blobs only
- **Container access** - anonymous public read and list access to the entire container, including the blobs

+ Container Change access level Refresh Delete

New container

Name *
container01 ✓

Public access level ⓘ
Private (no anonymous access) ▾

OK Cancel

Public access level ⓘ

Private (no anonymous access) ▴

Private (no anonymous access)

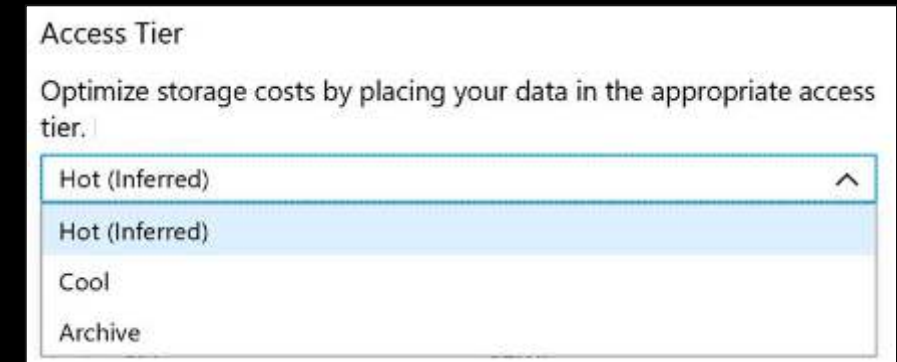
Blob (anonymous read access for blobs only)

Container (anonymous read access for containers and blobs)



Blob Access Tiers

- **Hot tier** - Optimized for frequent access of objects in the storage account
 - **Cool tier** - Optimized for storing large amounts of data that is infrequently accessed and stored for at least 30 days
 - **Archive** - Optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days
- ✓ You can switch between these access tiers at any time.





Blob Lifecycle Management

Blob Lifecycle Management allows for:

- Transitioning of blobs to a cooler storage tier to optimize for performance and cost
- Delete blobs at the end of their lifecycle
- Apply rules to filtered paths in the Storage Account

Rule name *

rule01 ✓

Blobs

Move blob to cool storage

Days after last modification

30 ✓

Move blob to archive storage

Days after last modification

180 ✓

Delete blob

Days after last modification

365 ✓

Snapshots

Delete snapshot

Days after blob is created

30 ✓



Uploading Blobs

- **Block blobs** (default) - useful for storing text or binary files
 - **Page blobs** - More efficient for frequent read/write operations
 - **Append blobs** - useful for logging scenarios
 - **Access tier** – select either Hot, Cool, or Archive
- ✓ You cannot change a blob type once it has been created

The screenshot shows the 'Upload blob' dialog box for a container named 'container01/'. The 'Files' section contains a text input field with the filename 'Cloud.jpg' and a file selection icon. Below this is a checkbox for 'Overwrite if files already exist'. The 'Advanced' section is expanded and contains several settings: 'Authentication type' is set to 'Account key' (selected) and 'Azure AD user account'; 'Blob type' is set to 'Block blob'; the checkbox 'Upload .vhd files as page blobs (recommended)' is checked; 'Block size' is set to '4 MB'; 'Access tier' is set to 'Hot (Inferred)'; and the 'Upload to folder' field is empty. An 'Upload' button is located at the bottom right of the dialog.



Blob upload tools

- **AZCopy**
- **Azure Storage Data Movement library**
- **Azure Data factory**
- **Blobfuse**
- **Azure Data Box Disk**
- **Azure Import/Export**



Storage Pricing

- Storage costs
- Blob storage
- Data access costs
- Transaction costs
- Geo-Replication data transfer costs
- Outbound data transfer costs
- Changing the storage tier

Block Blobs	Files
Scalable object storage for documents, videos, pictures, and unstructured text or binary data. Choose from Hot, Cool, or Archive tiers.	Fully managed file shares in the cloud, accessible via standard Server Message Block (SMB) protocol. Enables sharing files between applications using Windows APIs or REST API.
Prices for locally redundant storage (LRS) Archive Block Blob start from:	Prices for LRS File storage start from:
\$0.002 /GB per month	\$0.06 /GB per month
See Pricing >	See Pricing >



Demonstration – Blob Storage

- Create a container
- Upload a block blob
- Download a block blob



Azure Administrator Associate

EXAM: AZ-104



Module 07: Azure Storage

#31: Storage Security



Storage Security Overview

- Storage Security
- Shared Access Signatures
- URI and SAS Parameters
- Demonstration – SAS (Portal)
- Storage Service Encryption
- Customer Managed Keys
- Storage Security Best Practices



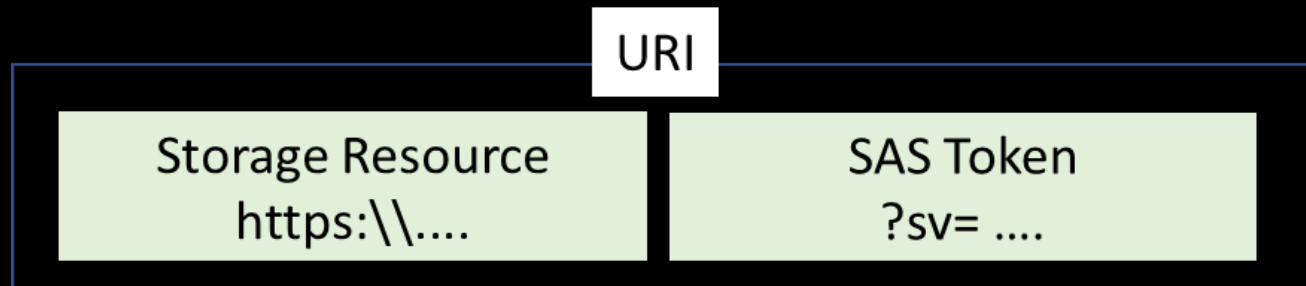
Storage Security

- Storage Encryption Services
- Authentication with Azure AD and RBAC
- Client-side encryption, HTTPS, and SMB 3.0 for data in transit
- Azure disk encryption
- Shared Access Signatures – delegated access
- Shared Key – encrypted signature string
- Anonymous access to containers and blobs



URI and SAS Parameters

- A SAS is a signed URI that points to one or more storage resources
- Consists of a storage resource URI and the SAS token



`https://myaccount.blob.core.windows.net/?sp=r&st=2020-05-11T18:31:43Z&se=2020-05-12T02:31:43Z&spr=https&sv=2019-10-10&sr=b&sig=j0qABJZHfUveBQ3yVn7kWiCKl00sxCiK1rzEchfAz8U%3D`

Includes parameters for resource URI, storage services version, services, resource types, start time, expiry time, resource, permissions, IP range, protocol, signature



Demonstration – SAS (Portal)



- Create a SAS at the service level
- Create a SAS at the account level



Storage Service Encryption

- Protects your data for security and compliance
 - Automatically encrypts and decrypts your data
 - Encrypted through 256-bit AES encryption
 - Is enabled for all new and existing storage accounts and cannot be disabled
 - Is transparent to users
- ✓ You can use your own key (next topic)

Encryption

 Save  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data in the storage account is encrypted using Microsoft Managed Keys. You may choose to bring your own key.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn More about Azure Storage Encryption](#) ↗

Encryption type

Microsoft Managed Keys

Customer Managed Keys



Customer Managed Keys

- Use the Azure Key Vault to manage your encryption keys
- Create your own encryption keys and store them in a key vault
- Use Azure Key Vault's APIs to generate encryption keys
- Custom keys give you more flexibility and control

Encryption type

- Microsoft Managed Keys
 Customer Managed Keys

i The storage account named 'storage987123' will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more about customer managed keys](#)

Encryption key

- Enter key URI
 Select from Key vault

Key vault and key *

Key vault: keyvault987123
Key: storagekey
[Select a key vault and key](#)



Storage Best Practices

- Always use HTTPS to create or distribute an SAS
- Reference stored access policies where possible
- Use near-term expiration times on an ad hoc SAS
- Have clients automatically renew the SAS if necessary
- Be careful with SAS start time
- Be specific with the resource to be accessed
- Understand that your account will be billed for any usage
- Validate data written using SAS
- Don't assume SAS is always the correct choice
- Use Storage Analytics to monitor your application



Azure Administrator Associate

EXAM: AZ-104



Module 07: Azure Storage

#32: Azure Files and File Sync



Azure Files and File Sync Overview

- Files vs Blobs
- Managing File Shares
- File Share Snapshots
- Demonstration – File Shares
- Azure File Sync
- Azure File Sync Components
- File Sync Steps



Files vs Blobs

Feature	Description	When to use
Azure Files	SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files.	<ul style="list-style-type: none">• Lift and shift an application to the cloud.• Store shared data across multiple virtual machines.• Store development and debugging tools that need to be accessed from many virtual machines.
Azure Blobs	Client libraries and a REST interface that allows unstructured data (flat namespace) to be stored and accessed at a massive scale in block blobs.	<ul style="list-style-type: none">• Support streaming and random-access scenarios.• Access application data from anywhere.



Managing File Shares

- File share quotas
- Windows – ensure port 445 is open
- Linux – mount the drive
- MacOS – mount the drive
- Secure transfer required - SMB 3.0 encryption

Windows Linux macOS

Drive letter

Z




To connect to this Azure file share from Windows, run these PowerShell commands from a normal (not elevated) PowerShell terminal:

```
$connectTestResult = Test-NetConnection -  
ComputerName storage987123.file.core.windows.net -  
Port 445  
if ($connectTestResult.TcpTestSucceeded) {  
    # Save the password so the drive will persist on reboot  
    cmd.exe /C "cmdkey  
/add:"storage987123.file.core.windows.net"
```

This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site \(P2S\) VPN](#), Azure [Site-to-Site \(S2S\) VPN](#), or [ExpressRoute](#) to tunnel SMB traffic to your Azure file share over a different port.



File Share Snapshots

 Add snapshot	 Refresh	 Delete
Name	Date created	Initiator
<input type="checkbox"/> 2020-03-12T00:58:38.0000000Z	3/11/2020, 8:58:38 PM	-

- Incremental snapshot that captures the share state at a point in time
- Is read-only copy of your data
- Snapshot at the file share level, and restore at the file level
- Uses:
 - Protection against application error and data corruption.
 - Protection against accidental deletions or unintended changes.
 - General backup purposes.



Demonstration – File Shares

- Create a file share and upload a file
- Manage snapshots
- Create a file share (PowerShell)
- Mount a file share (PowerShell)



Azure File Sync

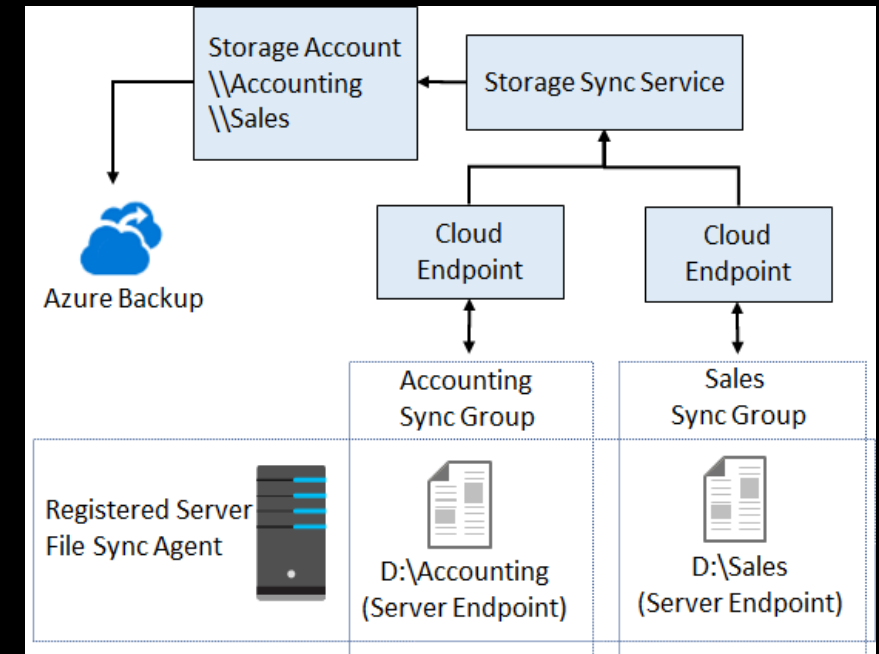
- Centralize file shares in Azure Files
- Lift and shift
- Branch Office backups
- Backup and Disaster Recovery
- File Archiving





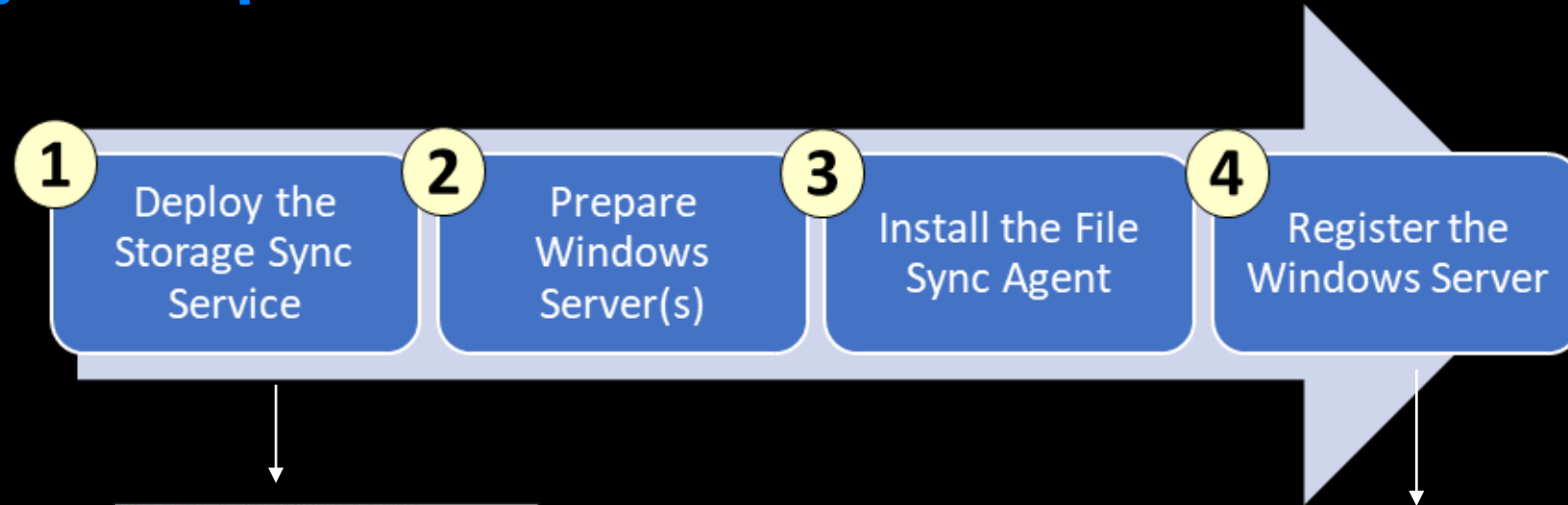
File Sync Components

- The Storage Sync Service is the top-level resource.
- The registered server object represents a trust relationship between your server (or cluster) and the Storage Sync Service
- The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share
- A server endpoint represents a specific location on a registered server, such as a folder
- A cloud endpoint is an Azure file share
- A sync group defines which files are kept in sync





File Sync Steps



Home > Deploy Storage Sync

Deploy Storage Sync

* Name
StorageSync1 ✓

* Subscription
Visual Studio Enterprise ▾

* Resource group
ASH ▾
[Create new](#)

* Location
South Central US ▾

[Create](#) [Automation options](#)

Microsoft Azure File Sync - Server Registration

Choose a Storage Sync Service

Azure Subscription
▾

Resource Group
▾

Storage Sync Service
▾

[Register](#)



Azure Administrator Associate

EXAM: AZ-104



Module 07: Azure Storage

#33: Managing Azure Storage



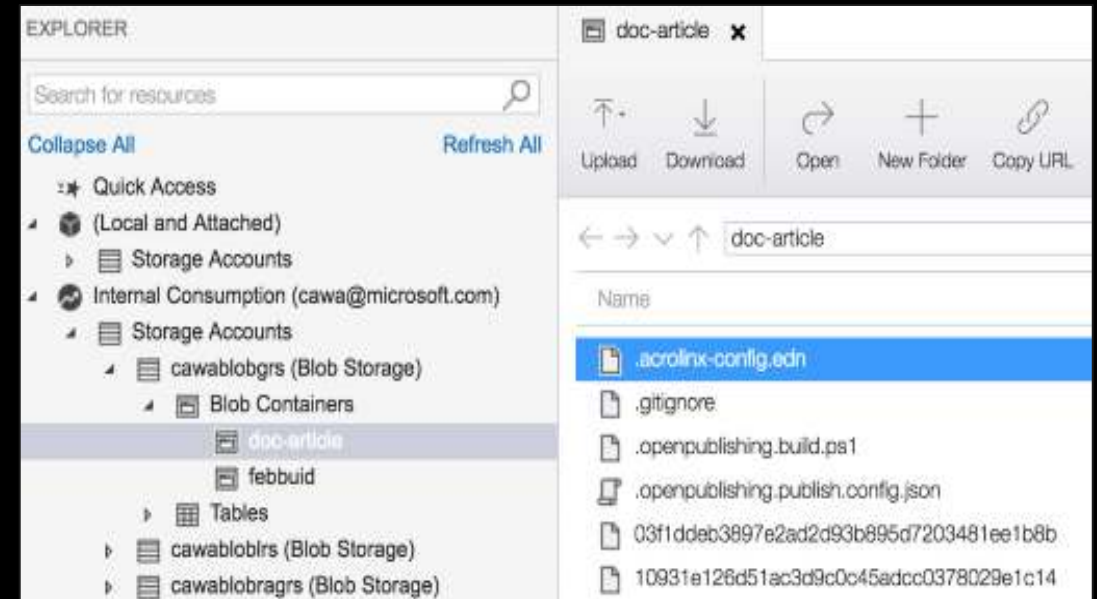
Managing Storage Overview

- Storage Explorer
- Import and Export Service
- Data Box
- AzCopy
- Data Transfer Tool Selection
- Demonstration – Storage Explorer
- Demonstration - AzCopy



Storage Explorer

- Access multiple accounts and subscriptions
- Create, delete, view, edit storage resources
- View and edit Blob, Queue, Table, File, Cosmos DB storage and Data Lake Storage

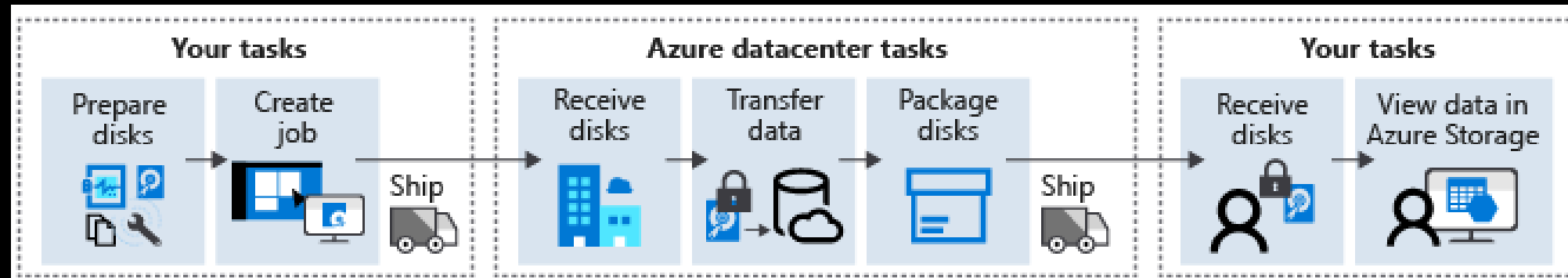


- Obtain shared access signature (SAS) keys
- Available for Windows, Mac, and Linux

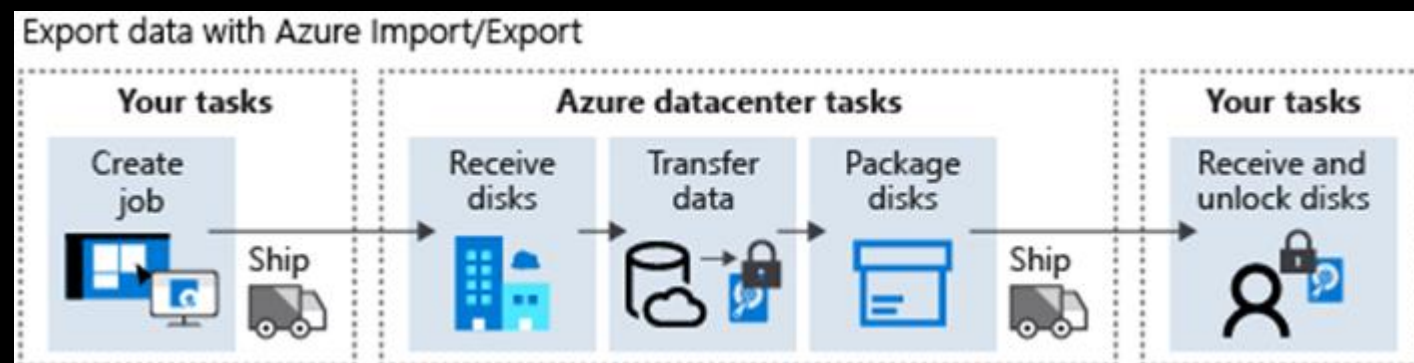


Import and Export Service

- **Import jobs** move large amounts of data to Azure blob storage or files

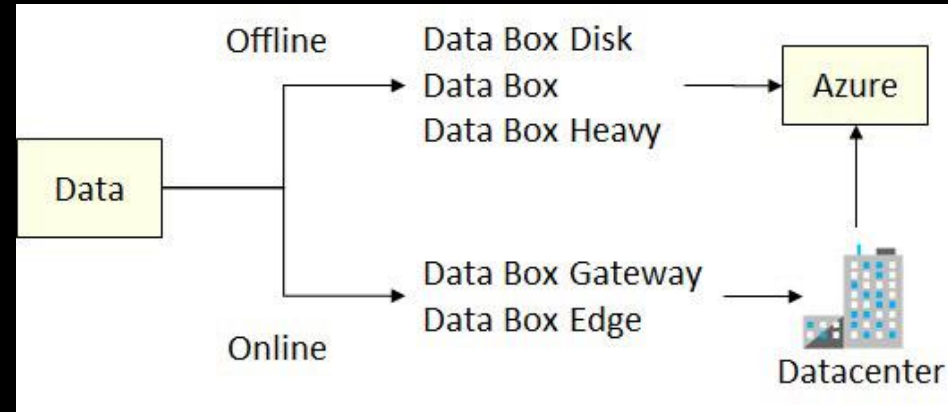


- **Export jobs** move large amounts of data from Azure storage (not files)



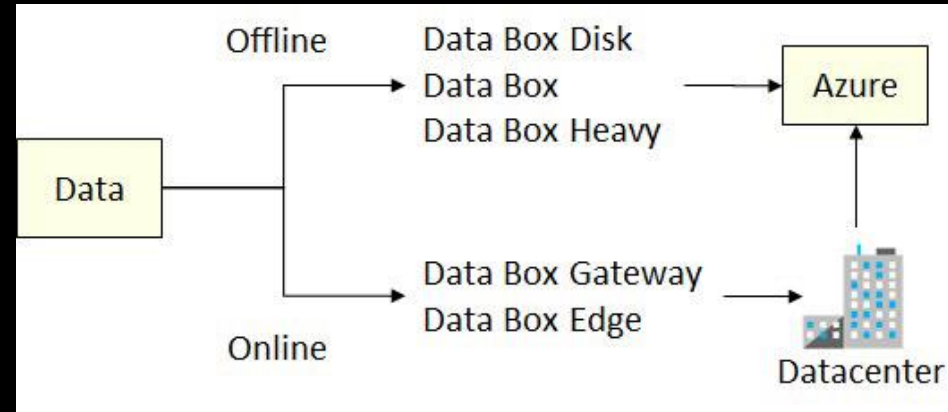


Data Box



- Easy, secure, fast large volume data transfer
- **Offline** usage - one-time migration, incremental transfer, periodic updates
- **Online** usage – cloud archival, data aggregation, integration with on-premises workloads, pre-process data (Edge), inference Azure Machine Learning (Edge)

Data Box



- Data Box Gateway
- Data Box Edge



```
azcopy copy /Source:<source> /Dest:<destination> [Options]
```

- Command-line utility
- Available on Windows, Linux, and MacOS
- Designed for copying data to and from Azure Blob, File, and Table storage
- Authentication options include Active Directory or SAS token
- Example 1: Copy a Blob storage account to another account
- Example 2: List/Remove files and blobs (wildcard support)

Data Transfer Tool Selection



Dataset	Network bandwidth	Solution to use
Large dataset	Low-bandwidth network or direct connectivity to on-premises storage is limited by organization policies	Azure Import/Export for export; Data Box Disk or Data Box for import where supported; otherwise use Azure Import/Export
Large dataset	High-bandwidth network: 1 gigabit per second (Gbps) - 100 Gbps	AzCopy for online transfers; or to import data, Azure Data Box Edge, or Azure Data Box Gateway
Large dataset	Moderate-bandwidth network: 100 megabits per second (Mbps) - 1 Gbps	Azure Import/Export for export or Azure Data Box family for import where supported
Small dataset: a few GBs to a few TBs	Low to moderate-bandwidth network: up to 1 Gbps	If transferring only a few files, use Azure Storage Explorer, Azure portal, AzCopy, or AZ CLI



Demonstration – Storage Explorer

- Download and install Storage Explorer
- Connect to an Azure subscription
- Attach an Azure storage account
- Generate a SAS connection string for the account you want to share
- Attach to a storage account by using a SAS Connection string



Demonstration - AzCopy

- Install the AzCopy tool
- Explore the help
- Download a blob from Blob storage to the file system
- Upload files to Azure blob storage



Azure Administrator Associate

EXAM: AZ-104



Module 07: Azure Storage

#34: Review Questions



Review Question 1

You work for an open source development company. You use Microsoft Azure for a variety of storage needs. Up to now, all the storage was used for internal purposes only. It is organized in block blobs. Each block blob is in its own container. Each container is set to default settings. In total, you have 50 block blobs. The company has decided to provide read access to the data in the block blobs, as part of releasing more information about their open source development efforts. You need to reconfigure the storage to meet the following requirements:

- **All block blobs must be readable by anonymous internet users.**

You need to configure the storage to meet the requirements. What should you do? Select one.

- Create a new container, move all the blobs to the new container, and then set the public access level to Blob.
- Set the public access level to Blob on all the existing containers.
- Create a new shared access signature for the storage account and then set the allowed permissions to Read, set the allowed resource types to Object, and set the allowed services to Blob.
- Create a new access key for the storage account and then provide the connection string in the storage connectivity information to the public.



Review Question 2

Your company is planning to storage log data, crash dump files, and other diagnostic data for Azure VMs in Azure. The company has issued the following requirements for the storage:

- **Administrators must be able to browse to the data in File Explorer.**
- **Access over SMB 3.0 must be supported.**
- **The storage must support quotas.**

You need to choose the storage type to meet the requirements. Which storage type should you use? Select one.

- **Azure Files**
- Table storage
- Blob storage
- Queue storage



Review Question 3

Your company provides cloud software to audit administrative access in Microsoft Azure resources. The software logs all administrative actions (including all clicks and text input) to log files. The software is about to be released from beta and the company is concerned about storage performance. You need to deploy a storage solution for the log files to maximize performance. What should you do? Select one.

- Deploy Azure Files using SMB 3.0.
- Deploy Azure Table Storage.
- Deploy Azure Queues Storage.
- Deploy blob storage using block blobs.
- Deploy blob storage using append blobs.



Review Question 4

Your company is building an app in Azure. The app has the following storage requirements:

- **Storage must be reachable programmatically through a REST API.**
- **Storage must be globally redundant.**
- **Storage must be accessible privately within the company's Azure environment.**
- **Storage must be optimal for unstructured data.**

Which type of Azure storage should you use for the app? Select one.

- Azure Data Lake store
- Azure Table Storage
- **Azure Blob Storage**
- Azure File Storage



Review Question 5

You use a Microsoft Azure storage account for storing large numbers of video and audio files. You create containers to store each type of file and want to limit access to those files for specific periods. Additionally, the files can only be accessed through shared access signatures (SAS). You need the ability to revoke access to the files and to change the period for which users can access the files. What should you do in order to accomplish this in the most simple and effective way? Select one.

- Create an SAS for each user and delete the SAS when you want to prevent access.
- Use Azure Rights Management Services (RMS) to control access to each file.
- Implement stored access policies for each container to enable revocation of access or change of duration.
- Periodically regenerate the account key to control access to the files.



Review Question 6

You need to provide a contingent staff employee temporary read-only access to the contents of an Azure storage account container named media. It is important that you grant access while adhering to the security principle of least-privilege. What should you do? Select one.

- Set the public access level to Container.
- Generate a shared access signature (SAS) token for the container.
- Share the container entity tag (Etag) with the contingent staff member.
- Configure a Cross-Origin Resource Sharing (CORS) rule for the storage account.



Review Question 7

Your organization maintains historical images for large media companies. There are thousands of photos requiring over 600 TB of storage. Your datacenter has only limited bandwidth, and you need to quickly move the data to Azure blob storage. Additionally, security of the data including chain of custody logs and 256-bit encryption is required. Which of the following products would you recommend using? Select one.

- CDN
- Data Box
- Data Box Heavy
- Data Box Gateway
- Data Box Edge
- Import/Export



Review Question 8

You are using blob storage. Which of the following is true? Select one.

- The cool access tier is for frequent access of objects in the storage account.
- The hot access tier is for storing large amounts of data that is infrequently accessed.
- The performance tier you select does not affect pricing.
- You can switch between hot and cool performance tiers at any time.



Review Question 9

You are planning a delegation model for your Azure storage. The company has issued the following requirements for Azure storage access:

- **Apps in the non-production environment must have automated time-limited access**
- **Apps in the production environment must have unrestricted access to storage resources**

You need to configure storage access to meet the requirements. What should you do? (Each answer presents part of the solution. Select two.)

- Use shared access signatures for the non-production apps.
- Use shared access signatures for the production apps.
- Use access keys for the non-production apps.
- Use access keys for the production apps.
- Use Stored Access Policies for the production apps.
- Use Cross Origin Resource Sharing for the non-production apps.



Review Question 10

Your company has a file server named FS01. The server has a single shared folder that users' access to shared files. The company wants to make the same files available from Microsoft Azure. The company has the following requirements:

- **Microsoft Azure should maintain the exact same data as the shared folder on FS01.**
- **Files deleted on either side (on-premises or cloud) shall be subsequently and automatically deleted from the other side (on-premises or cloud).**

You need to implement a solution to meet the requirements. What should you do? Select one.

- Deploy DFS Namespaces.
- Install and use AZCopy.
- **Deploy Azure File Sync.**
- Install and use Azure Storage Explorer.
- Deploy storage tiering.



Review Question 11

Which of the following replicates your data to a secondary region, maintains six copies of your data, and is the default replication option. Select one.

- Locally-redundant storage
- Geo-redundant storage
- Read-access geo-redundant storage
- Zone-redundant storage



Review Question 12

You have an existing storage account in Microsoft Azure. It stores unstructured data. You create a new storage account. You need to move half of the data from the existing storage account to the new storage account. What tool should you use? Select one.

- Use the Azure portal
- Use File Server Resource Manager
- Use the Robocopy command-line tool
- Use the AzCopy command-line tool



Azure Administrator Associate

EXAM: AZ-104



Module 08: Azure Virtual Machines

#35: Virtual Machine Planning



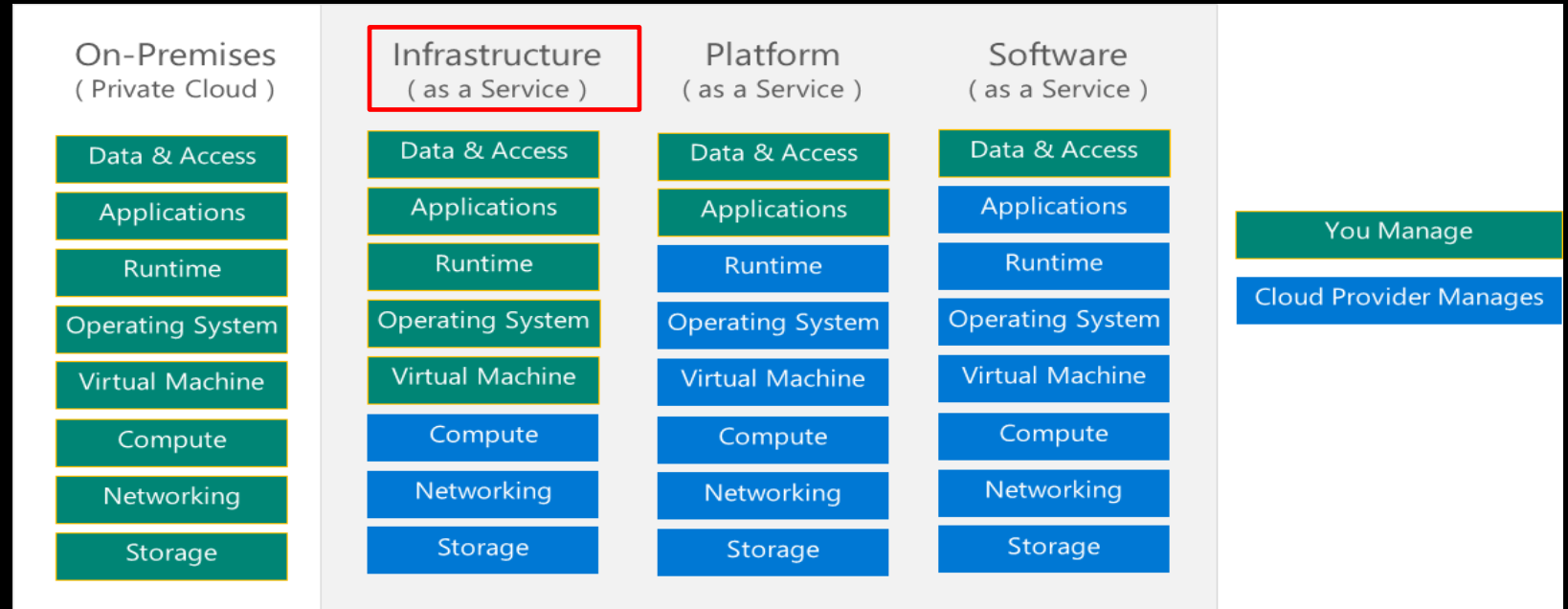
Virtual Machine Planning Overview

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



IaaS Cloud Services

- Test and development
- Website hosting
- Storage
- Backup
- Recovery
- High-performance computing
- Big data analysis
- Extended data center





Planning Checklist

- Start with the network
- Name the VM
- Decide the location for the VM
- Determine the size of the VM
- Understand the pricing model
- Consider storage for the VM
- Select an operating system

Planning Checklist



Name the VM

Element	Example	Notes
Environment	dev, prod, QA	Identifies the environment for the resource
Location	uw (US West), ue (US East)	Identifies the region into which the resource is deployed
Instance	01, 02	For resources that have more than one named instance (web servers, etc.)
Product or Service	service	Identifies the product, application, or service that the resource supports
Role	sql, web, messaging	Identifies the role of the associated resource



Location and Pricing

Location

- Each region has different hardware and service capabilities
- Locate virtual machines as close as possible to your users
- Locate virtual machines to ensure compliance and legal obligations

Pricing

- Compute costs
- Storage costs (consumption-based and reserved instances)



55+ Azure regions
Available in 140 countries



Virtual Machine Sizing

VM Type	Sizes	Purpose
General Purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute Optimized	Fsv2	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory Optimized	Esv3, Ev3, Easv4, Eav4, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage Optimized	Lsv2	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	NC, NCv2, NCv3, ND, NDv2 (Preview), NV, NVv3, NVv4 (Preview)	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
High Performance Compute	HB, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

Virtual Machine Disks



Disks	OS disk				
Size	NAME	SIZE	STORAGE ACCOUNT...	ENCRYPTION	HOST CACHING
Security	UbuntuServer_OsDisk_1_	30 GiB	Standard_LRS	Not enabled	Read/write
Extensions	Data disks				
Continuous delivery	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 Options

- Premium storage offers high-performance, low-latency SSD disk support
- Use premium storage for virtual machines with input/output (I/O)-intensive workloads

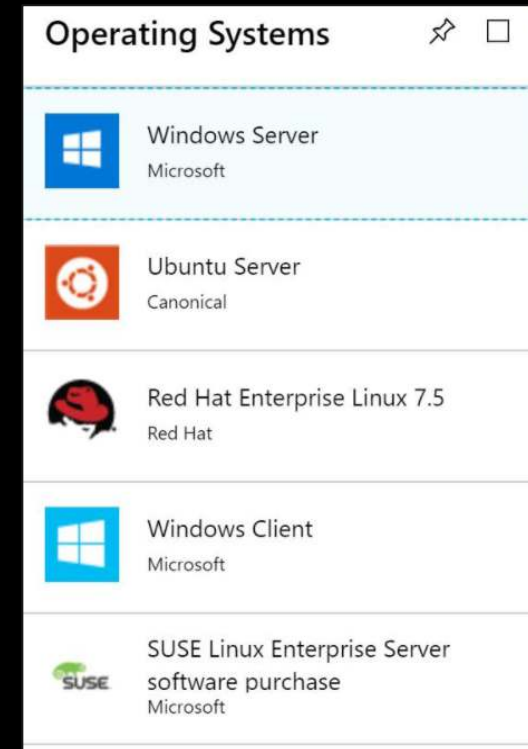
Two types of disks: Unmanaged and Managed

- Unmanaged disks require you to manage the storage accounts and VHDs
- Managed disks are maintained by Azure (recommended)



Supported Operating Systems

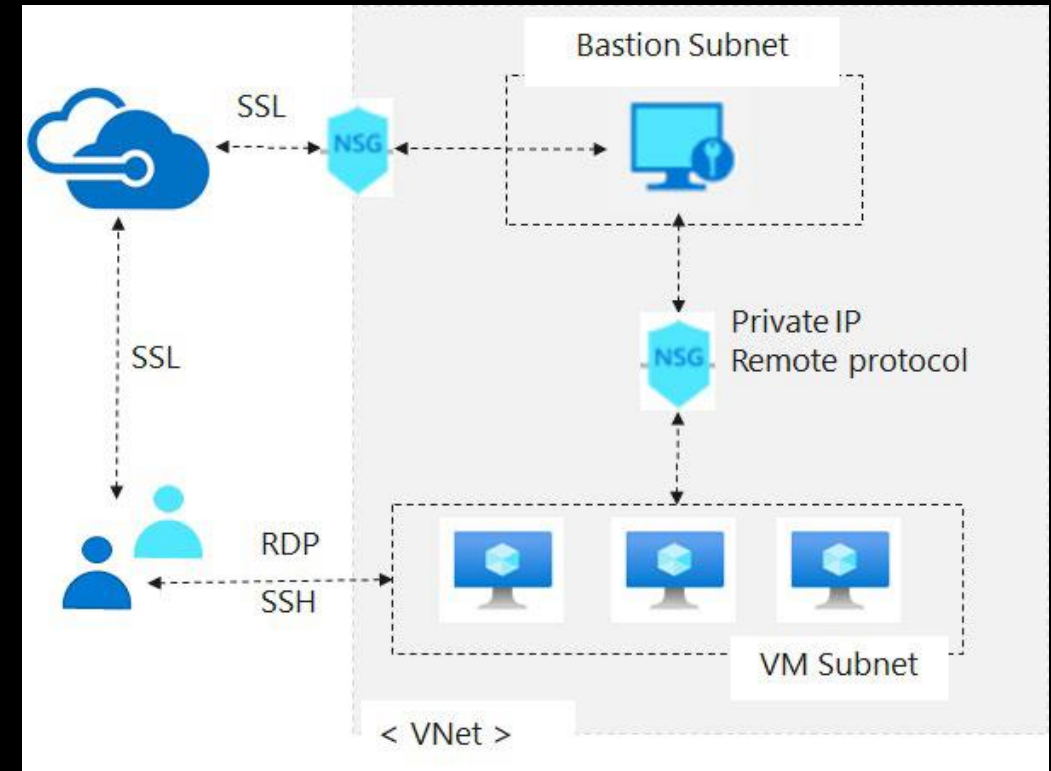
- Windows Server includes many common products, requires a license, doesn't support OS upgrades
- Linux distributions are supported, upgrade of the OS is supported





Virtual Machine Connections

- Remote Desktop Protocol for Windows-based virtual machines
- Secure Shell Protocol for Linux based virtual machines
- Bastion Subnet for RDP/SSH through the Portal over SSL





Azure Administrator Associate

EXAM: AZ-104



Module 08: Azure Virtual Machines

#36: Creating Virtual Machines



Creating Virtual Machines Overview

- Creating Virtual Machines in the Portal
- Windows Virtual Machines
- Windows VM Connections
- Demonstration – Creating a VM in the Portal
- Linux Virtual Machines
- Linux VM Connections
- Demonstration – Connect to Linux Virtual Machines



Creating Virtual Machines in the Portal

Create a virtual machine

Basics

Disks

Networking

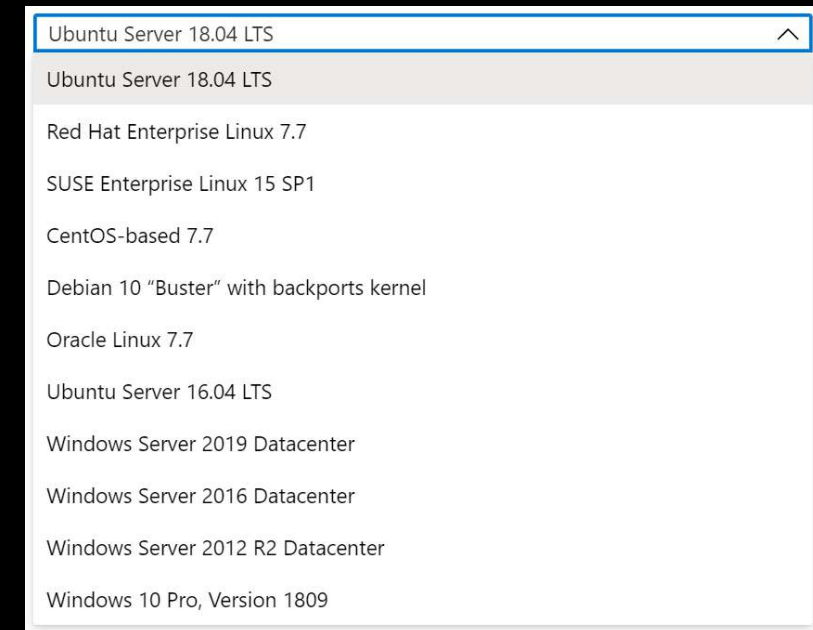
Management

Advanced

Tags

Review + create

- Basic (required) - Project details, Administrator account, Inbound port rules
- Disks - OS disk type, data disks
- Networking - Virtual networks, load balancing
- Management - Monitoring, Auto-shutdown, Backup
- Guest config - Add additional configuration, agents, scripts or applications





Windows Virtual Machines



- Unique hybrid capabilities
- Advanced multi-layer security
- Faster innovation for applications
- Unprecedented hyper-converged infrastructure

Windows VM Connections



- Remote Desktop Protocol (RDP) creates a GUI session and accepts inbound traffic on TCP port 3389
- WinRM creates a command-line session so can run scripts

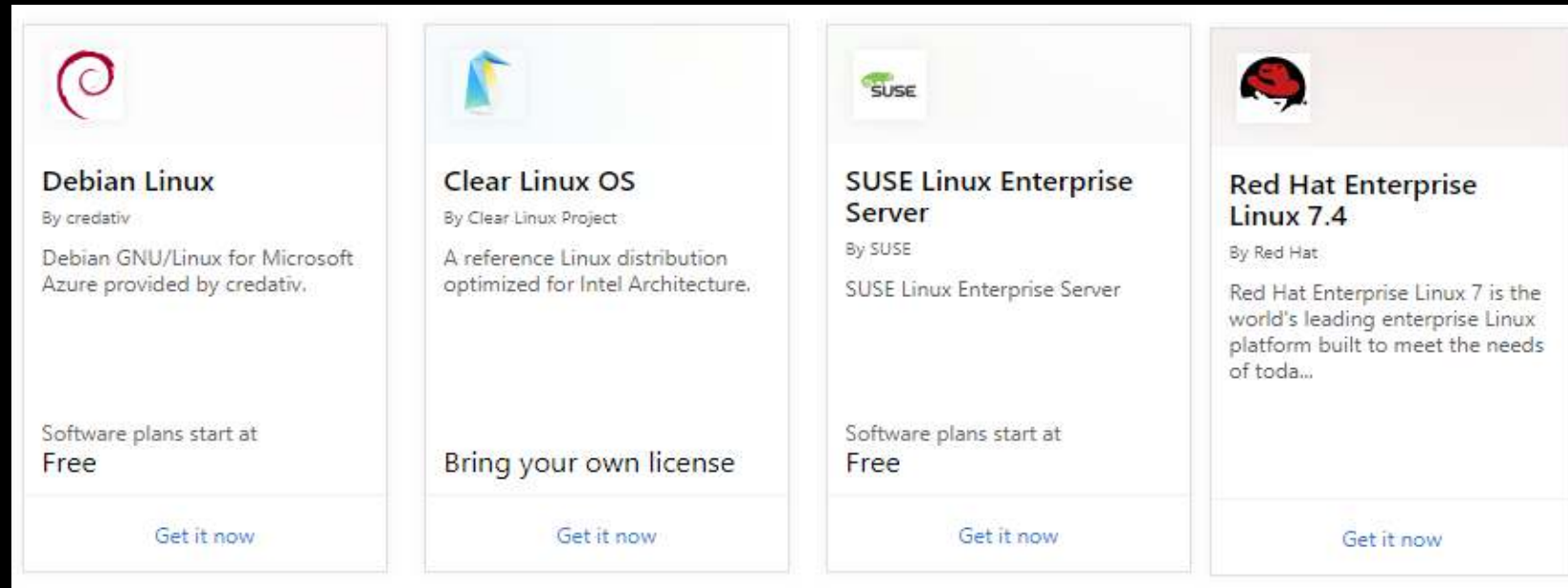




Demonstration – Creating a VM in the Portal

- Create the virtual machine
- Connect to the virtual machine
- Install the Web Server role
- View the IIS welcome page

Linux Virtual Machines



- 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



Administrator account

Authentication type

Username * ⓘ

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.

[Learn more about creating and using SSH keys in Azure](#)

- 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



Demonstration – Connect to Linux VMs

- Create the SSH keys
- Create the Linux machine and assign the public SSH key
- Access the server using SSH



Azure Administrator Associate

EXAM: AZ-104



Module 08: Azure Virtual Machines

#37: Virtual Machine Availability



Virtual Machine Availability Overview

- Maintenance and Downtime
- Availability Sets
- Update and Fault Domains
- Availability Zones
- Scaling Concepts
- Scale Sets
- Implementing Scale Sets
- Autoscale
- Implementing Autoscale



Maintenance vs. Downtime

Unplanned Hardware
Maintenance

Unexpected
Downtime

Planned
Maintenance

- When the platform predicts a failure, it will issue an unplanned hardware maintenance event. Action: Live migration.
- Unexpected Downtime is when a virtual machine fails unexpectedly. Action: Automatically migrate (heal).
- Planned Maintenance events are periodic updates made to the Azure platform. Action: No action.



Availability Sets

Instance details

Name * ⓘ

Region * ⓘ

Fault domains ⓘ

Update domains ⓘ

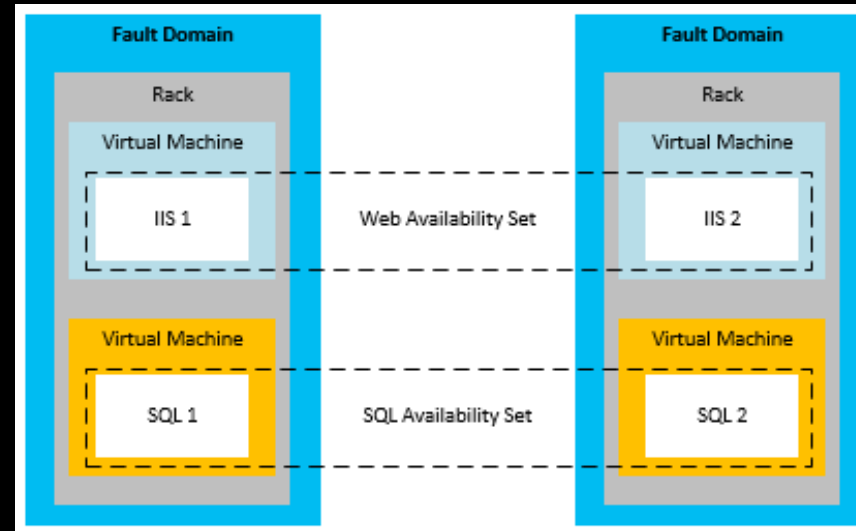
Use managed disks ⓘ

Two or more instances in
Availability Sets = 99.95% SLA

- Configure multiple virtual machines in an Availability Set
- Configure each application tier into separate Availability Sets
- Combine a Load Balancer with Availability Sets
- Use managed disks with the virtual machines



Update and Fault Domains

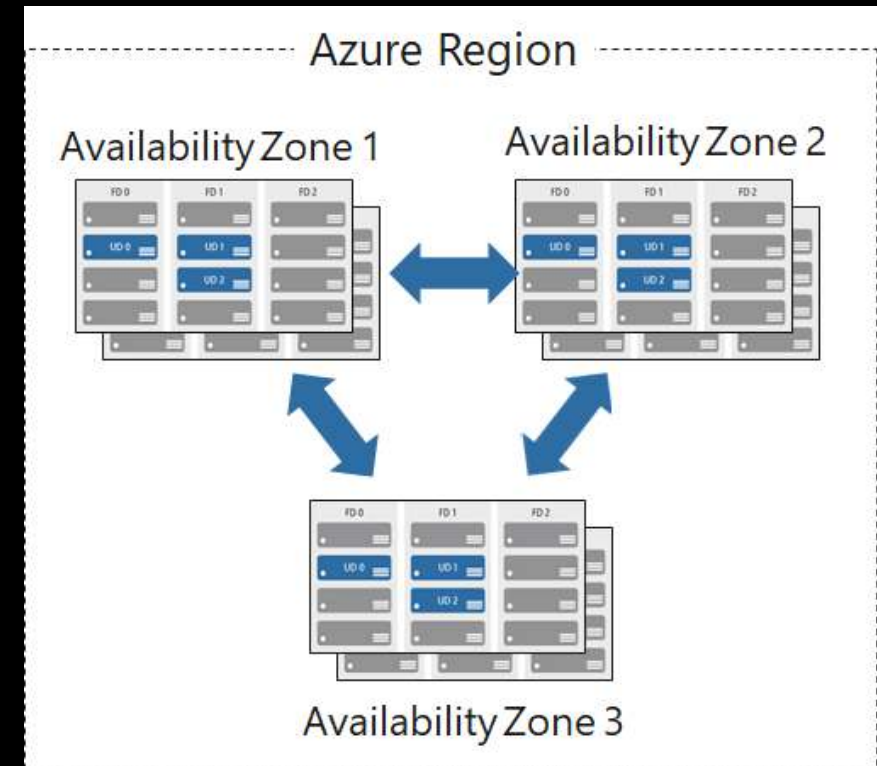


- **Update domains** allows Azure to perform incremental or rolling upgrades across a deployment. During planned maintenance, only one update domain is rebooted at a time.
- **Fault Domains** are a group of virtual machines that share a common set of hardware, switches, that share a single point of failure.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



Availability Zones

- Unique physical locations in a region
- Includes datacenters with independent power, cooling, and networking
- Protects from datacenter failures
- Combines update and fault domains
- Provides 99.99% SLA





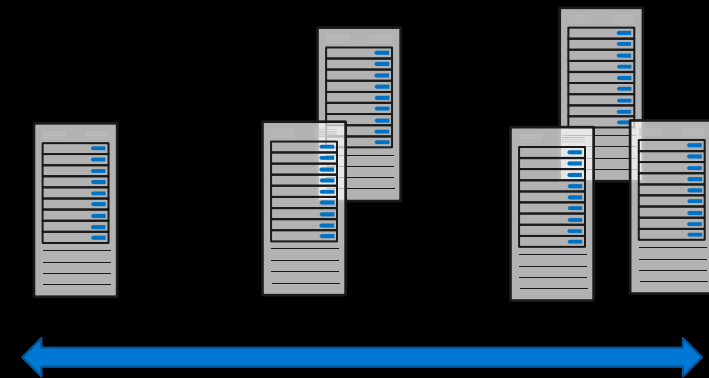
Scaling Concepts

- **Vertical scaling (scale up and scale down)** is the process of increasing or decreasing power to a single instance of a workload; usually manual
- **Horizontal scaling (scale out and scale in)** is the process of increasing or decreasing the number of instances of a workload; frequently automated

Vertical scaling

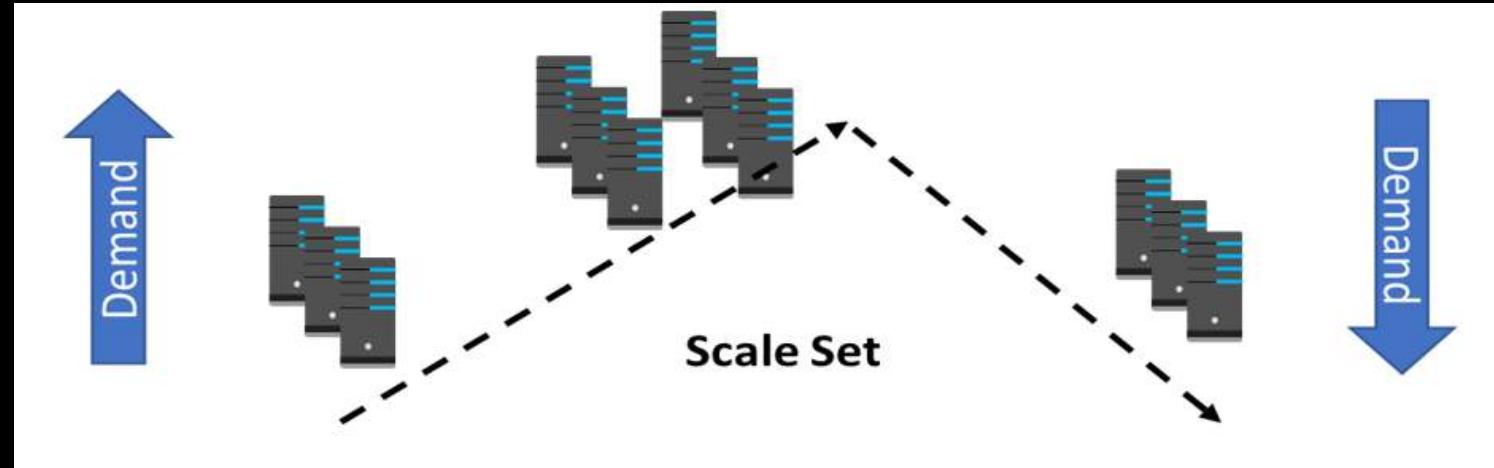


Horizontal scaling





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

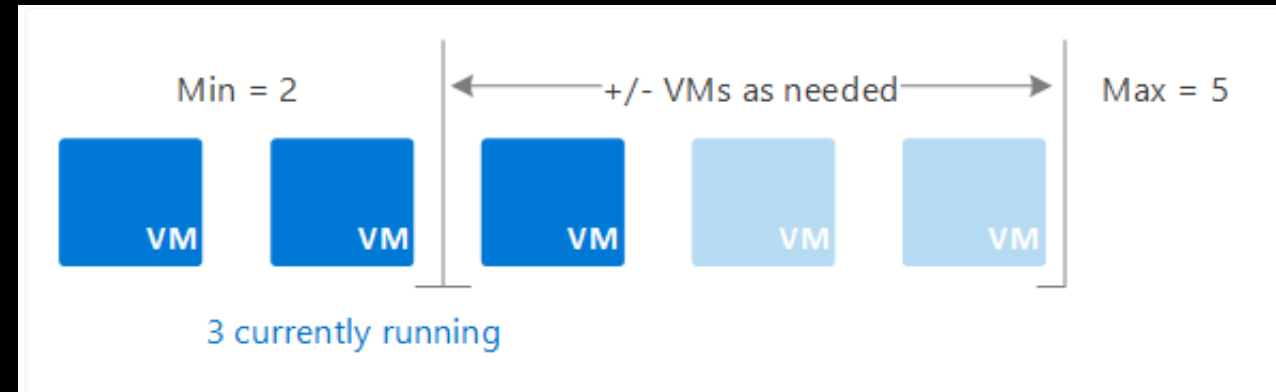


Implementing Scale Sets

- **Instance count.** Number of VMs in the scale set (0 to 1000)
- **Instance size.** The size of each virtual machine in the scale set
- **Azure Spot Instance.** Unused capacity at a discounted rate
- **Use managed disks**
- **Enable scaling beyond 100 instances**

The screenshot shows the 'Instance' configuration page in the Azure portal. The 'Initial instance count' is set to 2. The 'Size' is 'Standard D2s v3' (2 vcpus, 8 GiB memory, \$85.41/month). The 'Azure Spot instance' option is set to 'No'. The 'Use managed disks' option is set to 'Yes'. The 'Allocation policy' section shows 'Enable scaling beyond 100 instances' set to 'No' and 'Spreading algorithm' set to 'Fixed spreading (not recommended with zones)'.

Property	Value
Initial instance count *	2
Size *	Standard D2s v3 2 vcpus, 8 GiB memory (\$85.41/month) Change size
Azure Spot instance	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use managed disks	<input type="radio"/> No <input checked="" type="radio"/> Yes
Allocation policy	
Enable scaling beyond 100 instances	<input checked="" type="radio"/> No <input type="radio"/> Yes
Spreading algorithm	<input type="radio"/> Max spreading <input checked="" type="radio"/> Fixed spreading (not recommended with zones)



- Define rules to automatically adjust capacity
- Scale out (increase) the number of VMs in the set
- Scale in (reduce) the number of VMs in the set
- Schedule events to increase or decrease at a fixed time
- Reduces monitoring and optimizes performance



Implementing Autoscale

- Define a minimum, maximum, and default number of VM instances
- Create more advanced scale sets with scale out and scale in parameters

Instance	
Initial instance count * ⓘ	<input type="text" value="2"/>
Scaling	
Scaling policy ⓘ	<input type="radio"/> Manual <input checked="" type="radio"/> Custom
Minimum number of VMs * ⓘ	<input type="text" value="1"/>
Maximum number of VMs * ⓘ	<input type="text" value="10"/>
Scale out	
CPU threshold (%) * ⓘ	<input type="text" value="75"/>
Duration in minutes * ⓘ	<input type="text" value="10"/>
Number of VMs to increase by * ⓘ	<input type="text" value="1"/>
Scale in	
CPU threshold (%) * ⓘ	<input type="text" value="25"/>
Number of VMs to decrease by * ⓘ	<input type="text" value="1"/>



Azure Administrator Associate

EXAM: AZ-104



Module 08: Azure Virtual Machines

#38: Virtual Machine Extensions



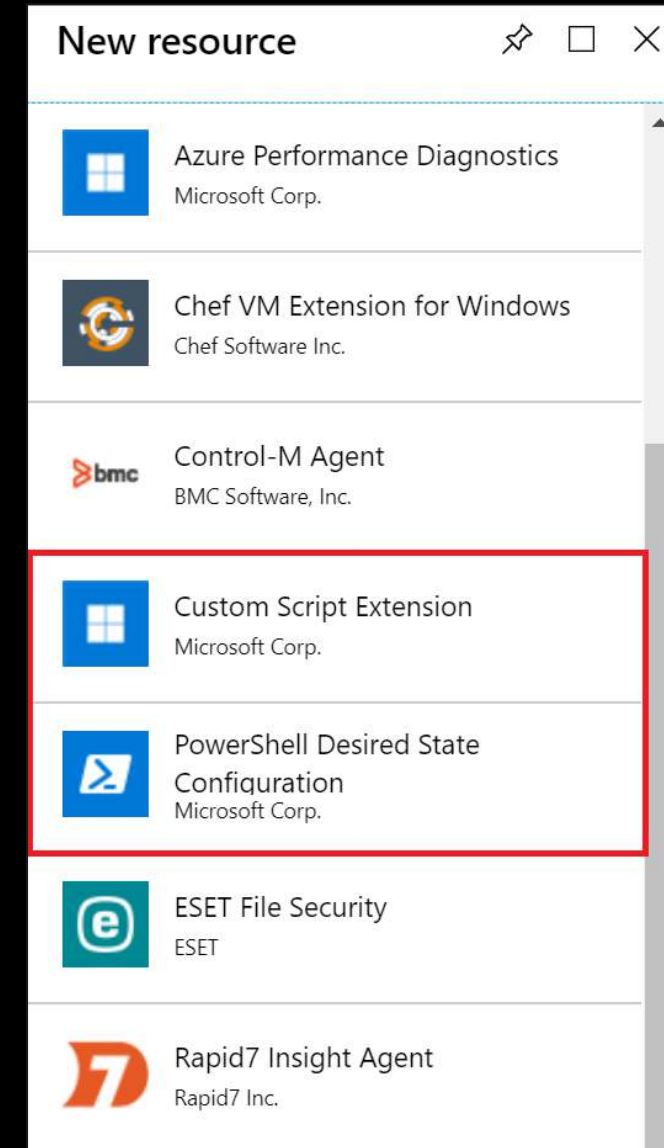
Virtual Machine Extensions Overview

- Virtual Machine Extensions
- Custom Script Extensions
- Desired State Configuration
- Demonstration – Custom Script Extension



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





Custom Script Extensions

- Extension scripts can be simple or complex
- Extensions have 90 minutes to run
- Double check dependencies to ensure availability
- Account for any errors that might occur
- Protect/encrypt sensitive information

Install extension

Script file (Required) * ⓘ

Select a file

Arguments (Optional) ⓘ

✓ For PowerShell use the `Set-AzVmCustomScriptExtension` command



Desired State Configuration

- Configuration block(s) have a name
- Node blocks define the computers or VMs that you are configuring
- Resource block(s) configure the resource and its properties
- There are many built-in configuration resources

```
configuration IISInstall
{
  Node "localhost"
  {
    WindowsFeature IIS
    {
      Ensure = "Present"
      Name = "Web-Server"
    }
  }
}
```



Demonstration – Custom Script Extension

- Verify the Web Server feature is available on a virtual machine
- Create a PowerShell script file to install the Web Server
- Configure an Extension in the Portal to run the script
- Verify the Web Server feature was installed



Azure Administrator Associate

EXAM: AZ-104



Module 08: Azure Virtual Machines

#39: Review Questions



Review Question 1

You host a service with two Azure virtual machines. You discover that occasional outages cause your service to fail. What two actions can you do to minimize the impact of the outages? Select two.

- Add a load balancer.
- Put the virtual machines in an availability set.
- Put the virtual machines in a scale set.
- Add a network gateway.
- Add a third instance of the virtual machine.



Review Question 2

You are researching Microsoft Azure for your company. The company is considering deploying Windows-based VMs in Azure. However, before moving forward, the management team has asked you to research the costs associated with Azure VMs. You need to document the configuration options that are likely to save the company money on their Azure VMs. Which options should you document? (Each answer presents part of the solution. Select four.)

- Use HDD instead of SSD for VM storage.
- Use unmanaged premium storage instead of managed standard storage.
- Bring your own Windows custom images.
- Use different Azure regions.
- Use the least powerful VMs that meet your requirements.
- Place all VMs in the same resource group.
- Bring your own Windows license for each VM.



Review Question 3

You are planning to deploy several Linux VMs in Azure. The security team issues a policy that Linux VMs must use an authentication system other than passwords. You need to deploy an authentication method for the Linux VMs to meet the requirement. Which authentication method should you use? Select one.

- SSH key pair
- Azure multi-factor authentication
- Access keys
- Shared access signature
- Security vault certificate



Review Question 4

Your company has Windows Server 2012 R2 VMs and Ubuntu Linux VMs in Microsoft Azure. The company has a new project to standardize the configuration of servers across the Azure environment. The company opts to use Desired State Configuration (DSC) across all VMs. You need to ensure that DSC can be used across all the VMs. What two things should you do? Select two.

- Replace the Ubuntu VMs with Red Hat Enterprise Linux VMs.
- Deploy the DSC extension for Windows Server VMs.
- Deploy the DSC extension for Linux VMs.
- Replace the Windows Server 2012 R2 VMs with Windows Server 2016 VMs.



Review Question 5

Another IT administrator creates an Azure virtual machine scale set with 5 VMs. Later, you notice that the VMs are all running at max capacity with the CPU being fully consumed. However, additional VMs are not deploying in the scale set. You need to ensure that additional VMs are deployed when the CPU is 75% consumed. What should you do? Select one.

- Enable the autoscale option.
- Increase the instance count.
- Add the scale set automation script to the library.
- Deploy the scale set automation script.



Review Question 6

Your company is preparing to deploy an application to Microsoft Azure. The app is a self-contained unit that runs independently on several servers. The company is moving the app to the cloud to provide better performance. To get better performance, the team has the following requirements:

- **If the CPU across the servers goes above 85%, a new VM should be deployed to provide additional resources.**
- **If the CPU across the servers drops below 15%, an Azure VM running the app should be decommissioned to reduce costs.**

You need to deploy a solution to meet the requirements while minimizing the administrative overhead to implement and manage the solution. What should you do? Select one.

- Deploy the app in a virtual machine scale set.
- Deploy the app in a virtual machine availability set.
- Deploy the app by using a resource manager template.
- Deploy the app and use PowerShell Desired State Configuration (DSC).



Review Question 7

Your company is deploying a critical business application to Microsoft Azure. The uptime of the application is of utmost importance. The application has the following components:

- **2 web servers**
- **2 application servers**
- **2 database servers**

You need to design the layout of the VMs to meet the following requirements:

- **Each VM in a tier must run on different hardware**
- **Uptime for the application must be maximized**

You need to deploy the VMs to meet the requirements. What should you do? Select one.

- Deploy 1 VM from each tier into one availability set and the remaining VMs into a separate availability set.
- **Deploy the VMs from each tier into a dedicated availability set for the tier.**
- Deploy the application and database VMs in one availability set and the web VMs into a separate availability set.
- Deploy a load balancer for the web VMs and an availability set to hold the application and database VMs.



Review Question 8

Your organization has a security policy that prohibits exposing SSH ports to the outside world. You need to connect to an Azure Linux virtual machine to install software. What should you do? Select one.

- Configure the Bastion service
- Configure a Guest configuration on the virtual machine
- Create a custom script extension
- Work offline and then reimagine the virtual machine.



Azure Administrator Associate

EXAM: AZ-104



Module 09: Serverless Computing

#40: Azure App Service Plans



Azure App Service Overview

- Azure App Service Plans
- App Service Plan Pricing Tiers
- App Service Plan Scaling
- App Service Plan Scale Out
- Demonstration - Create an App Service Plan



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 (next slide)

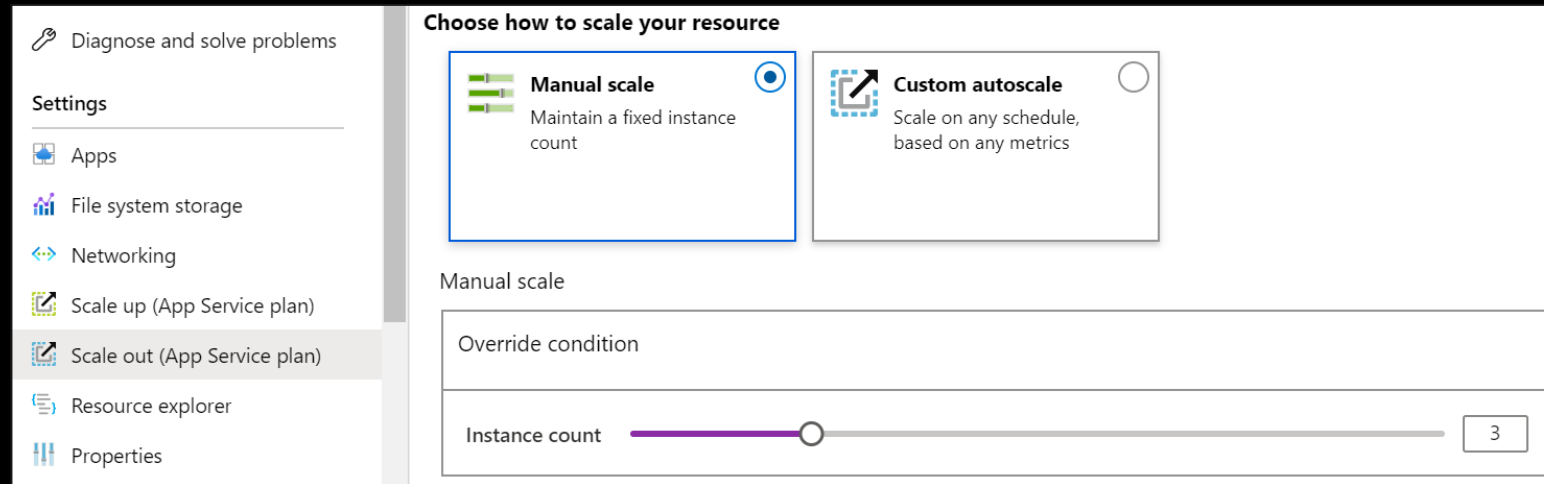


App Service Plan Pricing Tiers

Selected Features	Free	Shared (dev/test)	Basic (dedicated dev/test)	Standard (production workloads)	Premium (enhanced scale and performance)	Isolated (high-performance, security and isolation)
Web, mobile, or API apps	10	100	Unlimited	Unlimited	Unlimited	Unlimited
Disk space	1 GB	1 GB	10 GB	50 GB	250 GB	1 TB
Auto Scale	–	–	–	Supported	Supported	Supported
Deployment Slots	0	0	0	5	20	20
Max Instances	-	-	Up to 3	Up to 10	Up to 30	Up to 100

- **Shared compute** (Free and Shared). Run apps on the same Azure VM as other App Service apps, and the resources cannot scale out
- **Dedicated compute** (Basic, Standard, Premium). Run apps in the same plan in dedicated Azure VMs
- **Isolated**. Runs apps on dedicated Azure VMs in dedicated Azure virtual networks

App Service Plan Scaling



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 Scale Out

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

Rules  No metric rules defined; click hyperlink [Add a rule](#) to scale out and scale in your instances based on rules. For example: 'Add a rule that increases instance count by 1 when CPU percentage is above 70%'.
[+ Add a rule](#)

Instance limits
Minimum  Maximum  Default 

Schedule **This scale condition is executed when none of the other scale condition(s) match**

- 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



Demonstration – Create an App Service Plan

- Create an App Service Plan in the Azure Portal
- Review Pricing Tiers
- Configure Autoscaling



Azure Administrator Associate

EXAM: AZ-104



Module 09: Serverless Computing

#41: Azure App Services



Managing App Services Overview

- Azure App Service
- Creating an App Service
- Continuous Deployment
- Deployment Slots
- Creating Deployment Slots
- Securing an App Service
- Custom Domain Names
- Backup an App Service
- Application Insights
- Demonstration – Create an App Service

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 Container
- Linux or Windows
- Region closest to your users
- App Service Plan

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource Group * ⓘ
[Create new](#)

Instance Details

Name * .azurewebsites.net

Publish * Code Docker Container

Runtime stack *

Operating System * Linux Windows

Region *
ⓘ Not finding your App Service Plan? Try a different region.

App Service Plan

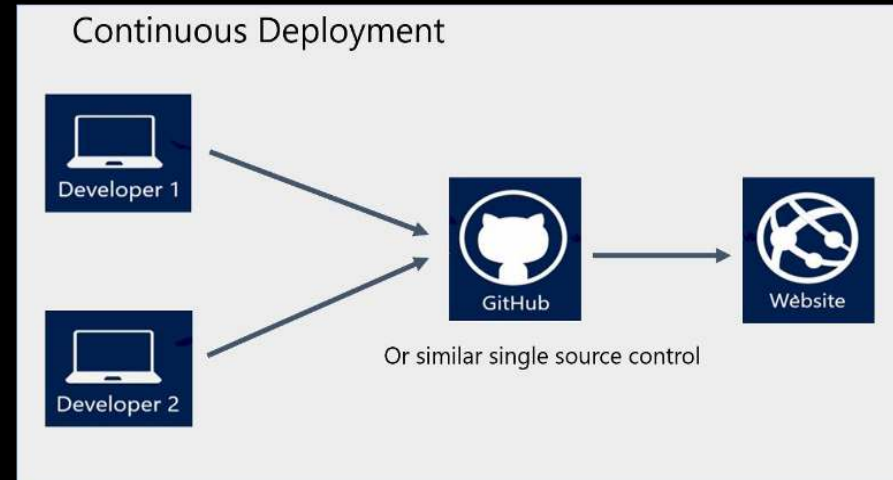
App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#) ⓘ

Windows Plan (East US) * ⓘ
[Create new](#)

Skus and size * **Standard S1**
100 total ACU, 1.75 GB memory
[Change size](#)



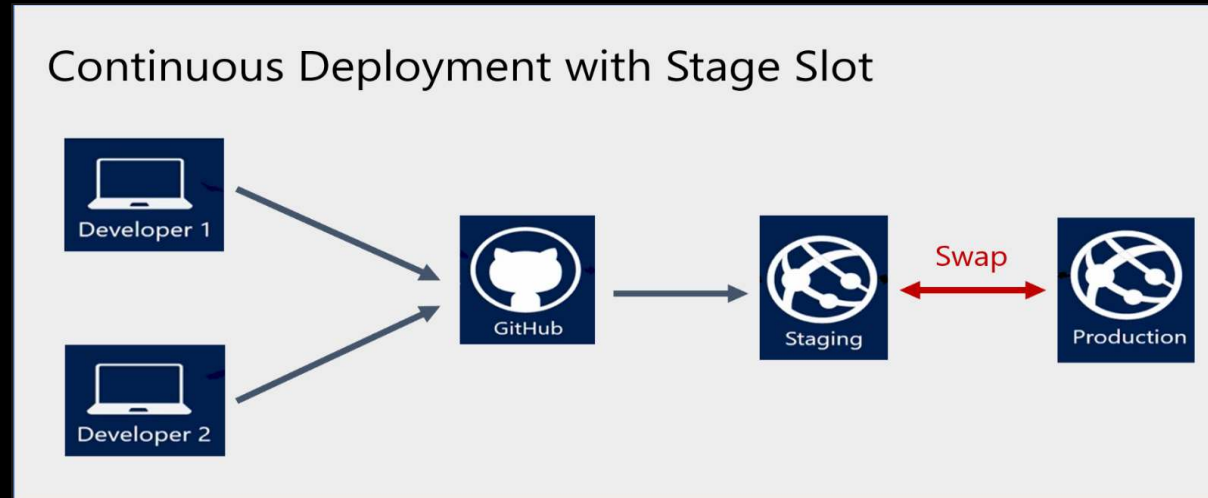
Continuous Deployment



- Work in a single source control
- Whenever code updates are pushed to the source control, then the website or web app will automatically pick up the updates
- A continuous deployment workflow publishes the most recent updates from a project
- Use the portal for continuous deployments from GitHub, Bitbucket, or Azure DevOps



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
- Auto Swap when pre-swap validation is not needed

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



Creating Deployment Slots

- A new slot can be empty or cloned
- Not all settings are sticky (endpoints, custom domain names, SSL certificates, scaling)
- Review and edit your settings before swapping

The screenshot shows a dialog box titled "Add a slot" with a close button in the top right corner. Inside the dialog, there is a "Name" label followed by a text input field containing the text "preproduction". Below this is a "Clone settings from:" label followed by a dropdown menu. The dropdown menu is open, showing three options: "Do not clone settings" (which is highlighted in light blue), "Do not clone settings", and "appservice09".

When you clone, pay attention to the settings

- Slot-specific app settings and connection strings
- Continuous deployment settings
- App Service authentication settings



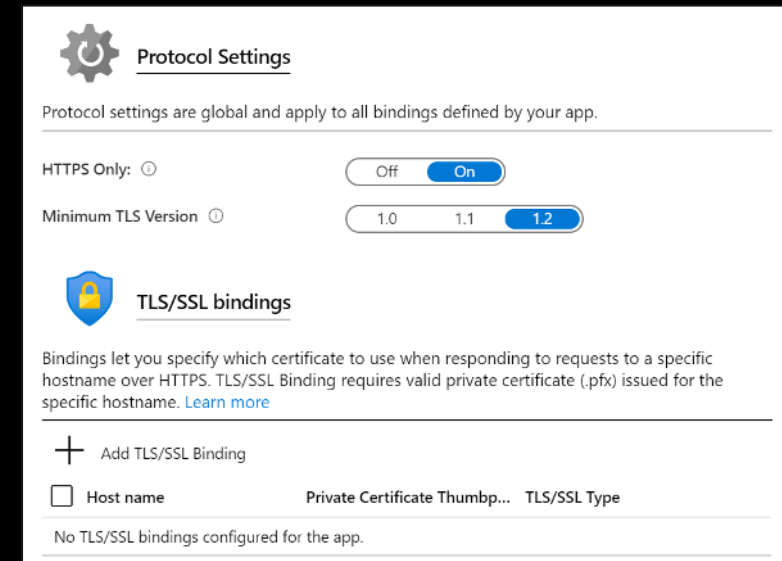
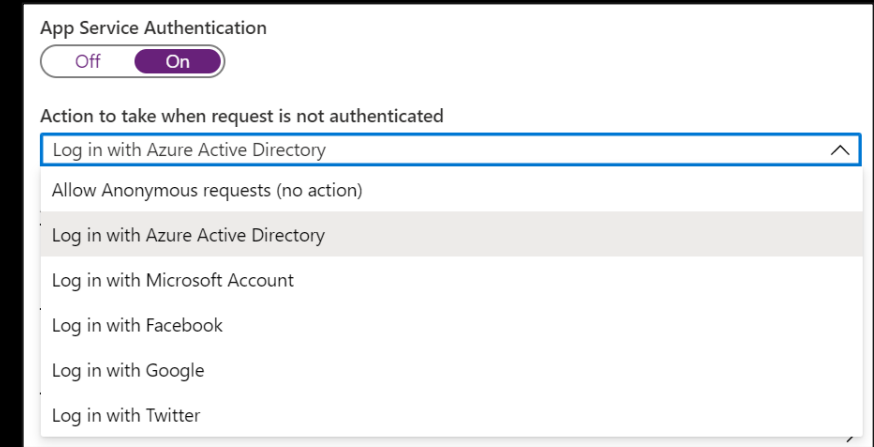
Securing an App Service

Authentication

- Enable authentication – default anonymous
- Log in with a third-party identity provider

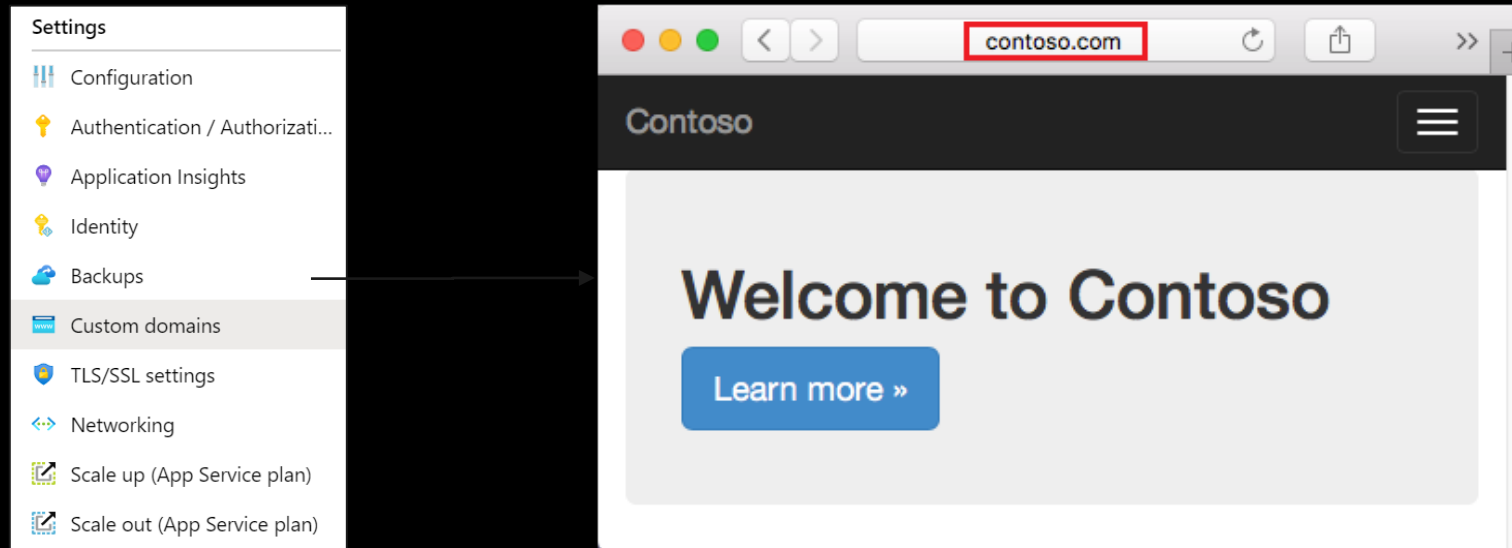
Security

- Troubleshoot with Diagnostic Logs – failed requests, app logging
- Add an SSL certificate – HTTPS
- Define a priority ordered allow/deny list to control network access to the app
- Store secrets in the Azure Key Vault





Custom Domain Names













- Redirect the default web app URL
- Validate the custom domain in Azure
- Use the DNS registry for your domain provider – create a CNAME or A record with the mapping
- Ensure App Service plan supports custom domains



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

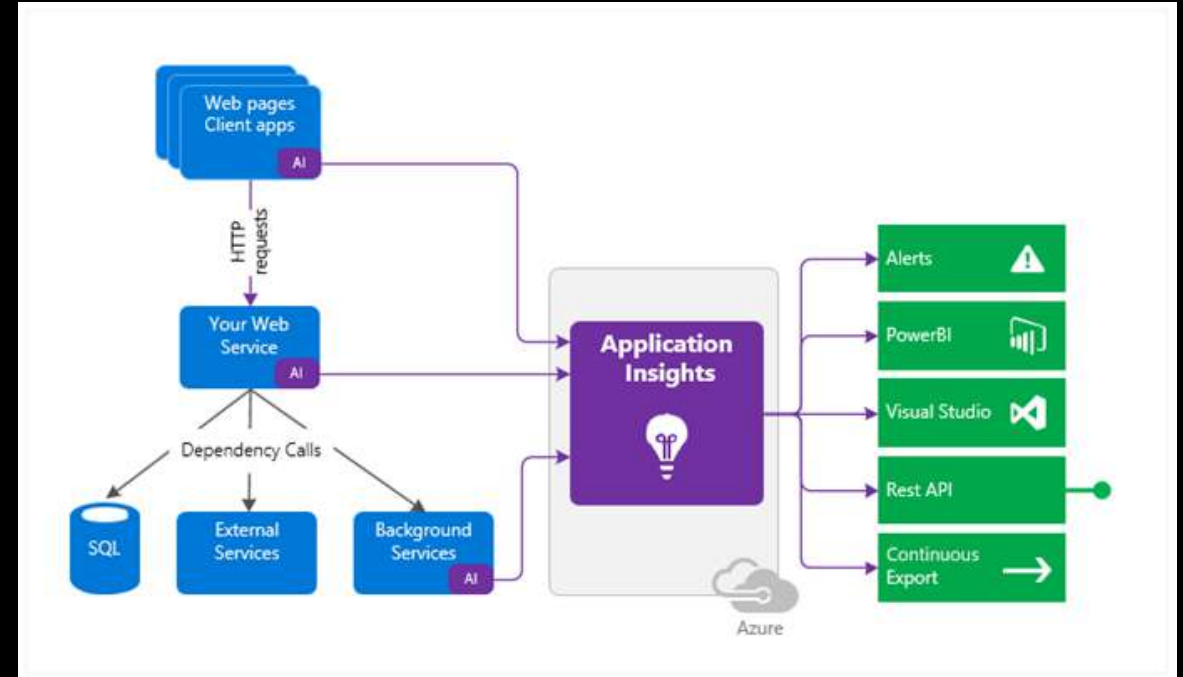
Settings

-  Configuration
-  Authentication / Authorizati...
-  Application Insights
-  Identity
-  Backups
-  Custom domains
-  TLS/SSL settings
-  Networking
-  Scale up (App Service plan)
-  Scale out (App Service plan)

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





Demonstration – Create an App Service

- Create a Web App in the Azure Portal
- Test the Web App
- Configure Deployment Slots
- Configure Backup



Azure Administrator Associate

EXAM: AZ-104



Module 09: Serverless Computing

#42: Container Services



Container Services Overview

- Containers vs. Virtual Machines
- Azure Container Instances
- Container Groups
- Docker

Containers vs Virtual Machines

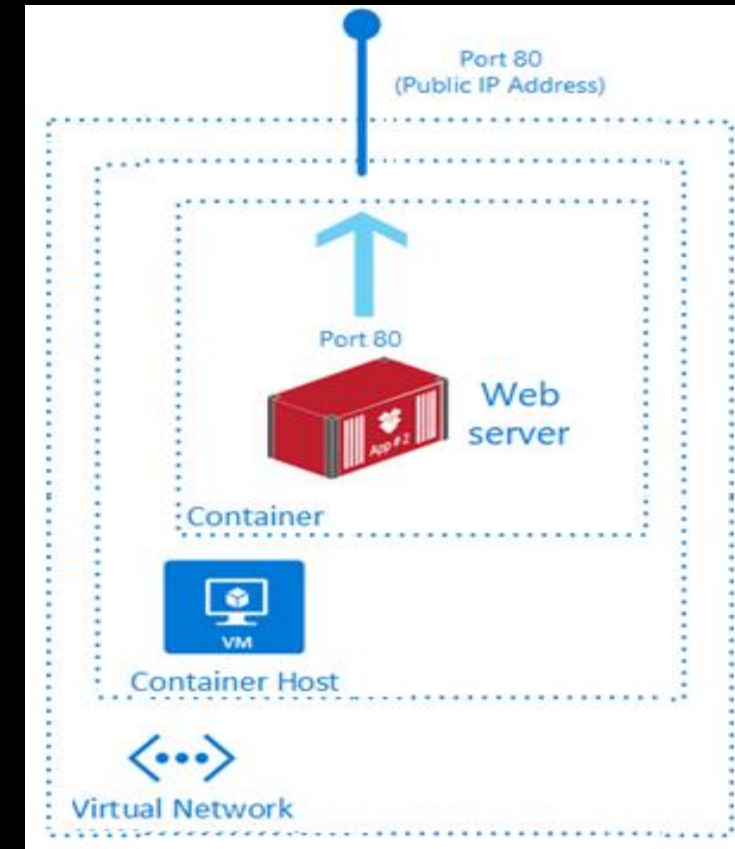


Feature	Containers	Virtual Machines
Isolation	Typically provides lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.	Provides complete isolation from the host operating system and other VMs. This is useful when a strong security 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 servers.
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

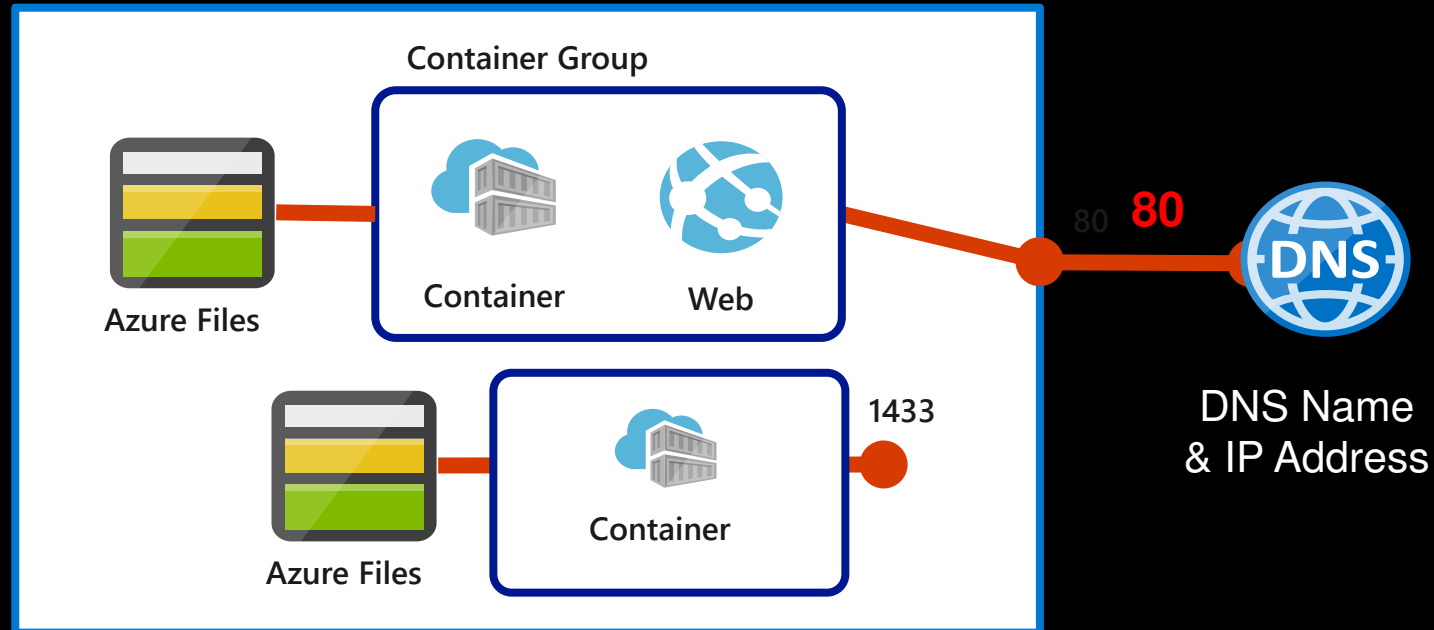
- PaaS Service
- Fast startup times
- Public IP connectivity and DNS name
- Hypervisor-level security
- Isolation features
- Custom sizes
- Persistent storage
- Linux and Windows Containers
- Co-scheduled Groups
- Virtual network Deployment



Fastest way to run a container in Azure
without provisioning a VM

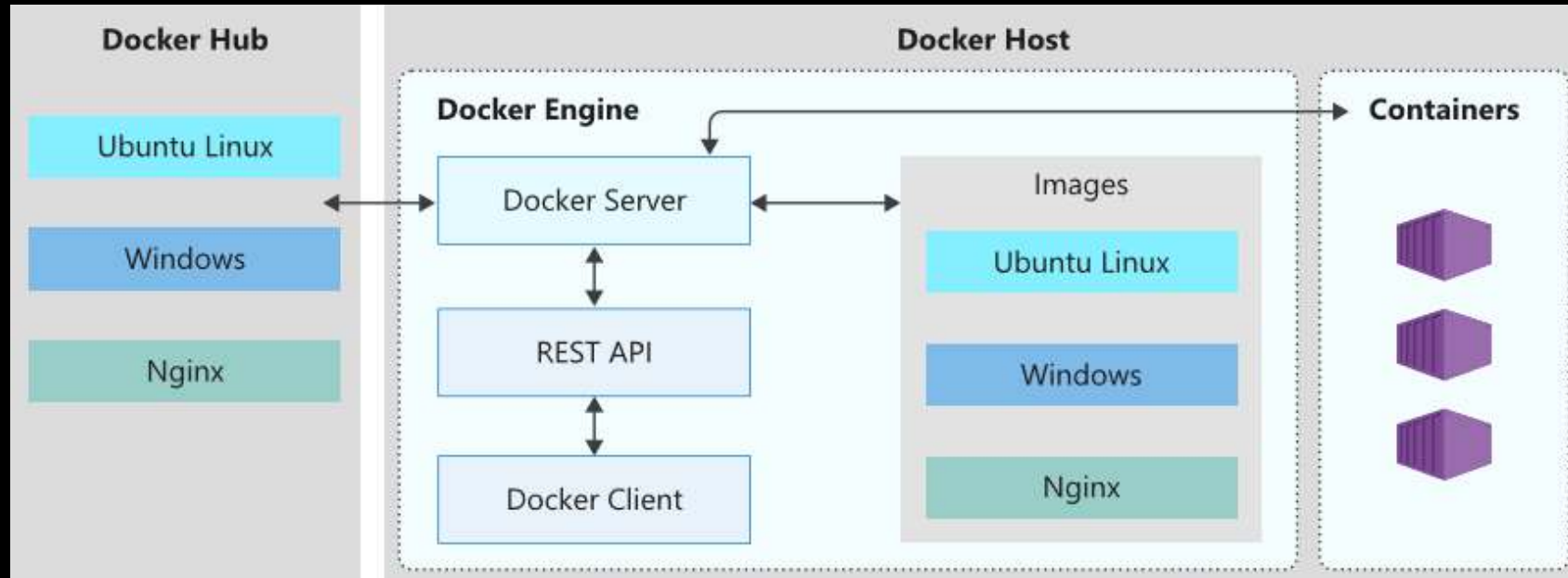


Container Groups



- Top-level resource in Azure Container Instances
- 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



Azure Administrator Associate

EXAM: AZ-104



Module 09: Serverless Computing

#43: Azure Kubernetes Service

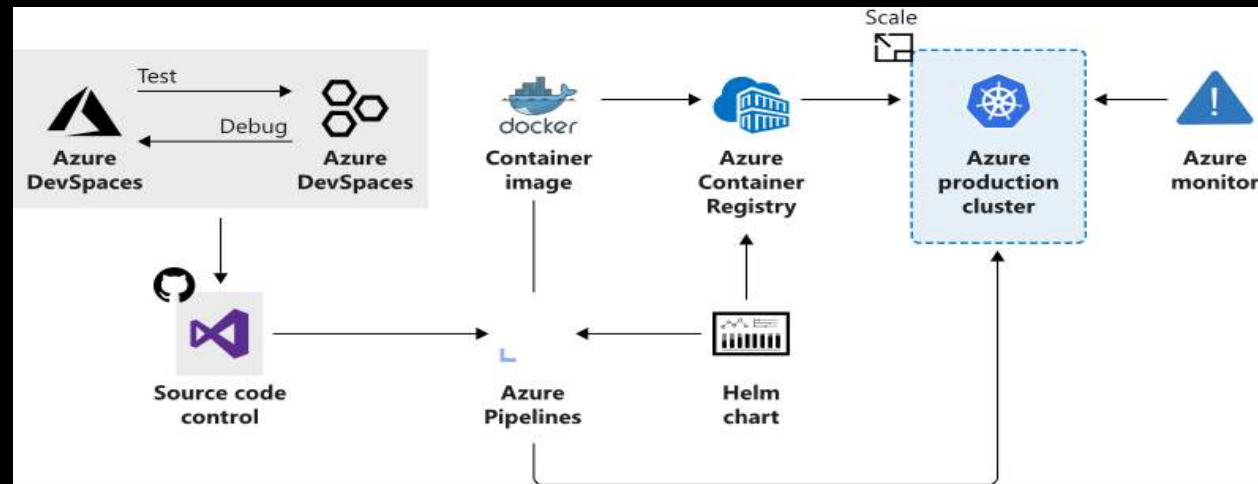


Azure Kubernetes Services Overview

- Azure Kubernetes Services (AKS)
- AKS Terminology
- AKS Clusters and Nodes
- AKS Networking
- AKS Storage
- AKS Security
- AKS and Azure Active Directory
- AKS Scaling
- AKS Scaling to ACI
- Virtual Kubelet
- Demonstration – Deploy Azure Kubernetes Service



Azure Kubernetes Service

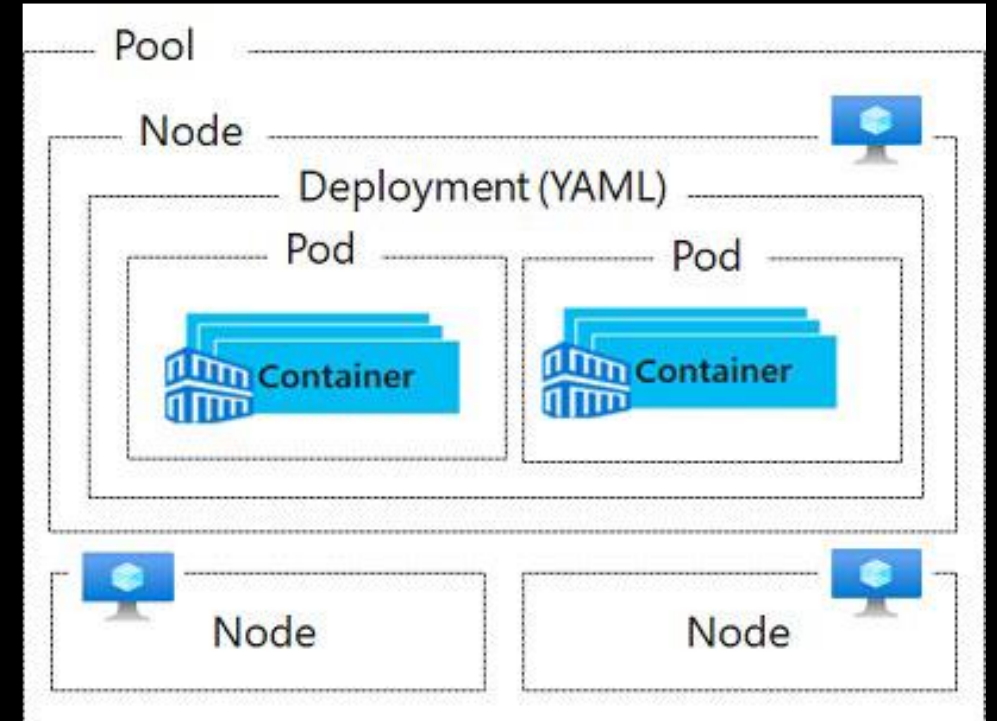


- Manages health monitoring and maintenance
- Performs simple cluster scaling
- Enables master nodes to be fully managed by Microsoft
- You're responsible only for managing the agent nodes
- Master nodes are free, and you pay only for running agent nodes

AKS Terminology

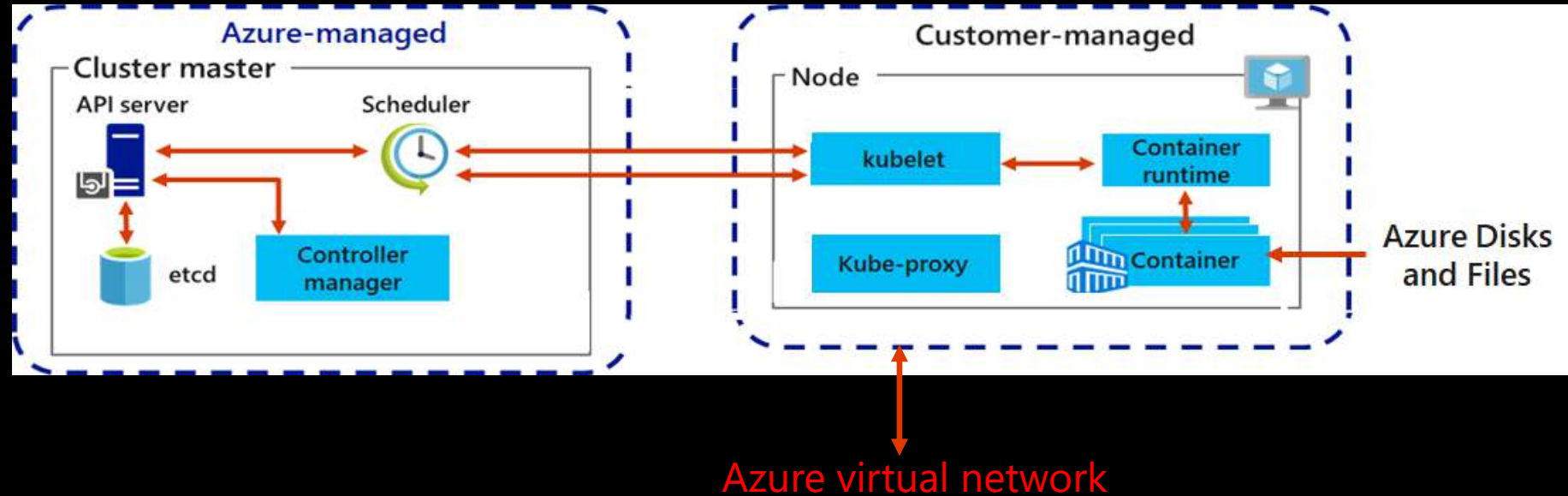


Term	Description
Pools	Groups of nodes with identical configurations.
Nodes	Individual VM running containerized applications.
Pods	Single instance of an application. A pod can contain multiple containers.
Deployment	One or more identical pods managed by Kubernetes.
Manifest	YAML file describing a deployment





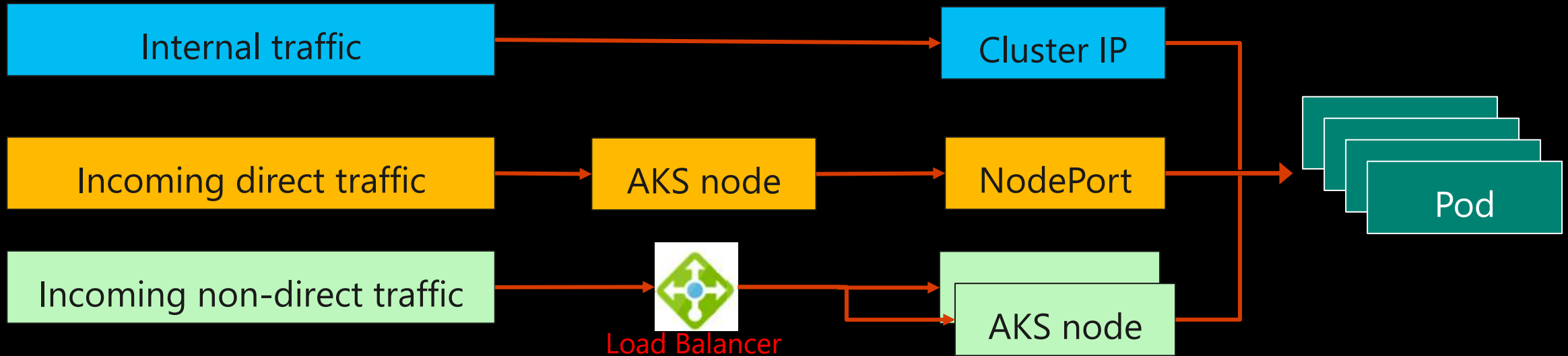
AKS Clusters and Nodes



- Cluster master provides core Kubernetes services and orchestration
- Nodes run applications and supporting services
- Each individual node is an Azure virtual machine



AKS Networking

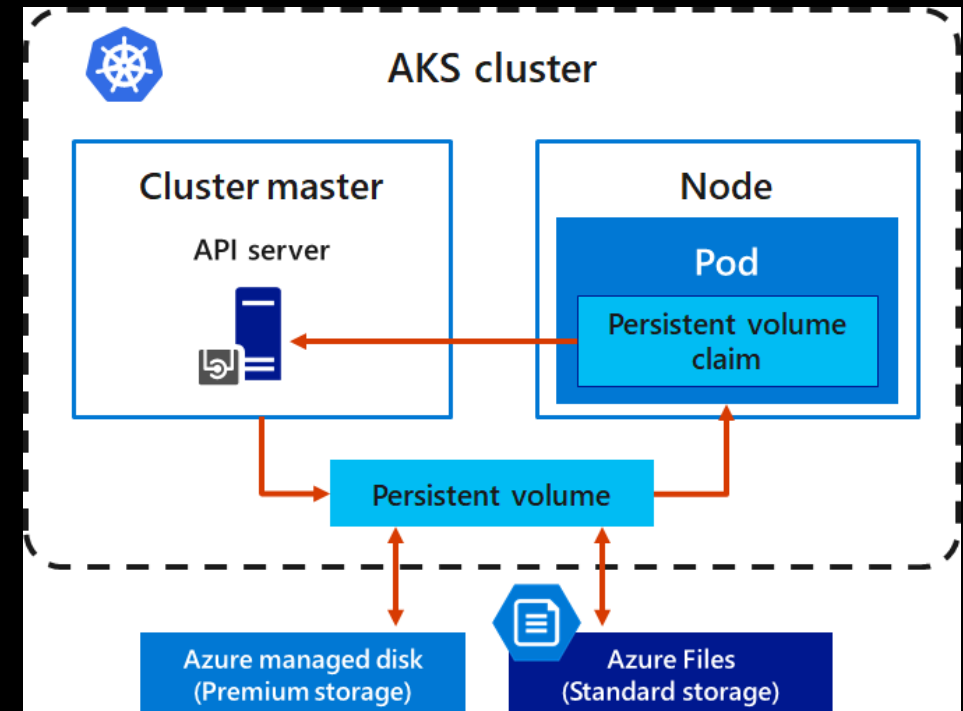


- Pods run an instance of your application
- Services group pods together to provide network connectivity
- Cluster IP provides internal traffic access
- NodePort provides mapping for incoming direct traffic
- Load balancer has external IP address for incoming non-direct traffic



AKS Storage

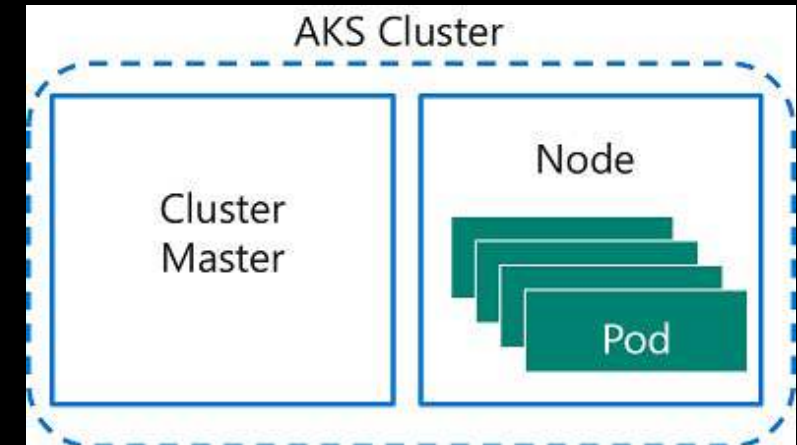
- Local storage on the node is fast and simple to use
- Local storage might not be available after the pod is deleted
- Multiple pods may share data volumes
- Storage could potentially be reattached to another pod





AKS Security

- AKS Cluster – Upgrade orchestration with node cordon and drain
- Cluster Master – fully managed
- Node – automatic OS security patches
- Networks – private virtual networks and network security groups
- Data - Kubernetes secrets for credentials and keys

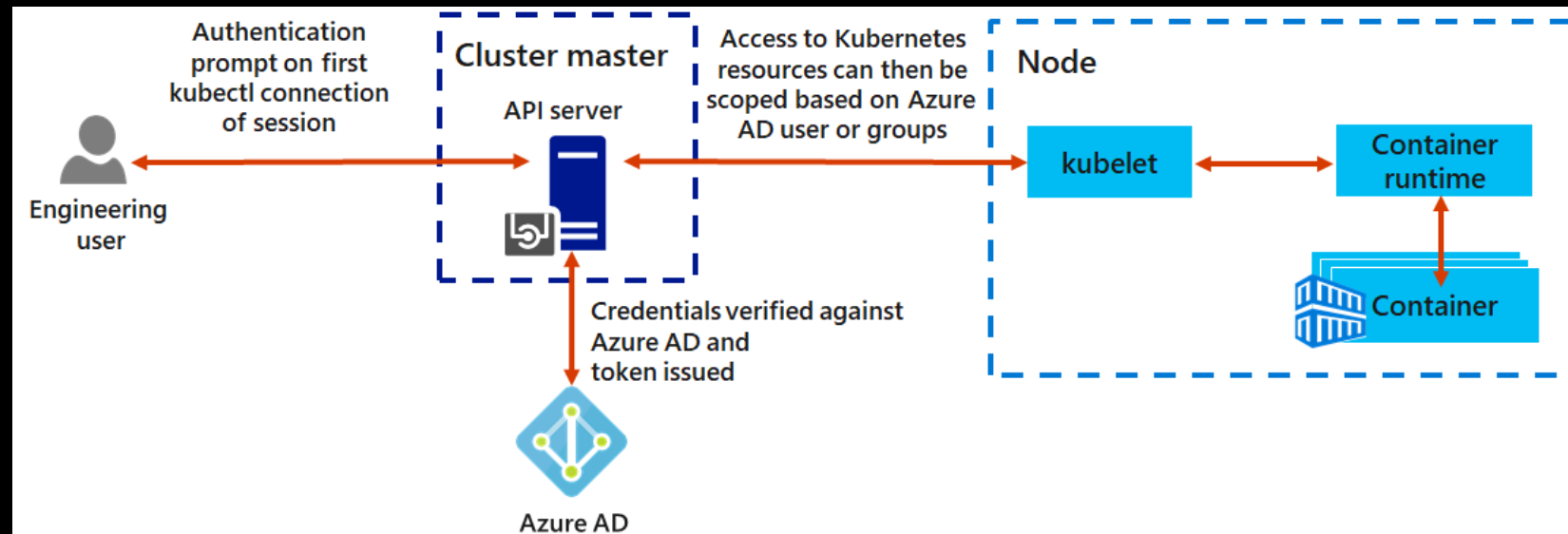


Consider security for all components



AKS and Azure Active Directory

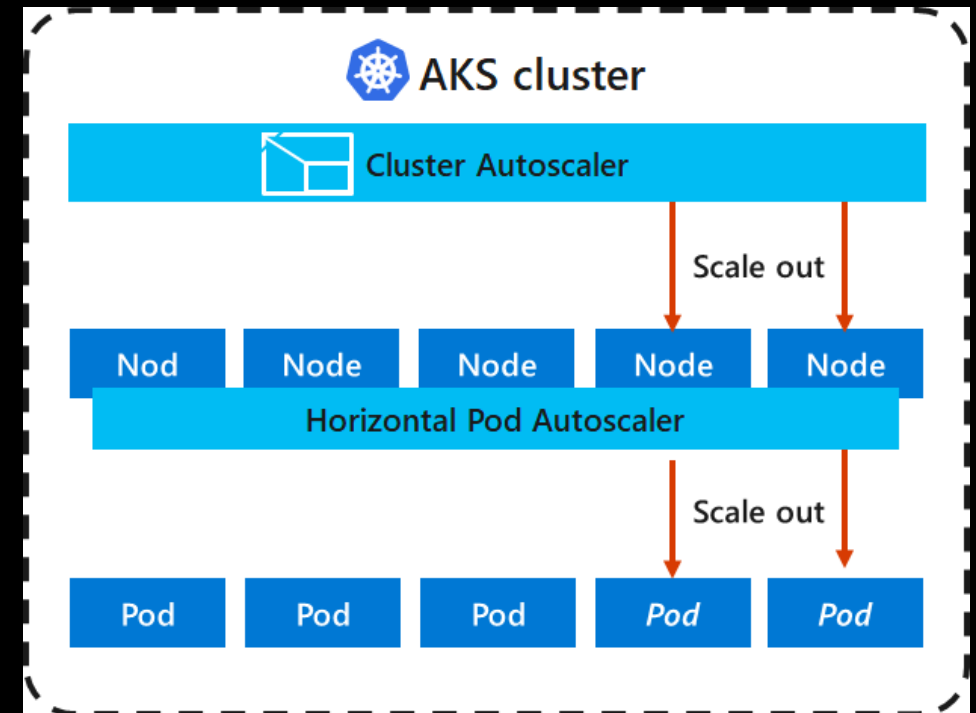
- Use Azure AD as an integrated identity solution
- Use service accounts, user accounts, and role-based access control





AKS Scaling

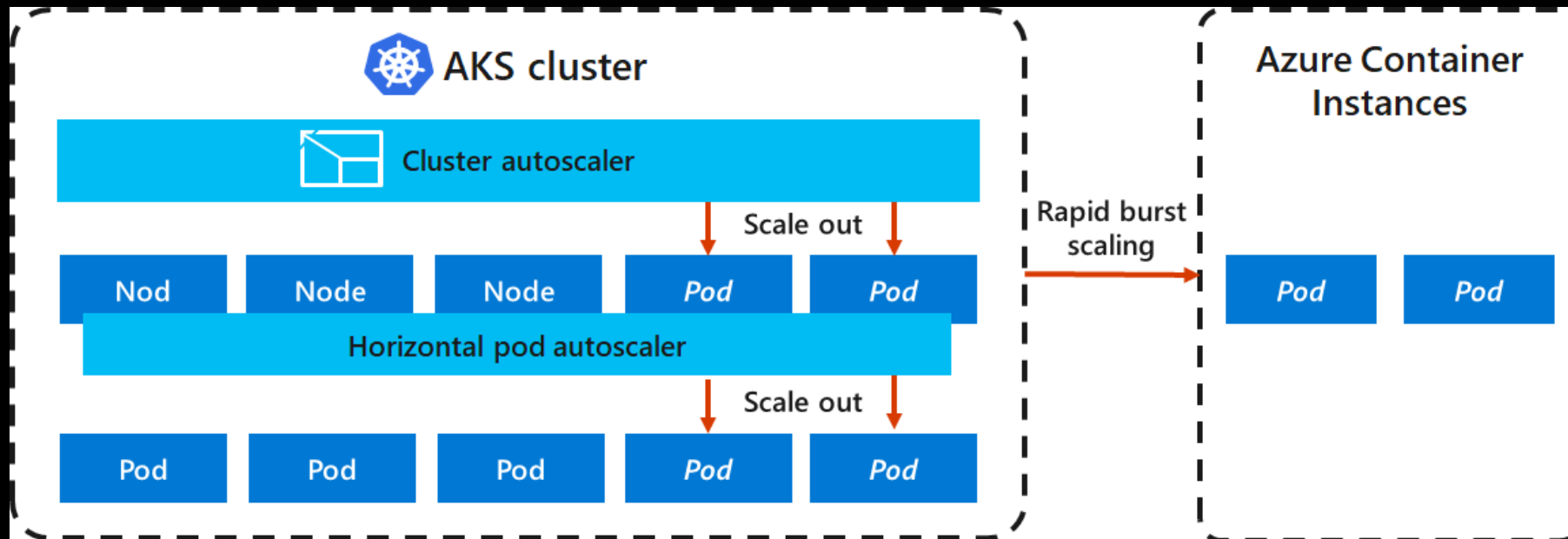
- Applications might grow beyond the capacity of a single pod
- Kubernetes has built-in autoscalers
- Cluster autoscaler scales based on compute resources
- Horizontal pod autoscaler scales based on metrics





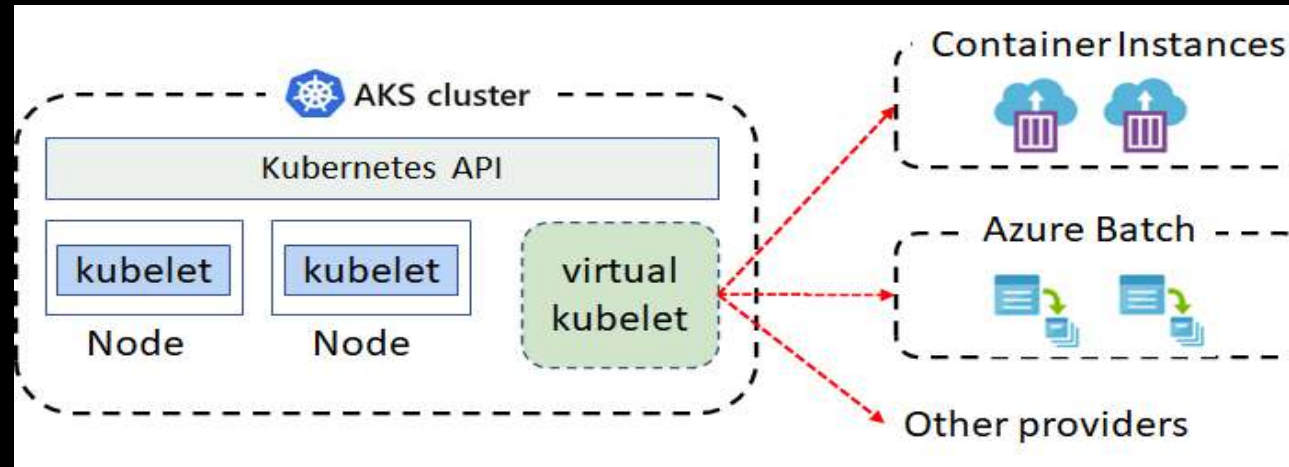
AKS Scaling to ACI

If you need to rapidly grow your AKS cluster, you can create new pods in Azure Container Instances





Virtual Kubelet

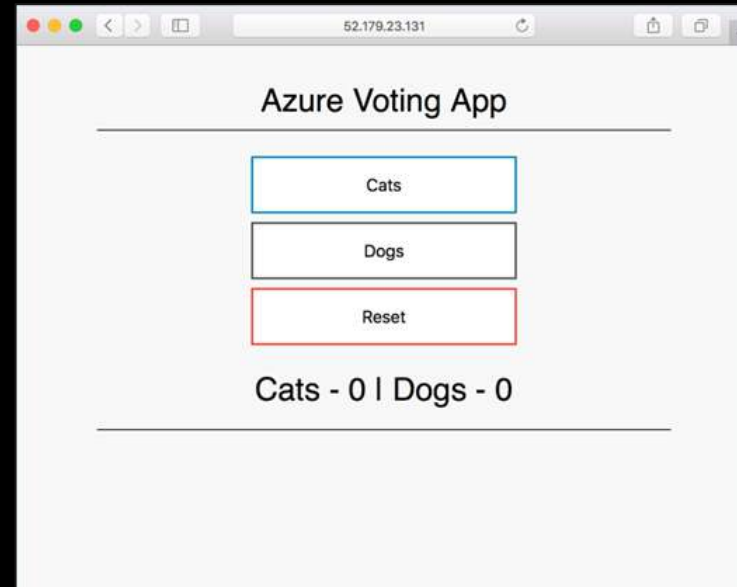


- Virtual kubelet is an open-source Kubernetes kubelet implementation
-
- The virtual kubelet registers itself as a node and allows developers to deploy pods and containers with their own APIs
- Supported by an ecosystem of providers

Demonstration - Deploy Azure Kubernetes Service



- Create a Kubernetes service
- Connect to the cluster.
- Test the applications.





Azure Administrator Associate

EXAM: AZ-104



Module 09: Serverless Computing

#44: Review Questions



Review Question 1

You have multiple apps running in a single App Service plan. True or False: Each app in the service plan can have different scaling rules.

- True

- False



Review Question 2

Which of the following settings are not swapped when you swap an app? Select three.

- Handler mappings
- Publishing endpoints
- General settings, such as framework version, 32/64-bit, web sockets
- Always On
- Custom domain names



Review Question 3

You are administering a production web app. The app requires scaling to five instances, 40GB of storage, and a custom domain name. Which App Service Plan should you select? Select one.

- Free
- Shared
- Basic
- Standard
- Premium



Review Question 4

You are backing up your App Service. Which of the following is included in the backup? Select two.

- App configuration
- Azure database for MySQL
 - Files and database content totalling 15GB
 - Firewall enabled-storage account
 - SSL enabled Azure Database for MySQL



Review Question 5

You decide to move all your services to Azure Kubernetes service. Which of the following components will contribute to your monthly Azure charge? Select one.

- Master Node
- Pods
- Node Virtual Machines
- Tables



Review Question 6

Which of the following is not true about container groups? Select one

- Is scheduled on a multiple host machines.
- Is assigned a DNS name label.
- Exposes a single public IP address, with one exposed port.
- Consists of two containers.
- Includes two Azure file shares as volume mounts.



Review Question 7

Which of the following is the Kubernetes agent that processes the orchestration requests from the cluster master, and schedules running the requested containers? Select one.

- controller master
- container runtime
- kube-proxy
- kubelet



Review Question 8

You are configuring networking for the Azure Kubernetes service. Which of the following maps incoming direct traffic to the pods? Select one.

- AKS node
- ClusterIP
- Load Balancer
- NodePort



Review Question 9

What method does Microsoft Azure App Service use to obtain credentials for users attempting to access an app? Select one.

- credentials that are stored in the browser
- pass-through authentication
- redirection to a provider endpoint
- synchronization



Azure Administrator Associate

EXAM: AZ-104



Module 10: Data Protection

#45: File and Folder Backups



File and Folder Backups Overview

- Azure Backup
- Recovery Service Vault Backup Options
- Demonstration – Backup Azure File Shares
- Implementing On-Premises File and Folder Backups
- Microsoft Azure Recovery Services Agent
- Demonstration – Backup Files and Folders



Azure Backup

- Azure-based service used to back up and restore data in Microsoft cloud
- Automatic Storage Management
- Multiple storage options
- Unlimited data transfer
- Data encryption
- Application consistent backup
- Long-term retention



Recovery Services Vault Backup Options

Azure Workloads

Where is your workload running?
Azure

What do you want to backup?
Virtual machine

- Virtual machine
- Azure FileShare**
- SQL Server in Azure VM
- SAP HANA in Azure VM

On-Premises workloads

vmbackuptest- Backup
Recovery Services vault

Where is your workload running?
On-Premises

What do you want to backup?
Files and folders

- Files and folders
- Hyper-V Virtual Machines
- VMware Virtual Machines
- Microsoft SQL Server
- Microsoft SharePoint
- Microsoft Exchange
- System State
- Bare Metal Recovery

Step: Prepare Infrastructure

Prepare Infrastructure



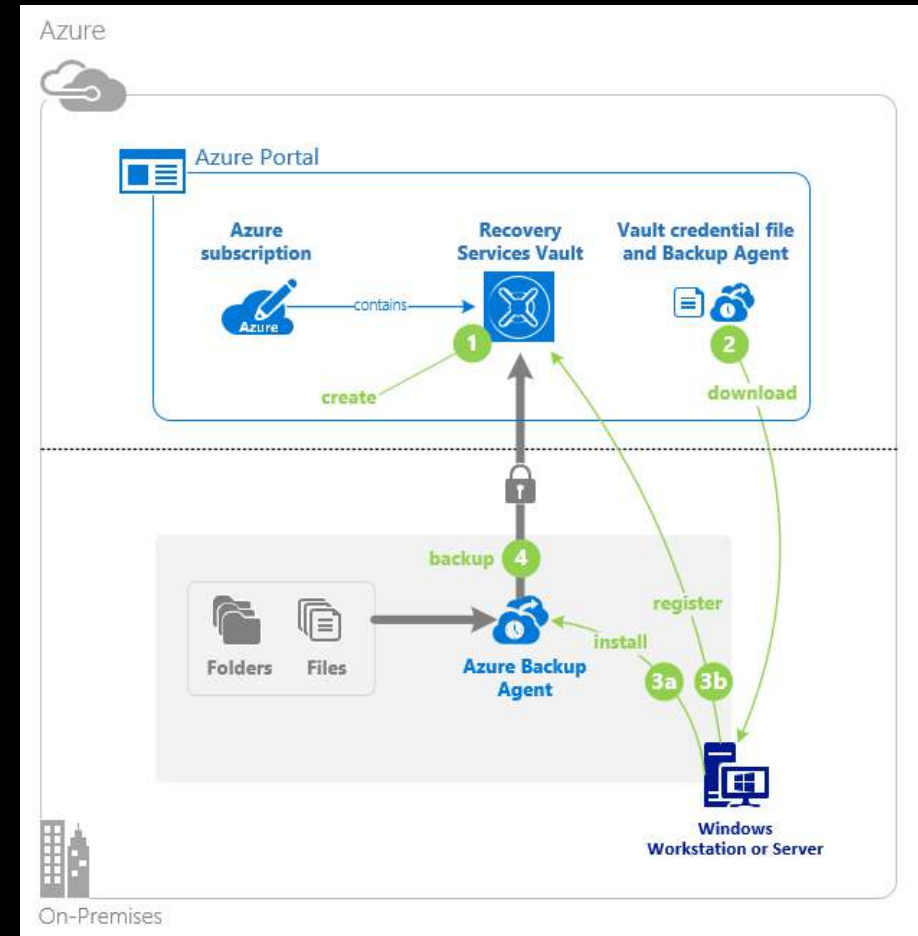
Demonstration – Backup Azure File Shares

- Configure a storage account with file share
- Create a Recovery Services vault
- Configure file share backup
- Verify the file share backup



Implementing On-Premises File and Folder Backup

- Create the recovery services vault
- Download the agent and credential file
- Install and register agent
- Configure the backup



Microsoft Azure Recovery Services Agent



Microsoft Azure Backup

Microsoft Azure Backup supports scheduled backups of files and folders to an cloud storage account.

⚠ Backups have not been configured for this server. Click "Schedule Backup" in the Actions pane to configure backups. You can also Configure Notifications from Alerts blade to receive email alerts for backup failures. [Learn More](#).

Jobs (Activity in the past 7 days, double click on the message to see details)

Status	Time	Message	Description
✓	2/28/2019 6:48 AM	Recovery	Job completed.
✓	2/28/2019 6:45 AM	Recovery	Job completed.
✓	2/28/2019 6:41 AM	Backup	Job completed.

Actions

- Backup
- Register Server
- Schedule Backup
- Recover Data
- Change Properties
- Open Portal
- Privacy & Cookies
- View
- Help

- Backup or recover files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)
- No separate backup server required
- Not application aware; file, folder, and volume-level restore only
- No support for Linux



Demonstration – Backup Files and Folders

- Create a Recovery Services vault
- Configure the vault
- Install and register the agent
- Create the backup policy
- Backup files and folders
- Explore the recover settings
- Explore the backup properties
- Delete your backup schedule



Azure Administrator Associate

EXAM: AZ-104



Module 10: Data Protection

#46: Virtual Machine Backups



Virtual Machine Backups Overview

- Virtual Machine Data Protection
- Workload Protection Needs
- Virtual Machine Snapshots
- Recovery Services Vault VM Backup Options
- Implementing VM Backups
- Implementing VM Restore
- Azure Backup Server
- Backup Component Comparison
- Soft Delete
- Azure Site Recovery
- Azure to Azure Architecture

Virtual Machine Data Protection



Snapshots

Azure Backup

Azure Site Recovery

- Managed snapshots provide a quick and simple option for backing up VMs that use Managed Disks
- Azure Backup supports application-consistent backups for both Windows and Linux VMs
- Azure Site Recovery protects your VMs from a major disaster scenario when a whole region experiences an outage

Workload Protection Needs

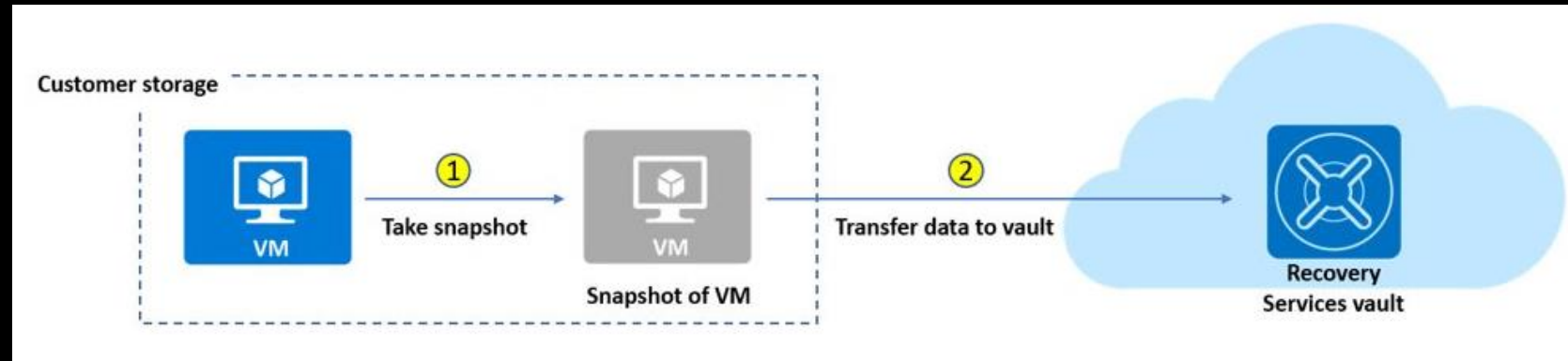


- Many backup options are available
- How the workload is being protected today?
- How often is the workload is backed up?
- What types of backups are being done?
- Is disaster recovery protection in place?

The screenshot shows the Microsoft Azure Marketplace interface. At the top, there's a navigation bar with 'Why Azure', 'Solutions', 'Products', 'Documentation', 'Pricing', 'Partners', 'Blog', 'Resources', and 'Support'. Below this is a search bar with 'backup' entered and a search icon. The search results are displayed in a grid format. On the left, there's a 'Product Category' sidebar with various categories like Compute, Networking, Storage, etc. The main content area shows 'Product results (23)'. The first row contains four 'Acronis Backup' results, each with a description: 'The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available'. The second row contains four other backup services: 'Seagate Backup Services', 'Managed Backup Portal', 'OFFICE 365 CLOUD BACKUP', and 'Quickbooks Online Backup'. Each result card includes a logo, a brief description, and a 'Get it now' button.



Virtual Machine Snapshots



- Use snapshots taken as part of a backup job
- Reduces recovery wait times – don't wait for data transfer to the vault to finish
- Configure Instant Restore retention (1 to 5 days)



Recovery Services Vault VM Backup Options

Azure Workloads

Where is your workload running?
Azure

What do you want to backup?
Virtual machine

- Virtual machine
- Azure FileShare
- SQL Server in Azure VM
- SAP HANA in Azure VM

On-Premises Workloads

vmbackuptest - Backup
Recovery Services vault

Where is your workload running?
On-Premises

What do you want to backup?
4 selected

- Files and folders
- Hyper-V Virtual Machines
- VMware Virtual Machines
- Microsoft SQL Server
- Microsoft SharePoint
- Microsoft Exchange
- System State
- Bare Metal Recovery

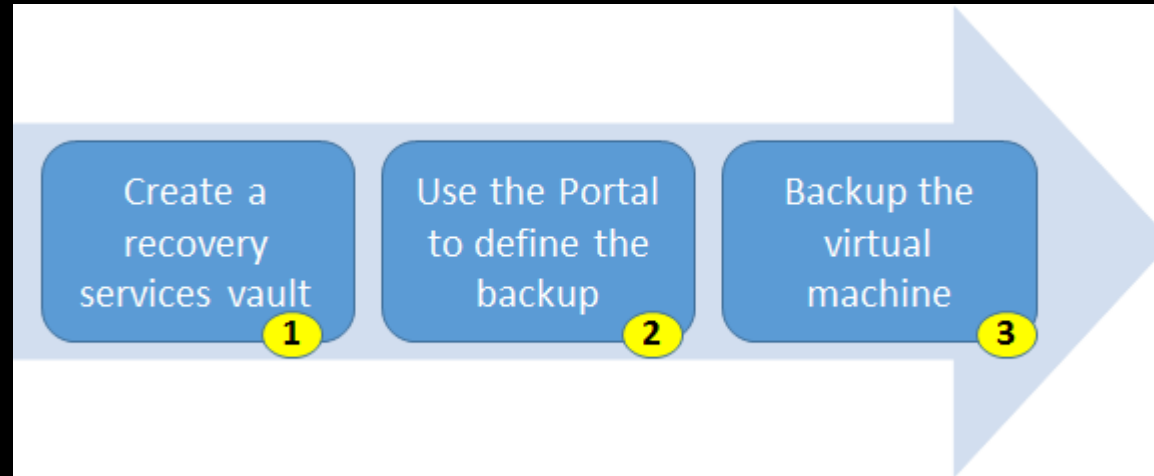
Step: Prepare Infrastructure

Prepare Infrastructure

- ✓ Multiple servers can be protected using the same Recovery Services vault



Implementing VM Backups



- Use a Recovery Services Vault in the region where you are performing your Virtual Machine backups and choose a replication strategy for the Vault.
- Take snapshots (recovery points) of your data at defined intervals. These snapshots are stored in recovery services vaults.
- For the Backup extension to work, the Azure VM Agent must be installed on the Azure virtual machine.



Implementing VM Restore

- Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation
- The Backup service also creates and temporarily displays notifications, so you monitor how the backup is proceeding

ContosoWebFE1
Backup Item

Backup now Restore VM File Recovery Stop backup Resume backup

Alerts and Jobs Backup status

[View all Alerts](#) (last 24 hours) Backup Pre-Check ✔ Passed

[View all Jobs](#) (last 24 hours) Last backup status ✔ Success 3/12/2020, 12:20:38 AM

Restore points (30)

CRASH CONSISTENT	APPLICATION CONSISTENT	FILE-SYSTEM CONSISTENT
30	0	0

Time	Consistency
3/12/2020, 12:20:42 AM	Crash Consistent
3/11/2020, 12:20:59 AM	Crash Consistent



Azure Backup Server



- App-aware backups, file/folder/volume backups, and machine state backups (bare-metal, system state)
- Each machine runs the DPM/MABS protection agent, and the MARS agent runs on the MABS/DPM
- Flexibility and granular scheduling options
- Manage backups for multiple machines in a protection group



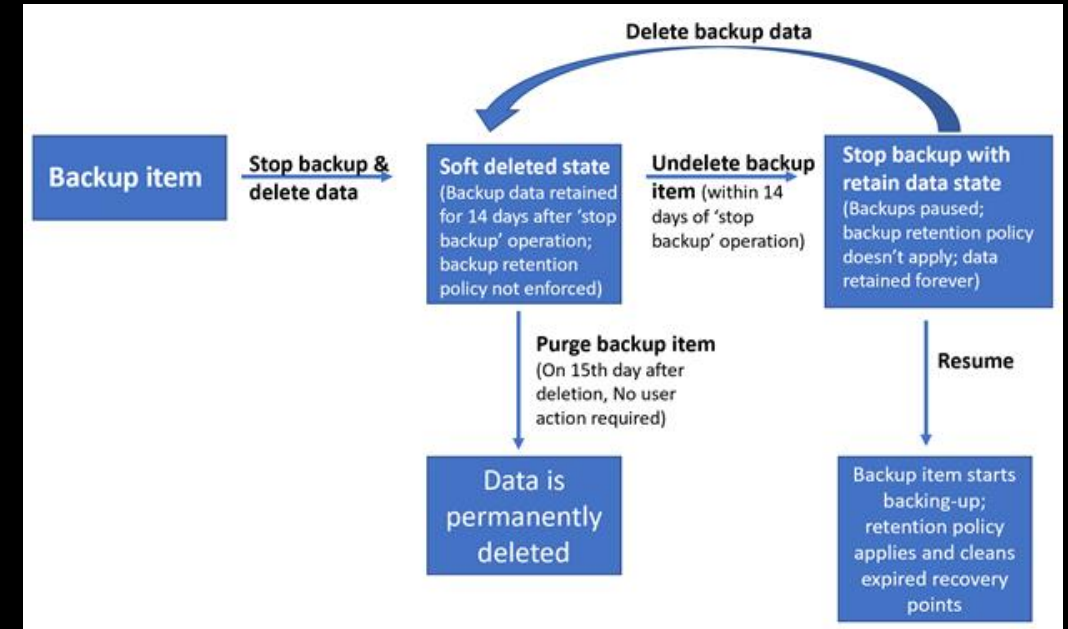
Backup Component Comparison

Component	Benefits	Limits	Protects	Backup Storage
Azure Backup (MARS) agent	<ul style="list-style-type: none"> • Backup files and folders on physical or virtual Windows OS • No separate backup server required. 	<ul style="list-style-type: none"> • Backup 3x per day • Not application aware • File, folder, and volume-level restore only • No support for Linux 	<ul style="list-style-type: none"> • Files • Folders 	<ul style="list-style-type: none"> • Recovery services vault
Azure Backup Server	<ul style="list-style-type: none"> • App aware snapshots • Full flex for when to backups • Recovery granularity • Linux support on Hyper-V and VMware VMs • Backup and restore VMware VMs • Doesn't require a System Center license 	<ul style="list-style-type: none"> • Cannot backup Oracle workloads • Always requires live Azure subscription • No support for tape backup 	<ul style="list-style-type: none"> • Files • Folders, • Volumes • VMs • Applications • Workloads 	<ul style="list-style-type: none"> • Recovery services vault • Locally attached disk

Soft Delete



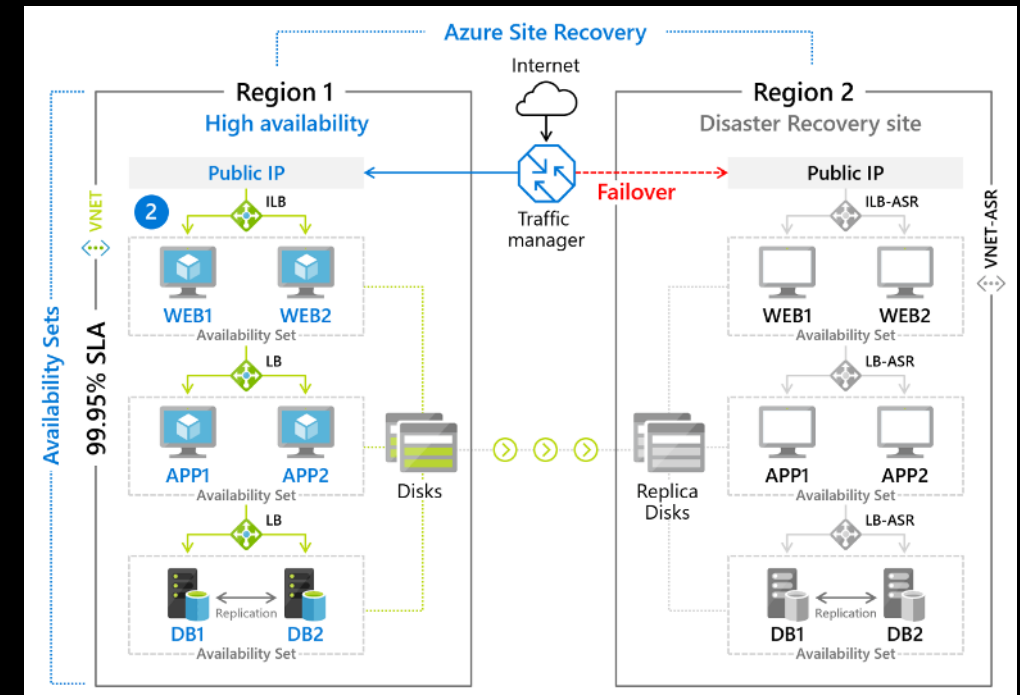
- Backup data is retained for 14 additional days
- Recover soft deleted backup items using an 'Undelete' operation
- Natively built-in for all the recovery services vaults





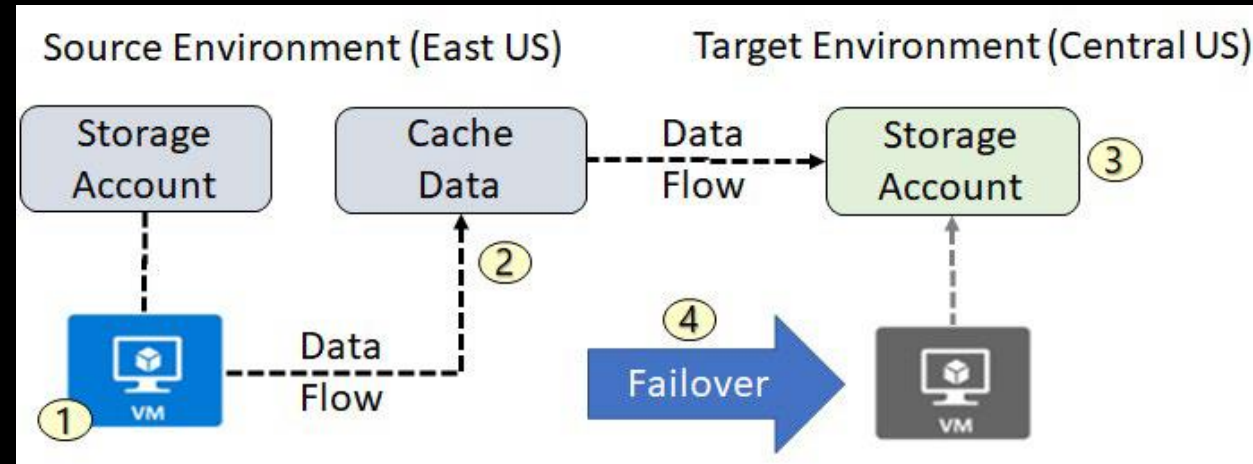
Azure Site Recovery

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





Azure to Azure Architecture



1. VM is registered with Azure Site Recovery
2. Data is continuously replicated to cache
3. Cache is replicated to the target storage account
4. During failover the virtual machine is added to the target environment



Azure Administrator Associate

EXAM: AZ-104



Module 10: Data Protection

#47: Review Questions



Review Question 1

You need to backup files and folders to Azure. Which three steps must you perform?

- Download, install and register the backup agent.
- Synchronize configuration.
- Back up files and folders.
- Create a backup services vault.
- Create a recovery services vault.



Review Question 2

You are responsible for creating a disaster recovery plan for your data center. You must be able to recreate virtual machines from scratch. This includes the Operating System, its configuration/ settings, and patches. Which of the following will provide a bare metal backup of your machines? Select one.

- Azure Backup (MARS) agent
- Enable disk snapshots
- Azure Site Recovery
- Azure Backup Server



Review Question 3

You have several Azure VMs that are currently running production workloads. You have a mix of Windows Server and Linux servers and you need to implement a backup strategy for your production workloads. Which feature should you use in this case? Select one.

- Managed snapshots.
- Azure Backup.
- Azure Site Recovery.
- Azure Migrate.



Review Question 4

You plan to use Azure Backup to protect your virtual machines and data and are ready to create a backup. What is the first thing you need to do? Select one.

- Define recovery points.
- Create a Recovery Services vault.
- Create a Backup policy.
- Install the Azure VM Agent.



Review Question 5

You deploy several virtual machines (VMs) to Azure. You are responsible for backing up all data processed by the VMs. In the event of a failure, you need to restore the data as quickly as possible. Which of these options would you recommend to restore a database used for development on a data disk? Select one.

- Virtual machine backup
- Azure Site Recovery
- Disk image backup
- Disk snapshot



Review Question 6

You deploy several virtual machines (VMs) to Azure. You are responsible for backing up all data processed by the VMs. In the event of a failure, you need to restore the data as quickly as possible. Which of these options would you recommend to restore the entire virtual machine or files on the virtual machine? Select one.

- Virtual machine backup
- Azure Site Recovery
- Disk image backup
- Disk snapshot



Review Question 7

Your organization needs a way to create application aware snapshots, and backup Linux virtual machines and VMware virtual machines. You have files, folders, volumes, and workloads to protect. You recommend which of the following solutions? Select one.

- Azure Backup (MARS) agent
- Azure Backup Server
- Enable disk snapshots
- Enable backup for individual Azure VMs



Review Question 8

You plan to use virtual machine soft delete. Which of the following statements are true? Select two.

- Soft delete provides 20 days extended retention of data.
- If you delete a backup, soft delete still provides recovery of data.
- Soft delete is built-in protection at no additional cost.
- Soft delete items are stored in archive storage.
- A recovery service vault can be deleted if it



Azure Administrator Associate

EXAM: AZ-104



Module 11: Monitoring

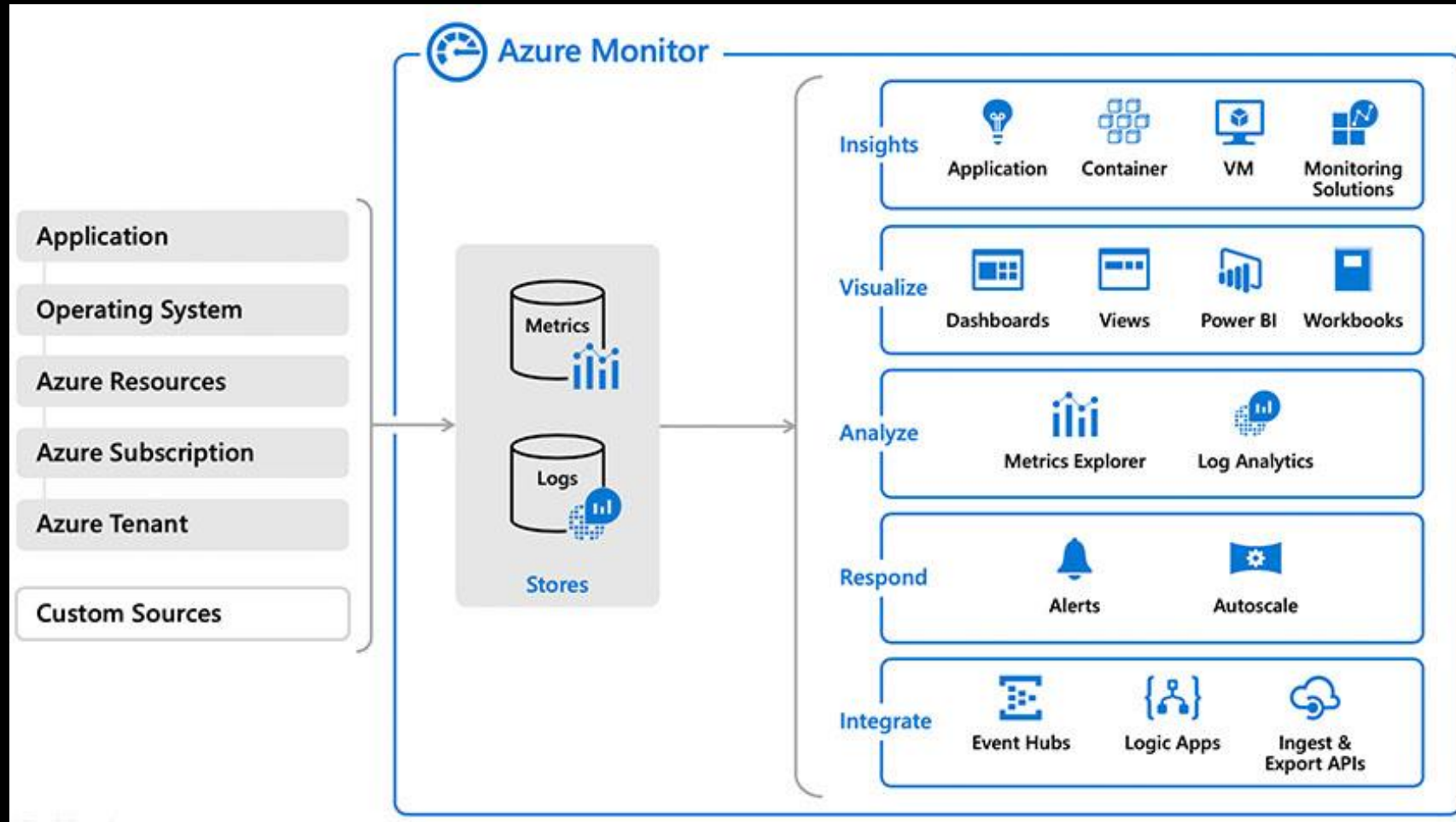
#48: Azure Monitor



Azure Monitor Overview

- Azure Monitor Service
- Key Capabilities
- Monitoring Data Platform
- Log Data
- Data Types
- Azure Advisor
- Activity Log
- Query the Activity Log

Azure Monitor Service



Key Capabilities



Monitor & Visualize Metrics
Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.
[Explore Metrics](#)

Query & Analyze Logs
Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.
[Search Logs](#)

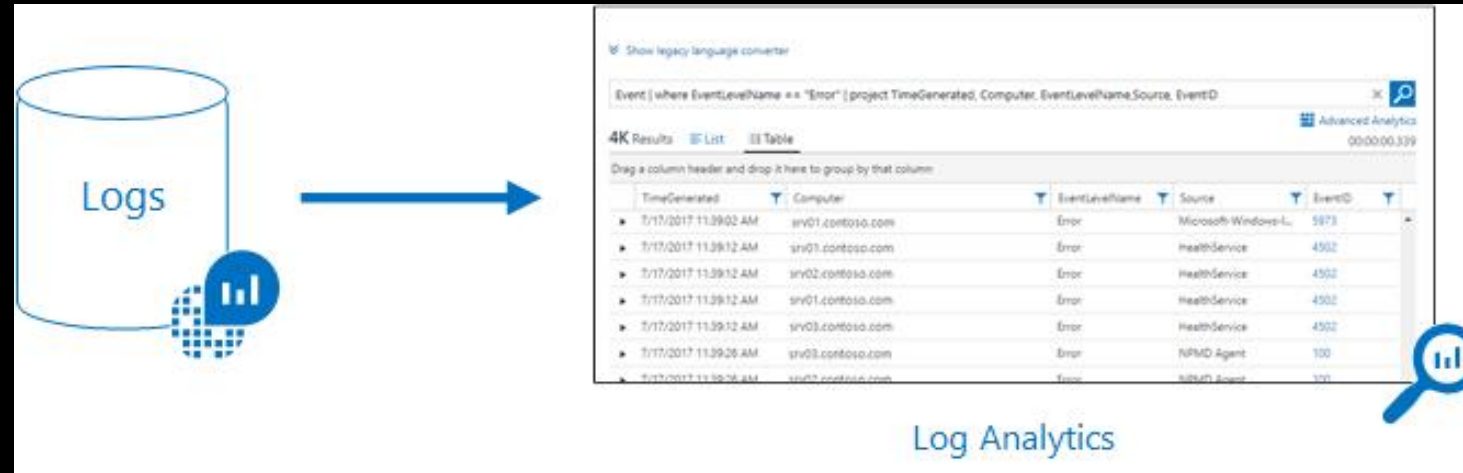
Setup Alert & Actions
Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.
[Create Alert](#)

- Core monitoring for Azure services
- Collects metrics, activity logs, and diagnostic logs
- Use for time critical alerts and notifications

Monitoring Data Platform



- **Metrics** are numerical values that describe some aspect of a system at a point in time. They are lightweight and capable of supporting near real-time scenarios.
- **Logs** contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis.



- Log data is stored in Log Analytics which includes a rich query language to quickly retrieve, consolidate, and analyze collected data
- The Data Explorer query language that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics



Data Types

Application monitoring data

- Performance and functionality of the code you have written, regardless of its platform

Guest OS monitoring

- Azure, another cloud, or on-premises

Azure resource monitoring

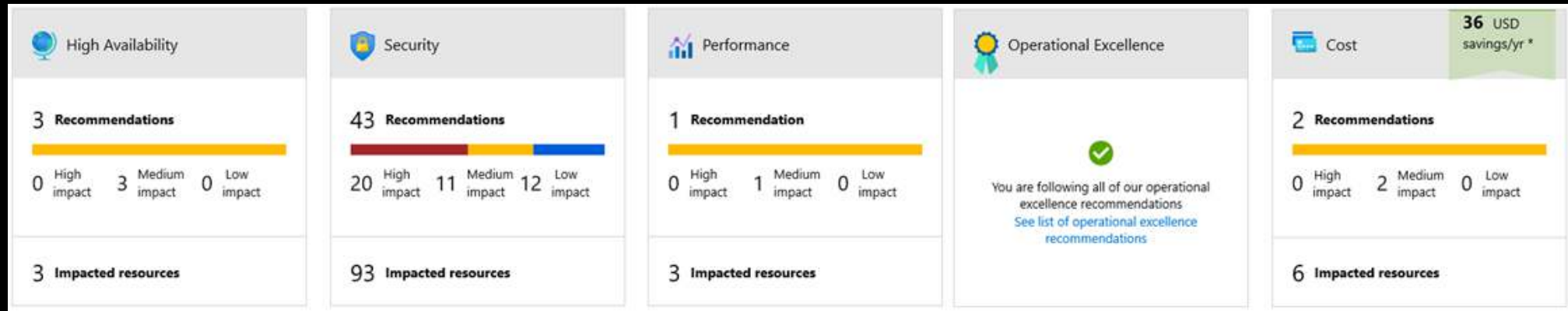
Azure subscription monitoring

- Operation and management of an Azure subscription, as well as data about the health and operation of Azure itself

Azure tenant monitoring

- Operation of tenant-level Azure services, such as Azure Active Directory

Azure Advisor

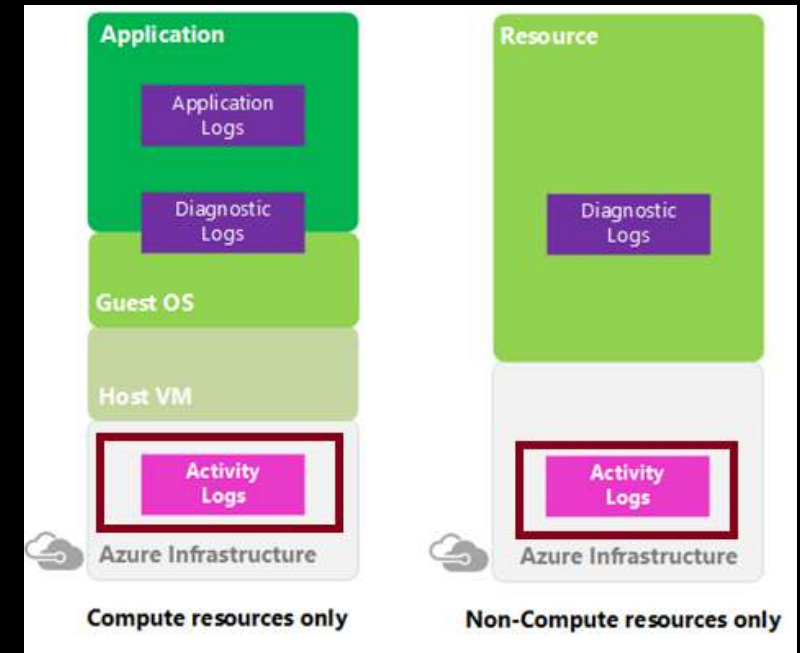


- Personalized cloud consultant
- Analyzes your configuration and recommends solutions
- High Availability, Security, Performance, Operational Excellence, and Cost

Activity Log



- Send data to Log Analytics for advanced search and alerts
- Query or manage events in the Portal, PowerShell, CLI, and REST API
- Stream information to Event Hub
- Archive data to a storage account
- Analyze data with Power BI





Query the Activity Log

Activity log

Edit columns Refresh Diagnostics settings Download as CSV Logs Pin current filters

Search Quick Insights Add Filter

Management Group : None Subscription : 2 selected Timespan : Last 6 hours Event severity : All

Operation name	Status	Time	Time stamp	Subscription
> Create or Update Virtual Network Subnet	Failed	a minute ago	Thu Mar 12 ...	ASC DEMO
> Write GuestConfigurationAssignments	Succeeded	17 minutes ...	Thu Mar 12 ...	ASC DEMO
> Gets workflow recommend operation groups	Succeeded	29 minutes ...	Thu Mar 12 ...	ASC DEMO

- Filter by: Management group, Subscription, Timespan, and Event Severity
- Add a filter, like Event Category (Security, Recommendations, Alerts)
- Pin current filters and download as CSV



Azure Administrator Associate

EXAM: AZ-104



Module 11: Monitoring

#49: Azure Alerts



Azure Alerts Overview

- Azure Monitor Alerts
- Creating Alert Rules
- Action Groups
- Demonstration - Alerts



Azure Monitor Alerts

Alerts

+ New alert rule ⚙️ Manage alert rules 👤 Manage actions 🔔 View classic alerts ↻ Refresh 😊 Provide feedback

Total alerts 1179 Since 2/11/2020, 11:07:58 AM	Smart groups (Preview) ⓘ 3 99.75% Reduction	Total alert rules 9 Enabled 7	Action rules (preview) ⓘ 0 Enabled 0	
Severity	Total Alerts	New	Acknowledged	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0
Sev 2	0	0	0	0
Sev 3	1178	1178	0	0
Sev 4	1	1	0	0

- Unified authoring experience
- Displayed by severity
- Categorized by New, Acknowledged, and Closed



Creating Alert Rules

1. Resource: Target selection, Alert criteria, and Alert logic
2. Condition: Alert rule name, description, and severity (0 to 4)
3. Action group: notify your team via email and text messages or automate actions using webhooks and runbooks

Create rule
Rules management

*** RESOURCE**
Select the target(s) that you wish to monitor
[Select](#)

*** CONDITION**
No condition defined, click on 'Add condition' to select a signal and define its logic
[Add condition](#)

ACTION GROUPS
Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more [here](#)

ACTION GROUP NAME	ACTION GROUP TYPE
No action group selected	

[Select existing](#) [Create New](#)

Action Groups



- Notifies a group of users that an alert has been triggered
- Is a collection of notification preferences

Action name *	Action Type *
Unique name for the action	Select an action type ^
	Automation Runbook
	Azure Function
	Email Azure Resource Manager Role
	Email/SMS/Push/Voice
	ITSM
	LogicApp
	Secure Webhook
	Webhook



Demonstration - Alerts

- Create an alert rule
- Explore alert targets
- Explore alert conditions
- Explore alert details



Azure Administrator Associate

EXAM: AZ-104



Module 11: Monitoring

#50: Log Analytics



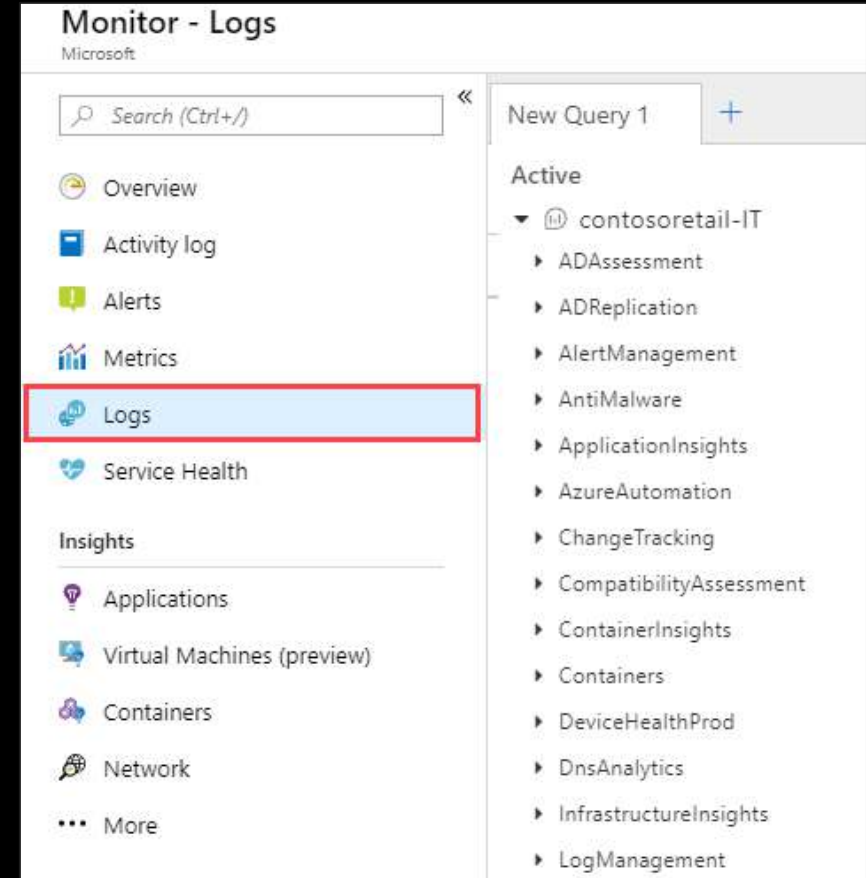
Log Analytics Overview

- Log Analytics
- Create a Workspace
- Connected Sources
- Data Sources
- Log Analytics Querying
- Query Language Syntax
- Demonstration – Log Analytics



Log Analytics

- A service that helps you collect and analyze data generated by resources in your cloud and on-premises environments
- Write log queries and interactively analyze their results
- Examples include assessing system updates and troubleshooting operational incidents





Create a Workspace

- A workspace is an Azure resource and is a container where data is collected, aggregated, analyzed, and presented
- You can have multiple workspaces per Azure subscription, and you can have access to more than one workspace
- A workspace provides a geographic location, data isolation, and scope

Log Analytics workspace

Create new or link existing workspace

Create New Link Existing

Log Analytics Workspace * ⓘ

Subscription *
Azure Pass - Sponsorship ▼

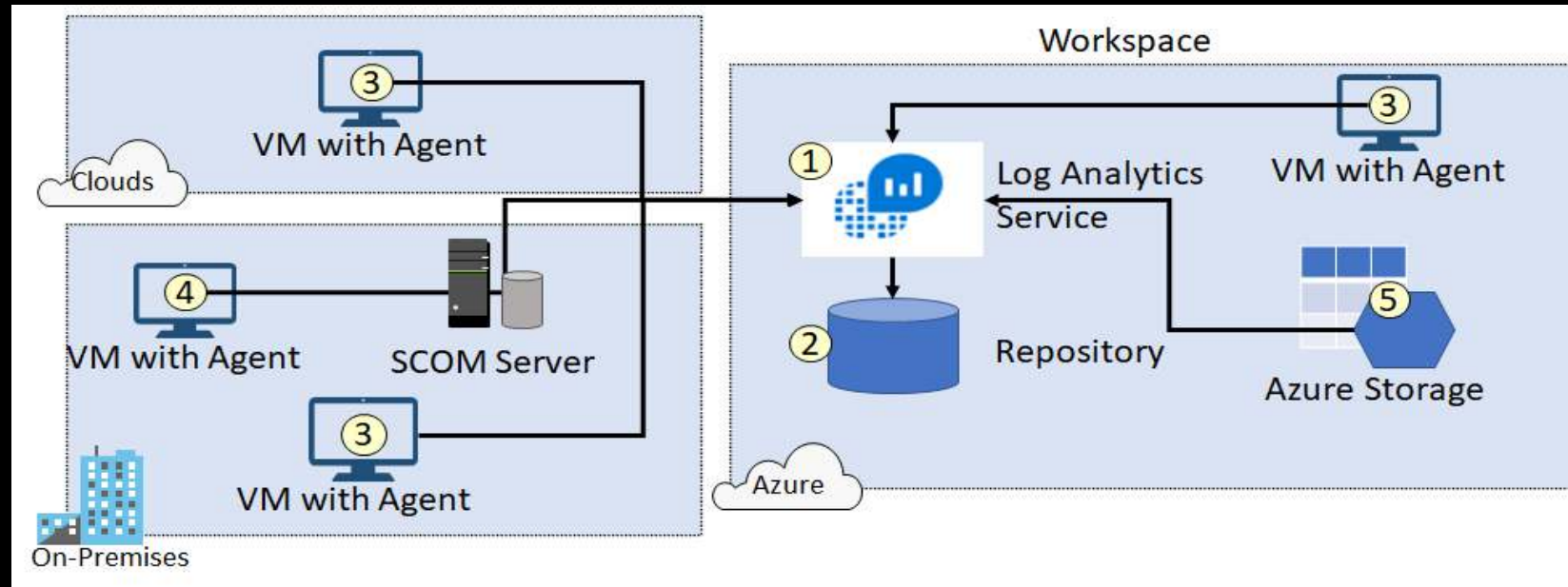
Resource group *
Select existing... ▼

[Create new](#)

Location *
West US ▼



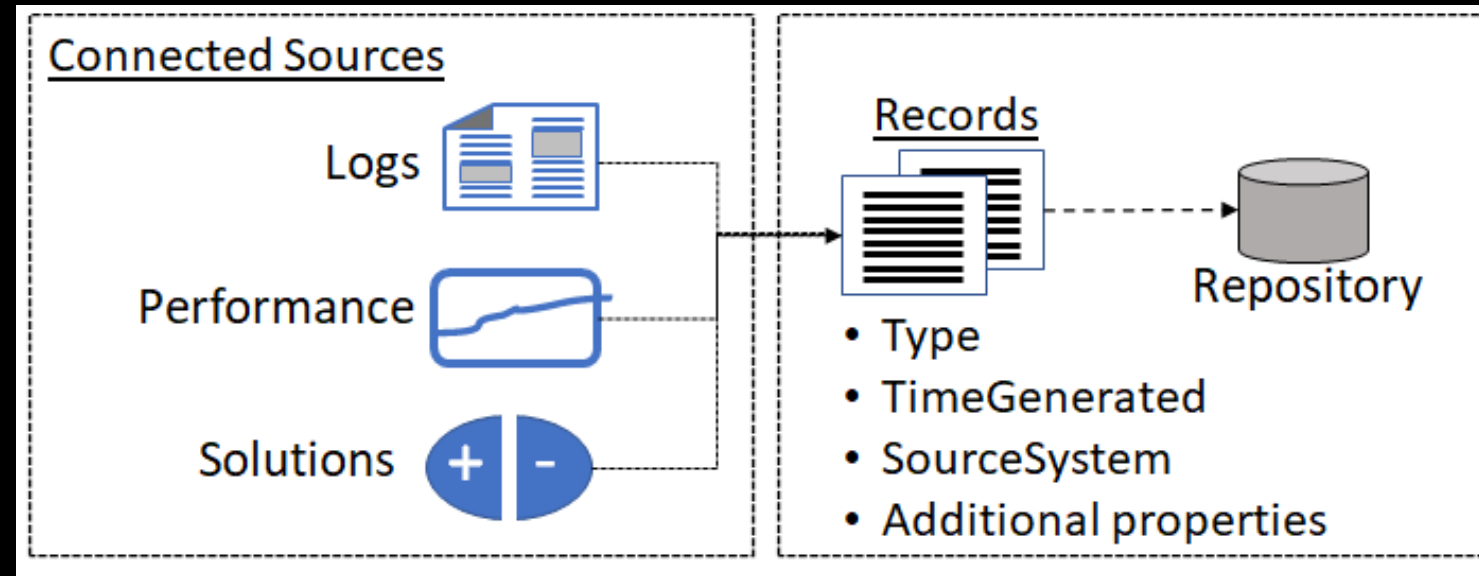
Connected Sources



- Connected Sources generate data
- Data can be collected from Windows, Linux, SCOM and Azure Storage



Data Sources



- Data sources include: Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog.
- Each data source has additional configuration options.



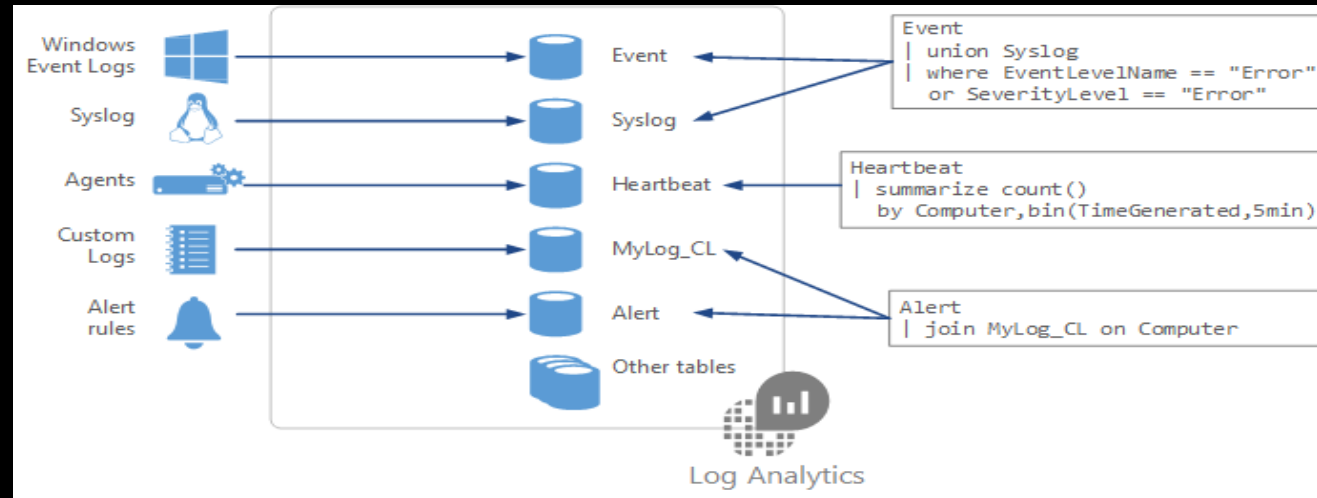
Log Analytics Querying

- Log Analytics provides a query syntax
- Quickly retrieve and consolidate data in the repository
- Save or have log searches run automatically to create an alert
- Export the data to Power BI or Excel





Query Language Syntax



Event

```
| where (EventLevelName == "Error")
| where (TimeGenerated > ago(1days))
| summarize ErrorCount = count() by Computer
| top 10 by ErrorCount desc
```



Demonstration – Log Analytics

- Access the demonstration environment
- Use the Query Explorer



Azure Administrator Associate

EXAM: AZ-104



Module 11: Monitoring

#51: Network Watcher



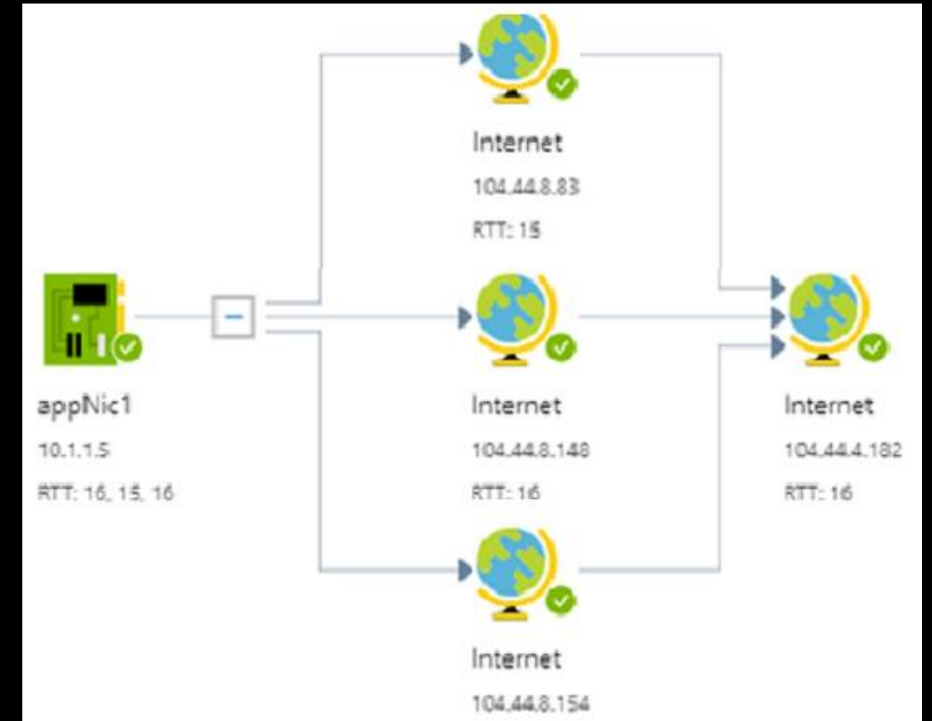
Network Watcher Overview

- Network Watcher
- Network Watcher Diagnostics
- Diagnostics – IP Flow Verify
- Diagnostics – Next Hop
- Diagnostics – Effective Security Rules
- Diagnostics – VPN Troubleshoot
- Diagnostics – Packet Capture
- Diagnostics - Connection Troubleshoot
- Logs - NSG Flow Logs
- Monitoring - Topology



Network Watcher

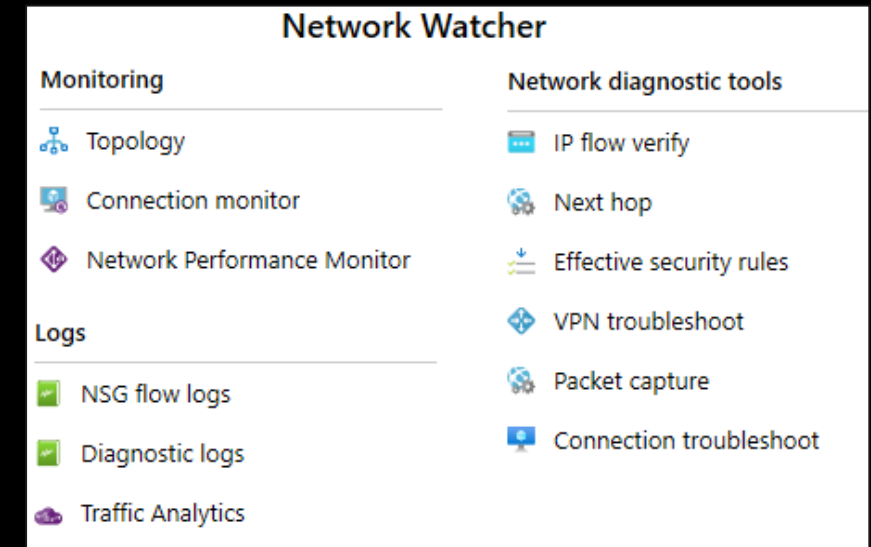
- Is a regional service
- Provides tools to monitor, diagnose, view metrics, and enable or disable logs
- Provides scenario level monitoring so you can diagnose problems at an end to end network level view
- Provides a visual representation of your networking elements





Network Watcher Diagnostics

- IP Flow Verify diagnoses connectivity issues
- Next Hop determines if traffic is being correctly routed
- VPN Diagnostics troubleshoots gateways and connections
- NSG Flow Logs maps IP traffic through a network security group
- Connection troubleshoot shows connectivity between source VM and destination
- Topology generates a visual diagram of resources





Diagnostics - IP Flow Verify

Diagnose connectivity issues from or to the internet and from or to the on-premises environment. Ideal for ensuring security rules are being correctly applied.

The screenshot shows the 'IP flow verify' tool in the Azure portal. The left sidebar lists various diagnostic tools, with 'IP flow verify' selected. The main area is divided into two sections: 'Network diagnostic tools' and 'Packet details'. The 'Packet details' section includes fields for Protocol (TCP selected), Direction (Inbound selected), Local IP address (10.1.1.4), Local port (3389), Remote IP address (13.24.35.46), and Remote port (3389). A 'Check' button is present, and the result shows 'Access denied' with a red 'X' icon. Below the result, the security rule 'DenyAllInBound' is identified.

Network diagnostic tools

- IP flow verify
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

Packet details

Protocol
 TCP UDP

Direction
 Inbound Outbound

Local IP address * ⓘ Local port * ⓘ

Remote IP address * ⓘ Remote port * ⓘ

[Check](#)

Access denied

Security rule
DenyAllInBound



Diagnostics - Next Hop

Helps with determining whether traffic is being directed to the intended destination by showing the next hop

Subscription * ⓘ
MSDN Platforms Subscription

Resource group * ⓘ
Demo

Virtual machine * ⓘ
vm01

Network interface *
vm01165

Source IP address * ⓘ
10.1.1.4

Destination IP address * ⓘ
13.24.35.46

Next hop

Result
Next hop type
None

IP address
10.1.1.100

Route table ID
/subscriptions/2301e3a0-8420-...



Diagnostics - Effective Security Rules

Details the Effective Security Rules (inbound and outbound) of the Network Interface card of a Virtual Machine.

nsg01

Inbound rules

Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access	↑↓
RDP_Inbound		100		13.23.34.45/32	0-65535		0.0.0.0/0	3389-3389		TCP		✔ Allow	
AllowVnetInBound		65000		Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All		✔ Allow	
AllowAzureLoadBalancerInBound		65001		Azure load balancer (2 prefixes)	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		✔ Allow	
DenyAllInBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		✘ Deny	

Outbound rules

Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access	↑↓
AllowVnetOutBound		65000		Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All		✔ Allow	
AllowInternetOutBound		65001		0.0.0.0/0,0.0.0.0/0	0-65535		Internet (216 prefixes)	0-65535		All		✔ Allow	
DenyAllOutBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		✘ Deny	

Diagnostics - VPN Troubleshoot



Subscription ⓘ MSDN Platforms Subscription

Resource group ⓘ Demo

Location ⓘ East US

*Storage account >

<https://samcteusvmdiagnosics.blob.core.windows.net/vpn>

	Name	↑↓	Troubleshooting s...↑↓	Resource status	↑↓	Resource Group	↑↓	Location	↑↓
<input checked="" type="checkbox"/>	✓ vng01		Running	Succeeded		Demo		East US	
<input checked="" type="checkbox"/>	cn01		-	Succeeded		Demo		East US	

- Helps you troubleshoot gateways and connections
- Provides summary information and detailed information
- Can troubleshoot multiple gateways or connections simultaneously



Diagnostics - Packet Capture

- Captures inbound and outbound traffic from a Virtual Machine
- Saves data to a storage account, a local file, or both.

Add packet capture

Subscription *
MSDN Platforms Subscription

Resource group *
Demo

Target virtual machine *
vm01

Packet capture name *
capture01 ✓

Capture configuration
The packet capture output file (.cap) can be stored in a storage account and/or on the target VM.

Storage account File Both

Storage accounts *
samcteusvmdiagnosics

Maximum bytes per packet ⓘ Maximum bytes per session ⓘ

Time limit (seconds) ⓘ

+ Add filter

Diagnostics - Connection Troubleshoot



- Check connectivity between source VM and destination
- Identify configuration issues that are impacting reachability
- Provide all possible hop by hop paths from the source to destination
- Review hop by hop latency - min, max, and average between source and destination
- View a graphical topology from your source to destination



The screenshot displays the 'Source' configuration section of the Azure Network Troubleshooter. It includes the following fields and options:







- Subscription ***: MSDN Platforms Subscription
- Resource group ***: Demo
- Source type ***: Virtual machine
- *Virtual machine**: vm01
- Destination**: Select a virtual machine, Specify manually
- URI, FQDN or IPv4 ***: 13.24.35.46
- Probe Settings**: **Protocol** TCP, ICMP
- Destination port ***: 3389
- Advanced settings**: **Source port** 3389

A blue 'Check' button is located at the bottom of the form.



Logs - NSG Flow Logs

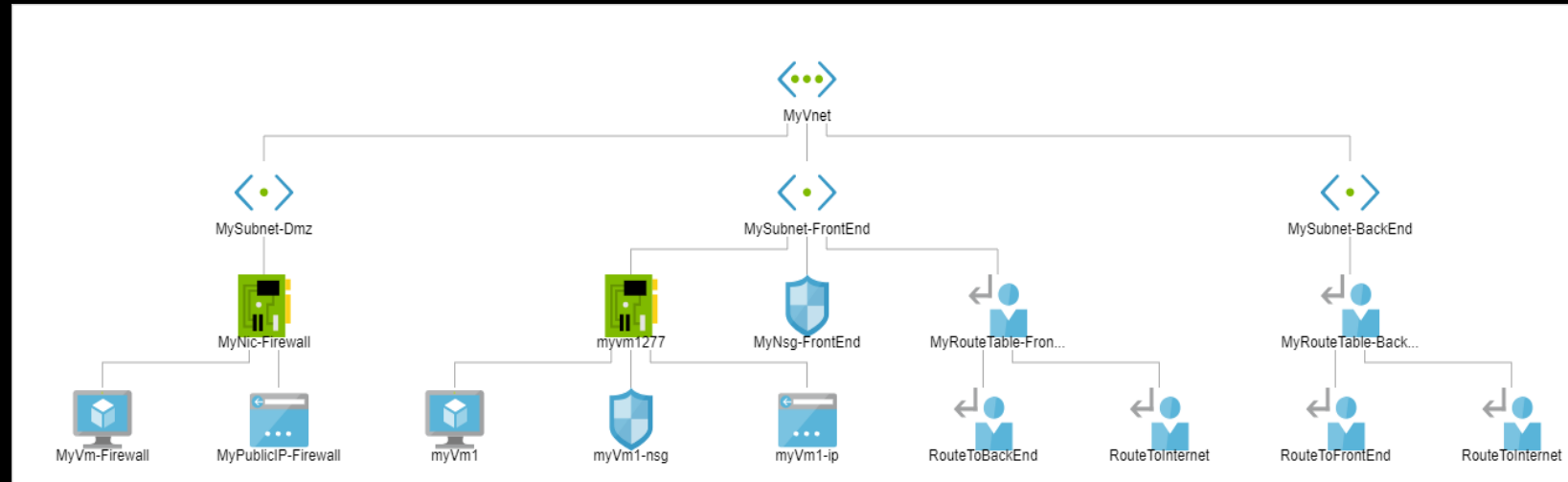
Metrics	
 Usage + quotas	
Logs	
 NSG flow logs	
 Diagnostic logs	

Name	Resource type	Resource group	Status	Location
 nsg01	Network security gro...	Demo	 Enabled	East US
 nsg02	Network security gro...	Demo	 Enabled	East US
 nsg03	Network security gro...	Demo	 Enabled	East US

- View information about ingress and egress IP traffic through an NSG
- Flow logs are written in JSON format and show outbound and inbound flows on a per rule basis
- The JSON format can be visually displayed in Power BI or third-party tools like Kibana



Monitoring - Topology



- Provides a visual representation of your networking elements
- View all the resources in a virtual network, resource to resource associations, and relationships between the resources
- The Network Watcher instance in the same region as the virtual network



Azure Administrator Associate

EXAM: AZ-104



Module 11: Monitoring

#52: Review Questions



Review Question 1

Your organization has a very large web farm with more than 100 virtual machines. You would like to use Log Analytics to ensure these machines are responding to requests. You plan to automate the process so you create a search query. You begin the query by identifying the source table. Which source table do you use? Select one

- Event
- SysLog
- Heartbeat
- MyLog_CL
- Alert



Review Question 2

Your organization has an app that is used across the business. The performance of this app is critical to day to day operations. Because the app is so important, four IT administrators have been identified to address any issues. You have configured an alert and need to ensure the administrators are notified if there is a problem. In which area of the portal will you provide the administrator email addresses? Select one.

- Activity log
- Performance group
- Signal Type
- Action Group



Review Question 3

Your organization has several Linux virtual machines. You would like to use Log Analytics to retrieve error messages for these machines. You plan to automate the process, so you create a search query. You begin the query by identifying the source table. Which source table do you use? Select one.

- Event
- SysLog
- Heartbeat
- MyLog_CL
- Alert



Review Question 4

You are analyzing the company virtual network and think it would helpful to get a visual representation of the networking elements. Which feature can you use? Select one.

- Network Watcher Auditing
- Network Watcher Connection Troubleshoot
- Network Watcher Flows
- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology



Review Question 5

Your company has a website and users are reporting connectivity errors and timeouts. You suspect that a security rule may be blocking traffic to or from one of the virtual machines. You need to quickly troubleshoot the problem, so you do which of the following? Select one.

- Configure IIS logging and review the connection errors.
- Turn on virtual machine diagnostic logging and use Log Analytics.
- Use Network Watcher's VPN Diagnostics feature.
- Use Network Watcher's IP Flow Verify feature.
- Configure Windows performance counters and use Performance Monitor.



Review Question 6

You are interested in finding a single tool to help identify high VM CPU utilization, DNS resolution failures, firewall rules that are blocking traffic, and misconfigured routes. Which tool can you use? Select one.

- Network Watcher Auditing
- Network Watcher Connection Troubleshoot
- Network Watcher Flows
- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology



Review Question 7

You are reviewing the Alerts page and notice an alert has been Acknowledged. What does this mean? Select one.

- The issue has just been detected and has not yet been reviewed.
- An administrator has reviewed the alert and started working on it.
- The issue has been resolved.
- The issue has been closed.



Review Question 8

You need to determine who deleted a network security group through Resource Manager. You are viewing the Activity Log when another Azure Administrator says you should use this event category to narrow your search. Select one.

- Administrative
- Service Health
- Alert
- Recommendation
- Policy



THANK YOU