



# Introduction to Azure AD

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Active Directory (**Azure AD**) is Microsoft's cloud-based **identity and access management service**, which helps your employees sign in and access resources

## External Resources

- Microsoft Office 365
- Azure Portal
- SaaS applications

## Internal Resources

- Applications within your internal networking
- Access to workstations on-premise

Use Azure AD to implement **Single-Sign On (SSO)**

Azure Active Directory comes in four editions

1. **Free** MFA, SSO, Basic Security and Usage Reports, User Management
2. **Office 365 Apps** Company Branding, SLA, Two-Sync between On-Premise and Cloud
3. **Premium 1** Hybrid Architecture, Advanced Group Access, Conditional Access
4. **Premium 2** Identity Protection, Identity Governance



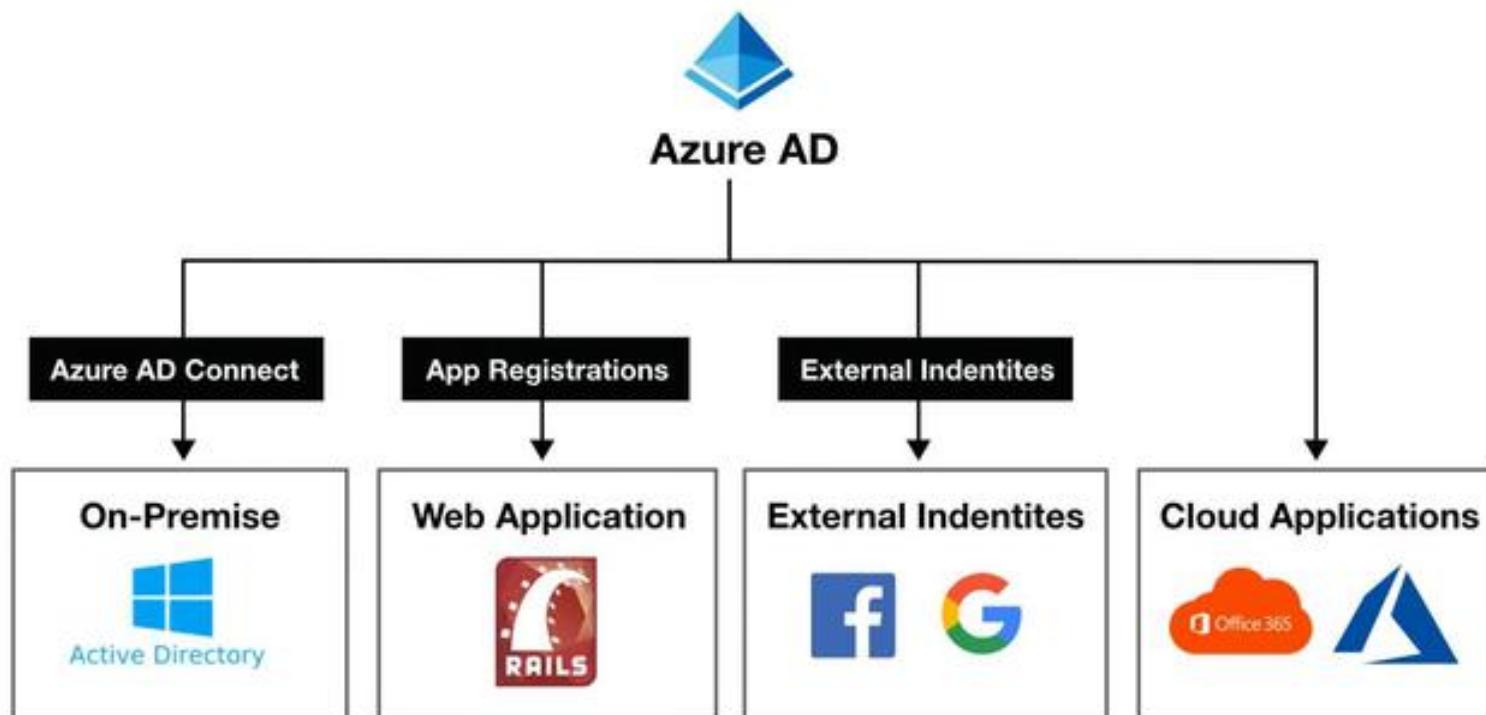


# Azure AD – Use Case

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure AD can **authorize** and **authenticate** to multiple sources.

- To your on-premise AD
- To your web-application
- Allow users to login with their IdP eg. Facebook or Google
- To Office 365 or **Azure Microsoft**





# Active Directory vs Azure Active Directory

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)



Microsoft introduced **Active Directory** Domain Services in **Windows 2000** to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.

Azure AD takes this approach to the next level by providing organizations with an **Identity as a Service (IDaaS)** solution for all their apps **across cloud and on-premises**.

Both versions are still used today



**Active Directory**

The **on-premise** version



**Azure AD**

The **cloud** version



# Active Directory Terminology

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Domain

A domain is an area of a network organized by a single authentication database

An Active Directory domain is a **logical grouping** of AD objects on a network

## Domain Controller (DC)

A domain controller is a server that **authenticates** user identities and **authorizes** their access to resources.

## Domain Computer

A computer that is registered with a central authentication database A domain computer would be an AD Object

## AD Object

An AD Object is the basic element of Active Directory such as:

Users, Groups, Printers, Computers, Shared folders

## Group Policy Object (GPO)

A virtual collection of policy settings. It controls what AD Objects have access to

## Organization Units (OU)

A subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units

## Directory Service

A directory service, such as **Active Directory Domain Services (AD DS)**, provides the methods for storing directory data and making this data available to network users and administrators. A Directory service runs on a Domain Controller





# Azure AD – Tenant

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**A tenant represents an organization** in Azure Active Directory.

A tenant is a dedicated Azure AD Service instance.

A tenant is automatically created when you sign up for either

- Microsoft Azure
- Microsoft Intune
- Microsoft 365

Each Azure AD tenant is distinct and separate from other Azure AD tenants.



 **Tenant information**

Your role	Global administrator <a href="#">More info</a>
License	Azure AD for Office 365
Tenant ID	f73244ae-3e74-43eb-8dbf-c66e... 
Primary domain	exampro.onmicrosoft.com



# Azure Active Directory Domain Services (AD DS)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

In some cases you'll need to setup your own domain controller(s).

When doing a *lift-and-shift from on-premise* to Microsoft Azure and migrating Active Directory, Azure AD does not support some **domain services**.

Azure Active Directory Domain Services (AD DS) provides **managed domain service** such as:

- Domain joins
- Group policies
- Lightweight directory access protocol (LDAP)
- and Kerberos / NTLM authentication.

You can use these domain services without the need to:  
**deploy, manage, and patch domain controllers (DCs) in the cloud**





# Azure AD Connect

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure AD Connect is a **hybrid service** to **connect your on-premise Active Directory to your Azure Account**

Azure AD Connect allows for seamless **Single Sign On** from your on-premise workstation to Microsoft Azure

Azure AD Connect has the following features:

- **Password hash synchronization** — sign-in method, synchronizes a hash of a users on-premises AD password with Azure AD
- **Pass-through authentication** — sign-in method, allows users to use the same password on-premises and in the cloud
- **Federation integration** — hybrid environment using an on-premises AD FS infrastructure, for certificate renewal
- **Synchronization** — Responsible for creating users, groups, and other objects, ensures on-prem and cloud data matches
- **Health Monitoring** — robust monitoring and provide a central location in the Azure portal to view this activity



Azure AD Connect Health  






# Active Directory – Users

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Users represent an **identity for a person or employee** in your domain.  
A user has login credentials and can use them to log into the Azure Portal

- You can assign roles and **administrative roles** to users
- You can add users to groups
- You can enforce authentication methods such as (MFA) Multi-Factor Authentication
- You can track users sign ins
- Track devices user's login from and allow or deny devices.
- Assign Microsoft licenses



Azure AD has two kinds of users:

- **Users** — A user belongs to your organization
- **Guest Users** — A guest user belongs to another organization

*We'll cover Azure AD roles in the roles section of course.*





# Azure AD - Groups

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

**Groups** lets the resource owner (or Azure AD directory owner), assign a set of access permissions to all the members of the group, instead of having to provide the rights one-by-one.

## Groups contain:

- **Owners** — Has permissions to add and remove members
- **Members** — Have permissions to do things

## Assignment

- You can assign roles directly to a group
- You can assign applications directly to a group

The screenshot shows the Azure AD Groups management interface. On the left, there's a sidebar with options: 'Diagnose and solve problems', 'Manage' (selected), 'Profile', 'Assigned roles', 'Administrative units', 'Groups' (highlighted in blue), 'Applications', 'Licenses', 'Devices', 'Azure role assignments', and 'Authentication methods'. At the top right, there are buttons for 'Add memberships', 'Remove memberships', and 'Refresh'. Below the sidebar is a message: 'This page includes previews available for your evaluation. View preview'. The main area displays a table of groups:

Name	Object Id
am Exampro Team	517dd36c-323b-4145-1b...
Section 31	10485f20-01d6-1f34-91a...
All Company	58a630d9-9bdc-48c3-ab...
ExamPro Creative	15adb941-c1c1-d732-bf...
ExamPro Workshop Master	6b2eea2b-5a1b-4bc7-a2...
Collaboration Team	2e22a5a7-fd27-1936-9b...
Sales	b0c187d4-b2b4-4e93-9c...

## Request to Join Groups

The group owner can let users find their own groups to join, instead of assigning them. The owner can also set up the group to automatically accept all users that join or to require approval.





# Azure AD – Assign Access Rights

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are **four ways to assign resource access rights** to your users:

**Direct assignment.** The resource owner directly assigns the user to the resource.

**Group assignment.** The resource owner assigns an Azure AD group to the resource, which automatically gives all of the group members access to the resource

**Rule-based assignment.** The resource owner creates a group and uses a rule to define which users are assigned to a specific resource.

**External authority assignment.** Access comes from an external source, such as an on-premises directory or a SaaS app.



# Azure AD – External Identities

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**External Identities** in Azure AD, allow people outside your organization to access your apps and resources, while letting them sign in using whatever identity they prefer.

Your partners, distributors, suppliers, vendors, and other guest users can "bring their own identities".

Supports Logins from **Google** and **Facebook**



- Share apps with external users (B2B collaboration).
- Develop apps intended for other Azure AD tenants (single-tenant or multi-tenant)
- Develop white-labeled apps for consumers and customers (Azure AD B2C)



# Azure Administrator

Azure Active Directory



## Create a tenant



Follow Along

Create a tenant - Microsoft Azure

portal.azure.com/#blade/Microsoft\_AAD\_IAM/ActiveDirectoryMenuBlade/CreateTenant

Microsoft Azure

Search resources, services, and more

Home > Husnock >

### Create a tenant

Azure Active Directory

\* Basics   Configuration   Review + create

Azure Active Directory and Azure Active Directory (B2C) enable users to...

Tenant type

! You must have a subscription in order to create an Azure Active Directory tenant.

Select a tenant type \*

Azure Active Directory

Azure Active Directory (B2C)

Help me choose...

SUBSCRIBE



# Azure Administrator

Azure Active Directory



## Upgrade Licenses



### Follow Along

The screenshot shows a Microsoft Edge browser window with the URL [activationservice.microsoft.com](https://www.microsoft.com/en-us/activationservice/). The page title is "Activate". A progress bar at the top indicates "Activating Azure AD Premium P2 trial" and "Activating Azure AD Premium P2 trial" with a progress of "3.08 / 3". Below the progress bar, there is a note: "If you would like to purchase a subscription directly from Microsoft, please see the Purchase service catalog." A "Free trial" button is visible. The main content area is titled "ENTERPRISE MOBILITY + SECURITY E3". It describes E3 as a comprehensive cloud solution for IT, BYOD, and SaaS challenges, mentioning Azure Active Directory Premium P2 and its features like Microsoft Intune and Azure Rights Management. Another "Free trial" button is shown. At the bottom, it says "Azure Active Directory Premium P2 enhances your directory with additional features that include multi-factor authentication, policy driven management and end-user self-service. Learn more about features". It also notes that the trial includes 100 licenses and will be active for 30 days. A "SUBSCRIBE" button with a Microsoft logo is at the bottom right.



# Azure Administrator

Azure Active Directory



## User and Groups



Follow Along

Microsoft Azure

Home > Starfleet > Users >

New user

Starfleet

Get feedback?

Last name:

Groups and roles

Groups: 0 groups selected

Roles: User

Settings

Block sign in: No

Usage location:

Job info

Job title:

Department:

Company name:

(A) SUBSCRIBE



# Azure Administrator

Azure Active Directory



## Guest Users



Follow Along

Microsoft Azure | Search resources, services, and docs (24)

Home > Husnock > Users > New user

Husnock

Get feedback?

Create user

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

I want to create users in bulk

Help me decide

Identity

User name \*

husnok

The domain name I need is

Name \*

Example: 'Chris Green'

First name

Last name

Done

(A) SUBSCRIBE

This screenshot shows the Microsoft Azure portal interface for creating a new user. The 'Create user' option is selected. The 'Identity' section includes fields for 'User name' (set to 'husnok'), 'Name' (example value 'Chris Green'), 'First name', and 'Last name'. At the bottom right, there are 'Done' and '(A) SUBSCRIBE' buttons.



# Azure Administrator

Azure Active Directory



## Mass Import



Follow Along

Microsoft Azure

Home > Starfleet >

Users | All users (Preview)

Starfleet - Azure Active Directory

All users (Preview)

New user New guest

This page includes preview features

UserCreateTemplate

version	name	display name	user principal name	initial password	sign-in status
v1.0	Chris Green	Chris Green	chris@contoso.com	myPassword1234	No
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

(A) SUBSCRIBE



# Azure Administrator

Azure Active Directory



## Multi-Factor Authentication



Follow Along

Microsoft Azure

Home > Starfleet > Password reset

Starfleet - Azure Active Directory

Save Discard

Diagnose and solve problems

Manage

- Properties
- Authentication methods
- Registration
- Notifications
- Customization
- On-premises integration

Select group

No groups selected

These settings only apply to end users and are required to use two-factor authentication policies.

(A) SUBSCRIBE



# Azure Administrator

Azure Active Directory



## Self-Service Rest Password



Follow Along

Microsoft Azure

Home > Starfleet > Password reset

### Password reset | Properties

Starfleet - Azure Active Directory

Save Discard

Self service password reset enabled: Selected

Select group: No groups selected

These settings only apply to end users and are required to use two-factor authentication policies.

Diagnose and solve problems

Manage

- Properties
- Authentication methods
- Registration
- Notifications
- Customization
- On-premises integration

Activity

- Audit logs
- Usage & insights

Troubleshooting + Support

- New support request

(A) SEARCH



# Azure Administrator

Azure Active Directory



## Azure Active Directory CheatSheet



# Azure Active Directory *CheatSheet*

Exam

Pro

Active Directory (AD) is Microsoft's **identity and access management service**. Helps your employees sign in and access resources.

Azure Active Directory (Azure AD) is Microsoft's cloud-based version of AD **Identity as a Service (IDaaS)**

Azure Active Directory comes in **4 editions**:

1. Free MFA, SSO, Basic Security and Usage Reports, User Management
2. Office 365 Apps Company Branding, SLA, Two-Sync between On-Premise and Cloud
3. Premium 1 (P1) Hybrid Architecture, Advanced Group Access, **Conditional Access**
4. Premium 2 (P2) Identity Protection, Identity Governance

Azure AD can **authorize** and **authenticate** to multiple sources.

- To your on-premise AD via **Azure AD Connect**
- To your web-application via **App Registrations**
- Allow users to login with their IPD eg. Facebook or Google via **External Identities**
- To Office 365 or **Azure Microsoft**

Active Directory Terminology:

- **Domain** A domain is an area of a network organized by a single authentication database
- **An Active Directory domain** is a **logical grouping** of AD objects on a network
- **Domain Controller (DC)** A domain controller is a server that **authenticates** user identities and **authorizes** their access to resources.
- **Domain Computer** A computer that is registered with a central authentication database. A domain computer would be an AD Object
- **AD Object** An AD Object is the basic element of Active Directory such as: Users, Groups, Printers, Computers, Shared folders
- **Group Policy Object (GPO)** A virtual collection of policy settings. It controls what AD Objects have access to
- **Organization Units (OU)** A subdivision within an AD into which you can place users, groups, computers, and other organizational units
- **Directory Service** A directory service, such as **Active Directory Domain Services (AD DS)**, provides the methods for storing directory data and making this data available to network users and administrators. A Directory service runs on a Domain Controller



# Azure Active Directory *CheatSheet*

Exam

Pro

A tenant represents an organization in Azure Active Directory. A tenant is a dedicated Azure AD Service instance. A tenant is automatically created when you sign up for either: Microsoft Azure, Microsoft Intune, Microsoft 365.

Each Azure AD tenant is distinct and separate from other Azure AD tenants.

When performing a lift-and-shift of AD to Azure, not all AD features are supported and in that case you need to use AD DS

**Azure Active Directory Domain Services (AD DS)** provides managed domain services (features) such as:

- Domain joins, Group policies, Lightweight directory access protocol (LDAP), and Kerberos / NTLM authentication.

Azure AD Connect has the following features:

- **Password hash synchronization** — sign-in method, synchronizes a hash of a user's on-premises AD password with Azure AD
- **Pass-through authentication** — sign-in method, allows users to use the same password on-premises and in the cloud
- **Federation integration** — hybrid environment using an on-premises AD FS infrastructure, for certificate renewal
- **Synchronization** — Responsible for creating users, groups, and other objects, ensures on-prem and cloud data matches
- **Health Monitoring** — robust monitoring and provide a central location in the Azure portal to view this activity

Users represent an identity for a person or employee in your domain. A user has login credentials and can use them to log into the Azure Portal. Azure AD has two kinds of users:

- **Users** — A user belongs to your organization
- **Guest Users** — A guest user belongs to another organization

Groups lets the resource owner (or Azure AD directory owner), assign a set of access permissions to all the members of the group, instead of having to provide the rights one-by-one. **Groups contain:**

- **Owners** — Has permissions to add and remove members
- **Members** — Have permissions to do things

## Assignment

- You can assign roles directly to a group
- You can assign applications directly to a group



# Azure Active Directory *CheatSheet*



**Request to Join Groups** The group owner can let users find their own groups to join, instead of assigning them. The owner can also set up the group to automatically accept all users that join or to require approval.

There are four ways to **assign resource access rights** to your users:

- **Direct assignment.** The resource owner directly assigns the user to the resource.
- **Group assignment.** The resource owner assigns an Azure AD group to the resource, which automatically gives all of the group members access to the resource
- **Rule-based assignment.** The resource owner creates a group and uses a rule to define which users are assigned to a specific resource.
- **External authority assignment.** Access comes from an external source, such as an on-premises directory or a SaaS app.



# Azure Administrator

Device Management

## Introduction to Device Management



# Azure AD - Device Management

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is Device identity management?

The management of **physical devices** such as **phones, tablets, laptops and desktop** computers, that are granted access to company resources such as Printers, Cloud Resources via **device-based Conditional Access**.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Complia...	Registered	Activity
<input type="checkbox"/>  DESKTOP-J1KCQ...	 Yes	Windows	10.0.18362.0	Azure AD registered	Miles O'Brien	None	N/A	2020-07-12, 10:05:4...	2021-03-22, 9:
<input type="checkbox"/>  DESKTOP-00B6Q...	 Yes	Windows	10.0.19042.867	Azure AD registered	Sonya Gomez	None	N/A	2020-08-24, 4:43:28 ...	2021-03-13, 7:
<input type="checkbox"/>  LAPTOP-HIELPOBE	 No	Windows	10.0.19041.388	Azure AD registered	Reginald Barclay	None	N/A	2020-08-07, 2:57:31 ...	2020-09-19, 7:
<input type="checkbox"/>  DESKTOP-P9TM...	 Yes	Windows	10.0.19041.867	Azure AD registered	Alyssa Ogawa	None	N/A	2021-03-31, 8:00:10 ...	2021-03-31, 8:

For companies with a distributed workforce, that allows remote employees and employees who Are allowed you use their own personal equipment eg. **Bring Your Own Device (BYOD)**.

A company needs a way to protect their organization's assets such as access to cloud resources across these devices where they have less control over the physical securities of the work environment



# Azure AD - Device Management

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are **3 ways** to get devices into Azure AD

## 1. Azure AD Registered

- personally owned or mobile devices,
- And signed in with a personal Microsoft or local account

- Windows 10
- iOS
- Android
- MacOS

## 2. Azure AD Joined

- owned by an organization
- And signed in with an Azure AD account belonging to the organization.
- They exist **only in the cloud**.

- Windows 10
- Windows Server 2019 VMs running in Azure  
(Server core is not supported)

## 3. Hybrid Azure AD Joined

- owned by an organization
- And are signed in with an Active Directory Domain Services account belonging to that organization
- They exist **in the cloud and on-premises**

- Windows 7, 8.1, or 10
- Windows Server 2008 or newer





# Azure Administrator

Device Management

## AD Registered Devices

(A)  
SUBSCRIBE

# Azure AD Registered Devices

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Definition** Registered to Azure AD without requiring organizational account to sign in to the device

**Primary audience** Bring your own device (BYOD), Mobile devices

**Device ownership** User or Organization

**Operating Systems** Windows 10, iOS, Android, and MacOS

## Provisioning

- Windows 10 – Settings
- iOS/Android – Company Portal or Microsoft Authenticator app
- MacOS – Company Portal

## Device sign in options

- End-user local credentials, Password, **Windows Hello**, PIN
- Biometrics or Pattern for other devices

## Device management

- **Mobile Device Management** (example: **Microsoft Intune**)
- **Mobile Application Management**

## Key capabilities

- **SSO** to cloud resources
- Conditional Access when **Enrolled into Intune**
- Conditional Access via **App protection policy**
- Enables Phone sign in with **Microsoft Authenticator app**





# Azure Administrator

Device Management

## Windows Hello

(A)  
SUBSCRIBE

# Azure AD Registered Devices – Windows Hello

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)



## Windows Hello

Gives Windows 10 users **an alternative way** to log into their devices and applications using:

- fingerprint
- iris scan
- facial recognition



# Azure Administrator

Device Management

## Mobile Device Management and Mobile Application Management



# Azure AD Registered Devices – MDM and MAM

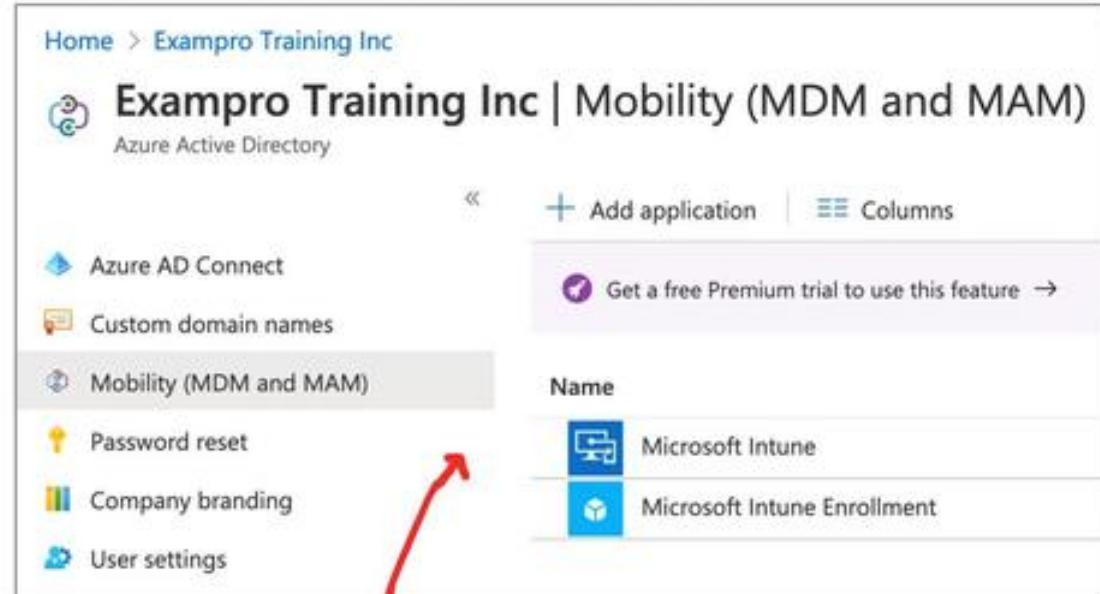
Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Mobile Device Management (MDM)

control the entire device, can wipe data from it, and also reset it to factory settings

## Mobile Application Management (MAM)

Publish, push, configure, secure, monitor, and update mobile apps for your users



The screenshot shows the Azure Active Directory portal with the navigation bar "Home > Exampro Training Inc". Under "Azure Active Directory", there is a list of applications: "Azure AD Connect", "Custom domain names", "Mobility (MDM and MAM)" (which is highlighted with a gray box and has a red arrow pointing to it), "Password reset", "Company branding", and "User settings". To the right, there is a table with two rows: "Name" (Microsoft Intune) and "Microsoft Intune Enrollment". A purple button "Get a free Premium trial to use this feature" is also visible.

MDM and MAM is founder under Azure AD

MDM and MAM is managed via **Microsoft Intune**

To use Microsoft Intune you have to upgrade to **Azure AD Premium 2**

Microsoft Intune is part of **Microsoft Endpoint Manager**

Microsoft Endpoint Manager and Intune are part of **Microsoft Enterprise Mobility + Security (EMS)**

**Intune = Endpoint Manager = EMS** Yes, I am confused too by all these names...





# Azure Administrator

Device Management

## Enterprise Mobility + Security



# Azure AD Registered Devices – EMS

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Microsoft Enterprise Mobility + Security (EMS)** is an intelligent mobility management and security platform. Protect and secure your organization and empowers your employees to work in new and flexible ways.



*EMS is an **umbrella** of multiple Microsoft and Azure services*

## Azure Active Directory

The most trusted identity and access management solution in the market that helps you safeguard user credentials and connect people securely to the apps they need.

[Learn more >](#)

## Microsoft Endpoint Configuration Manager

Systems management software for managing on-premises PCs, servers, and mobile devices with cloud-powered insights.

[Learn more >](#)

## Microsoft Intune

Cloud-based unified endpoint management, access management, and data protection.

[Learn more >](#)

## Azure Information Protection

Cloud-based data classification, tracking, protection, and encryption.

[Learn more >](#)

## Microsoft Cloud App Security

Cloud access security broker with discovery, behavioral analytics, risk assessment, data protection, and threat protection.

[Learn more >](#)

## Microsoft Advanced Threat Analytics

On-premises platform that protects against advanced targeted cyberattacks and insider threats.

[Learn more >](#)

## Microsoft Defender for Identity

Cloud-based solution that helps protect your organization's identities from multiple types of advanced targeted cyberattacks.

[Learn more >](#)

## Microsoft Secure Score

Intelligent insights and guidance that help maximize your security posture with Microsoft 365 and Azure.

[Learn more >](#)





# Azure Administrator

Device Management

## Microsoft Authenticator App

(A)  
SUBSCRIBE

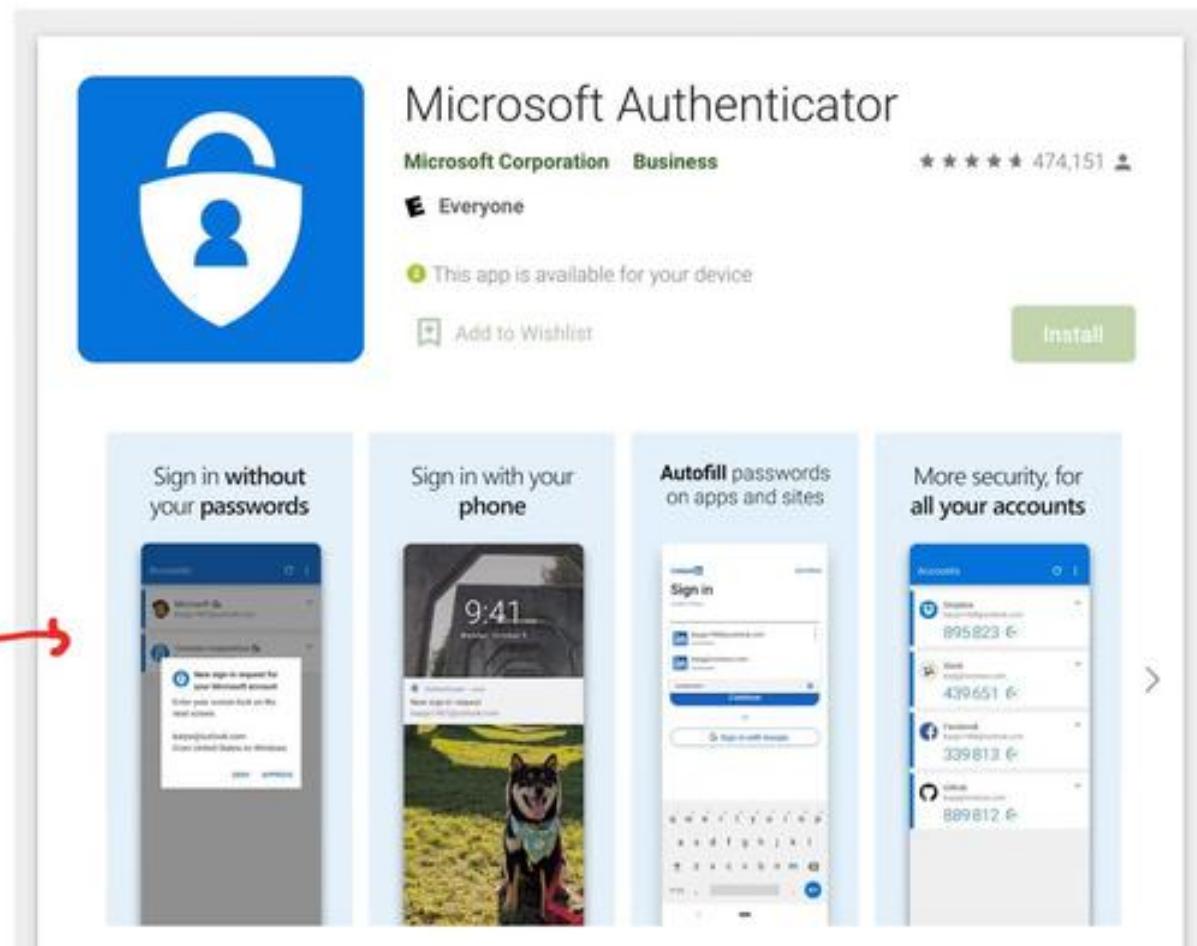
# Azure AD Registered Devices – Microsoft Authenticator

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**secure sign-ins** for all your online accounts using:

- multi-factor authentication
- Passwordless
- password autofill

You can download from the **Apple App Store or Google Play**



The image shows the Microsoft Authenticator app page on the Google Play Store. The app icon is a blue shield with a white padlock and a person icon. The title is "Microsoft Authenticator". Below it, the developer is listed as "Microsoft Corporation" and the category is "Business". It has a rating of 4.5 stars and 474,151 reviews. The app is labeled as "Everyone". A green "Install" button is visible. Below the main info, there are four screenshots showing features: "Sign in without your passwords", "Sign in with your phone", "Autofill passwords on apps and sites", and "More security for all your accounts". A red arrow points from the Google Play logo towards the screenshots.



# Azure Administrator

Device Management

## AD Joined Devices

(A)  
SUBSCRIBE

# Azure AD Joined Devices

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Definition** Joined only to Azure AD requiring organizational account to sign-in to the device

**Primary audience**

- Suitable for both cloud-only and hybrid organizations.
- Applicable to all users in an organization

**Device ownership** Organization

**Operating Systems**

- All Windows 10 devices **except Windows 10 Home**
- Windows Server 2019 Virtual Machines running in Azure (Server core is not supported)

**Provisioning**

- Self-service: Windows OOBЕ or Settings, Bulk enrollment, Windows Autopilot

**Device sign in options**

- Organizational accounts using: Password, Windows Hello for Business, **FIDO2.0 security keys** (preview)

**Device management**

- Mobile Device Management (Microsoft Intune)
- Co-management with Microsoft Intune and Microsoft Endpoint Configuration Manager

**Key capabilities**

- SSO to both cloud and on-premises resources
- Conditional Access through MDM enrollment and MDM compliance evaluation
- Self-service Password Reset and Windows Hello PIN reset on lock screen
- Enterprise State Roaming across devices





# Azure Administrator

Device Management

## FIDO2 and Security Keys



# Azure AD Joined Devices – FIDO2.0 Security Keys

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)



## Fast Identity Online (FIDO) Alliance

An open industry association whose mission is to **develop and promote authentication standards** that **help reduce the world's over-reliance on passwords**

FIDO Alliance has published three sets of **open specifications** for simpler, stronger user authentication:

- FIDO Universal Second Factor (FIDO U2F)
- FIDO Universal Authentication Framework (FIDO UAF)
- Client to Authenticator Protocols (CTAP)
- CTAP is complementary to the W3C's Web Authentication (WebAuthn) specification; together, they are known as **FIDO2**



# Azure AD Joined Devices – FIDO2.0 Security Keys

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a Security Key?

A secondary device used as second step in authentication process to gain access to a device, workstation or application.

A security key can resemble a memory stick. When your finger makes contact with a button or exposed metal on the device it will generate And autofill a security token.

A popular brand of security key is an Yubikey



- Works out of the box with Gmail, Facebook, and hundreds more
- Supports **FIDO2**/WebAuthn, U2F
- Waterproof and crush resistant
- USB-A and NFC dual connectors on a single key





# Azure Administrator

Device Management

## Hybrid Azure AD Joined Devices

# Hybrid Azure AD joined devices

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Definition** Joined to on-premises AD and Azure AD requiring organizational account to sign in to the device

**Primary audience** Suitable for hybrid organizations with existing on-premises AD infrastructure  
Applicable to all users in an organization

**Device ownership** Organization

## Operating Systems

- Windows 10, 8.1 and 7, Windows Server 2008/R2, 2012/R2, 2016 and 2019

## Provisioning

- Windows 10, Windows Server 2016/2019
- Domain join by IT and autojoin via Azure AD Connect or ADFS config
- Domain join by **Windows Autopilot** and autojoin via Azure AD Connect or ADFS config
- Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 - Require MSI

**Device sign in options** Organizational accounts using:

- Password
- Windows Hello for Business for Win10

## Device management

- Group Policy, Configuration Manager standalone or co-management with Microsoft Intune

## Key capabilities

- SSO to both cloud and on-premises resources
- Conditional Access through Domain join or through Intune if co-managed
- Self-service Password Reset and Windows Hello PIN reset on lock screen
- Enterprise State Roaming across devices





# Azure Administrator

Device Management

## Windows Autopilot

# Hybrid Azure AD joined devices – Windows Autopilot

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Windows Autopilot** is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use.

When initially deploying new Windows devices

- Windows Autopilot uses the OEM-optimized version of Windows 10.
- This version is preinstalled on the device, so you don't have to maintain custom images and drivers for every device model
- Instead of re-imaging the device, your existing Windows 10 installation can be transformed into a “business-ready” state that can

Once deployed, you can manage Windows 10 devices with:

- Microsoft Intune
- Windows Update for Business
- Microsoft Endpoint Configuration Manager
- other similar tools





# Azure Administrator

Device Management



## Device Management Cheatsheet

(A)  
SUBSCRIBE

# Device Management *CheatSheet*



Device Management allows organization to manage laptops, desktops and phones that need access to cloud resources.

Device management is found under **Azure Active Directory (Azure AD)**

There are 3 ways to join types in (bring devices into) Device Management:

- Azure Registered
  - **personally** owned devices or mobile devices
  - Signed in with a local or personal account
  - Windows 10, iOS, Android and MacOS
- Azure AD Joined
  - Devices owned by the organization
  - Signed in with an organizational account
  - Access to devices that exist in **only in the cloud** (**Cloud Native**)
    - Windows 10, Windows Server 2019
- Hybrid Azure AD Joined
  - Devices owned by the organization
  - Signed in with Active Directory Domain Services account owned by organization
  - Devices that exist in the cloud or **on-premise**
  - Windows 7,8,1,10, Windows Server 2008 or newer

## Mobile Device Management (MDM)

- control the entire device, can wipe data from it, and also reset it to factory settings

## Mobile Application Management (MAM)

- Publish, push, configure, secure, monitor, and update mobile apps for your users





# Azure Administrator

Azure Roles

## Type of Roles in Azure

# Types of Azure roles

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Roles can be confusing because Azure has **three types of roles** that can serve same purpose

## 1. Classic subscription administrator roles

This is the original role system.

## 2. Azure roles

This is an authorization system known as Role-Based Access Controls (RBAC) and is built on top of Azure Resource Manager

## 3. Azure Active Directory (Azure AD) roles

Azure AD roles are used to manage Azure AD resources in a directory





# Azure Administrator

Azure Roles

## IAM Access Controls





# Access Controls (IAM)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Identity Access Management (IAM)** allows you to create and assign roles to users

## Azure Roles (RBAC system)

Roles restrict access to resource actions (also known as operations). There are two types of roles:

1. **BuiltInRole** – Managed Microsoft roles are read only pre-created roles for you to use
2. **CustomRole** – A role created by you with your own custom logic

## Role Assignment

Is when you apply a role to a

- service principle
- (user) group
- user

## Deny Assignments

block users from performing specific actions even if a role assignment grants them access. The only way to apply Deny assignments is through **Azure BluePrints**

Name	Type	Users	Groups	Service Principals	...
Owner	BuiltInRole	1	0	0	...
Contributor	BuiltInRole	0	0	0	...
Reader	BuiltInRole	0	0	0	...
AcrDelete	BuiltInRole	0	0	0	...
AcrlImageSigner	BuiltInRole	0	0	0	...
AcrPull	BuiltInRole	0	0	0	...



# Azure Administrator

Azure Roles

## Classic Administrator

(A)  
SUBSCRIBE



# Azure Administrator

Azure Roles

## Classic Administrator

(A)  
SUBSCRIBE



# Classic Administrators

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Classic Administrators is the **original role system**. You should use the new RBAC system when possible



+ Add    Download role assignments    Edit columns    Refresh    ...

Roles    Deny assignments    Classic administrators    ...

Classic administrators are only needed if you are still using Azure classic deployments. We recommend using role assignments for all other purposes. [Learn more](#)

Name	Role
<input type="checkbox"/> Name	↑↓
<input type="checkbox"/> Andrew Bayko bayko@exampro.co	Service administrator

Classic Administrators have three types of roles:

1. **Account Administrator** The billing owner of the subscription. Has no access to the Azure portal.
2. **Service Administrator** same access of a user assigned the Owner role at subscription scope. Full access to the Azure portal.
3. **Co-Administrator** same access of a user who is assigned the Owner role at the subscription scope





# Azure Administrator

Azure Roles

## Role-based Access Control

# Azure Role-Based Access Control (RBAC)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure role-based access control (Azure RBAC) helps you manage **who has access to Azure resources**, what they can do with those resources, and what areas they have access to.

**Role Assignments** the way you control access to resources

A Role Assignment consists of these **three** elements

1. security principal
2. role definition
3. scope

There are **four fundamental** Azure roles

Azure RBAC includes over **70 built-in roles**



# Azure Role-Based Access Control (RBAC)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**A Security Principal** represents the identities requesting access to an Azure resource such as:

**User** An individual who has a profile in Azure Active Directory

**Group** A set of users created in Azure Active Directory.

**Service Principal** A security identity used by applications or services to access specific Azure resources.

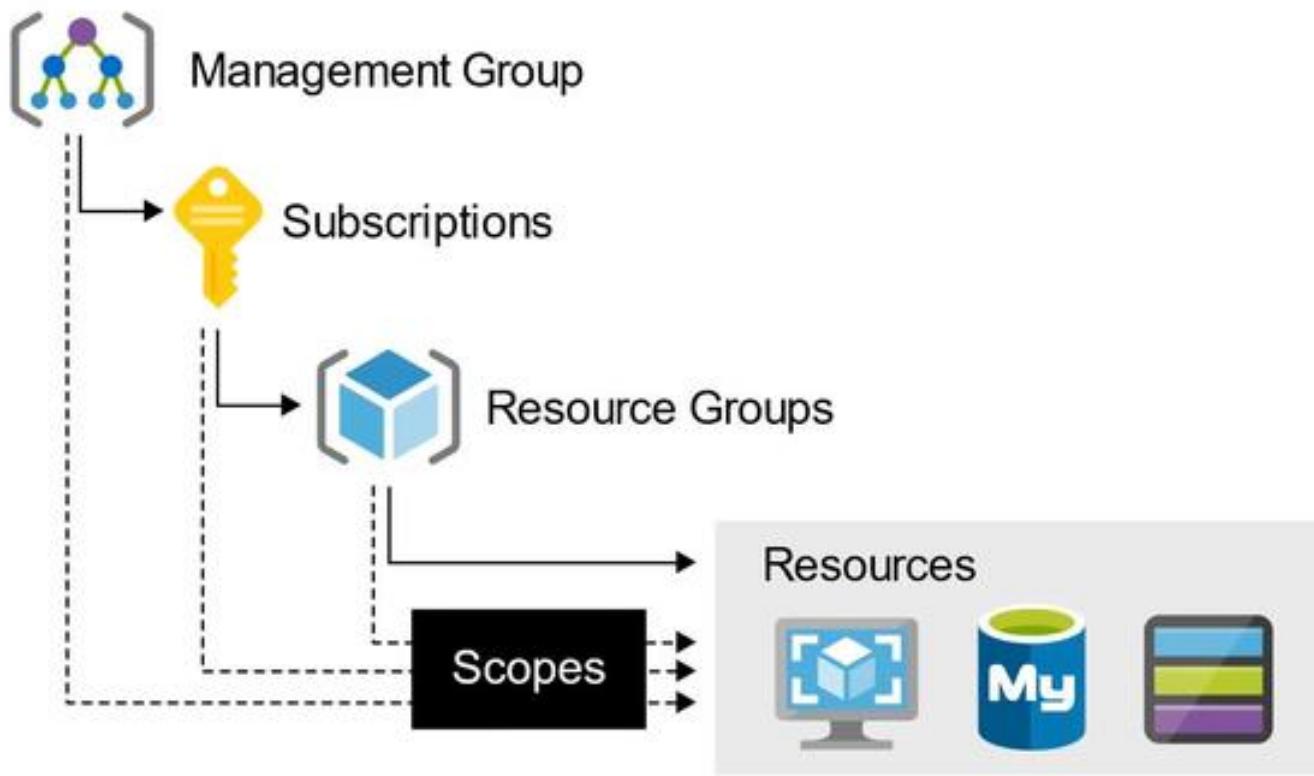
**Managed identity** An identity in Azure Active Directory that is automatically managed by Azure.



# Azure Role-Based Access Control (RBAC)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Scope** is the **set of resources** that access for the Role Assignment applies to.  
Scope Access Controls at the Management, Subscription or Resource Group level.



# Azure Role-Based Access Control (RBAC)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**A Role Definition** is a collection of permissions.

A role definition lists the operations that can be performed, such as **read, write, and delete**.

Roles can be high-level, like owner, or specific, like virtual machine reader.

Azure has **built-in roles** and you can define **custom roles**



	Read	Grant	Create, Update, Delete
Owner			
Contributor			
Reader			
User Access Administrator			

These are the four fundamental built-in role





# Azure Administrator

Azure Roles

## Azure AD Roles



# Azure AD Roles

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure AD roles are used to **manage Azure AD resources** in a directory such as:

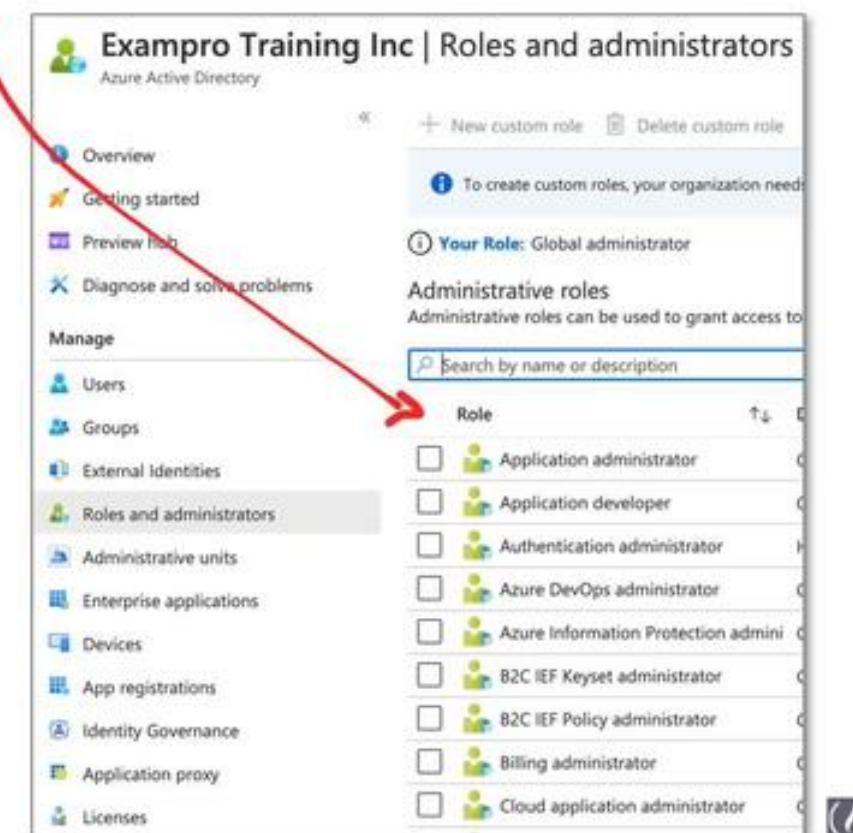
- create or edit users
- assign administrative roles to others
- reset user passwords
- manage user licenses
- manage domains.

A few important Built-In Azure AD roles you should know:

- **Global Administrator** Full access to everything
- **User Administrator** Full access to create and manage users
- **Billing Administrator** Make purchases, manage subscriptions and support tickets

You can create custom roles but you need to purchase either:

- Azure AD Premium P1 or P2



The screenshot shows the 'Roles and administrators' section of the Azure Active Directory portal for 'Exampro Training Inc'. A red arrow points from the text above to this section. The page includes a sidebar with links like Overview, Getting started, Preview hub, and Diagnose and solve problems. The main area has a 'Manage' section with links for Users, Groups, External Identities, and Roles and administrators (which is selected). To the right is a table of built-in roles:

Role	Description
Application administrator	
Application developer	
Authentication administrator	
Azure DevOps administrator	
Azure Information Protection administrator	
B2C IEF Keyset administrator	
B2C IEF Policy administrator	
Billing administrator	
Cloud application administrator	



# Azure Administrator

Azure Roles

## Azure Roles

# Anatomy of an Azure Role

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Role document syntax of the property names will change whether its Azure PowerShell or Azure CLI

**Name** (roleName) The display name of the custom role

**Id** (name) The unique ID of the custom role. This is autogenerated for you

**IsCustom** (roleType) Indicates whether this is a custom role. (true or false)

**Description** (description) The description of the custom role

**Actions** (actions) An array of strings that specifies the management operations that the role allows to be performed.

**NotActions** (notActions) An array of strings that specifies the management operations that are excluded from the allowed Actions

**DataActions** (dataActions) An array of strings that specifies data operations the role is allowed perform to your data within that object.

**NotDataActions** (notDataActions) An array of strings that specifies the data operations that are excluded from the allowed DataActions

**AssignableScopes** (assignableScopes) An array of strings that specifies the scopes that the custom role is available for assignment. You can only define one management group in AssignableScopes of a custom role.

```
{  
  "Name": "Virtual Machine Operator",  
  "Id": "88888888-8888-8888-8888-888888888888",  
  "IsCustom": true,  
  "Description": "Can monitor and restart virtual machines.",  
  "Actions": [  
    "Microsoft.Storage/**/read",  
    "Microsoft.Network/**/read",  
    "Microsoft.Compute/**/read",  
    "Microsoft.Compute/virtualMachines/start/action",  
    "Microsoft.Compute/virtualMachines/restart/action",  
    "Microsoft.Authorization/**/read",  
    "Microsoft.ResourceHealth/availabilityStatuses/read",  
    "Microsoft.Resources/subscriptions/resourceGroups/read",  
    "Microsoft.Insights/alertRules/*",  
    "Microsoft.Insights/diagnosticSettings/*",  
    "Microsoft.Support/*"  
  ],  
  "NotActions": [],  
  "DataActions": [],  
  "NotDataActions": [],  
  "AssignableScopes": [  
    "/subscriptions/{subscriptionId1}",  
    "/subscriptions/{subscriptionId2}",  
    "/providers/Microsoft.Management/managementGroups/{groupId1}"  
  ]  
}
```

# Anatomy of an Azure Role

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Wildcard permissions

Actions, NotActions, DataActions,  
and NotDataActions support wildcards (\*)

A wildcard allows you to apply to match **everything**

```
Microsoft.CostManagement/exports/action
Microsoft.CostManagement/exports/read
Microsoft.CostManagement/exports/write
Microsoft.CostManagement/exports/delete
Microsoft.CostManagement/exports/run/action
```

```
{
  "Name": "Virtual Machine Operator",
  "Id": "88888888-8888-8888-8888-888888888888",
  "IsCustom": true,
  "Description": "Can monitor and restart virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read",
    "Microsoft.ResourceHealth/availabilityStatuses/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Insights/diagnosticSettings/*",
    "Microsoft.Support/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/{subscriptionId1}",
    "/subscriptions/{subscriptionId2}",
    "/providers/Microsoft.Management/managementGroups/{groupId1}"
  ]
}
```



# Azure Administrator

Azure Roles

## Policies vs RBAC





# Azure Policies vs Azure Roles (RBAC)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Azure Policies

They are used to **ensure compliance** of resource.

Evaluates state by examining properties on resources that are represented in Resource Manager and properties of some Resource Provider

doesn't restrict actions (also called *operations*)

ensures that resource state is compliant to your business rules without concern for who made the change or who has permission to make a change

Even if an individual has access to perform an action, if the result is a non-compliant resource, Azure Policy still blocks the create or update

## Azure Roles

They are used to **control access** to Azure resources

Focuses managing user actions at different scopes

Does restriction on Azure resources





# Azure Administrator

Azure Roles

## Azure AD Roles vs RBAC





# Azure AD Roles vs Azure Roles (RBAC)

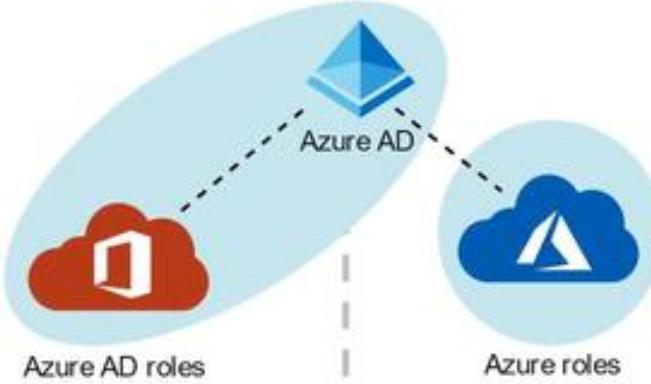
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Azure AD Roles

They are used to **control access** of **AD resources**

AD resources being:

- Users
- Groups
- Billing
- Licensing
- Application Registration
- Etc...



## Azure Roles

They are used to **control access** to **Azure resources**

Azure resources being:

- Virtual Machines
- Databases
- Cloud Storage
- Cloud Networking
- Etc..

- By default, Azure roles and Azure AD roles do not span Azure and Azure AD
- By default, the **Global Administrator** doesn't have access to Azure resources.
- Global Administrator can gain access to Azure resource if granted the User Access Administrator role (an Azure role)





# Azure Administrator

Azure Roles



## Azure Roles CheatSheet



# Azure Roles *CheatSheet*



Within Azure there are 3 kinds of roles:

1. **Classic subscription administrator roles** This is the original role system.
2. **Azure roles** known as Role-Based Access Controls (RBAC), built on top of Azure Resource Manager
3. **Azure Active Directory (Azure AD) roles** Azure AD roles are used to manage Azure AD resources in a directory

**Identity Access Management (IAM)** allows you to create and assign Azure (RBAC system) roles to users

Roles restrict access to resource actions (also known as operations). There are 2 types of roles:

1. **BuiltInRole** – Managed Microsoft roles are read only pre-created roles for you to use
2. **CustomRole** – A role created by you with your own custom logic

**Role assignment** is when you apply a role to user. A role assignment is composed of a Security Principle, Role Definition and Scope.

Azure's 4 built in roles are: Owner, Contributor, Reader, User Access Administrator

**Classic Administrators have three types of roles:**

1. **Account Administrator** The billing owner of the subscription. Has no access to the Azure portal.
2. **Service Administrator** same access of a user assigned the Owner role at subscription scope. Full access to the Azure portal.
3. **Co-Administrator** same access of a user who is assigned the Owner role at the subscription scope

**Important Azure AD Roles**

- **Global Administrator** Full access to everything
- **User Administrator** Full access to create and manage users
- **Billing Administrator** Make purchases, manage subscriptions and support tickets

You can create custom Azure AD Roles roles but you need to purchase either: Azure AD Premium P1 or P2





# Azure Administrator

Azure Policies

## Introduction to Azure Policies





# Introduction to Azure Policies

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Policy enforce organizational standards and to assess **compliance** at-scale  
Policies do not restrict access, they only observe for compliance.

## Policy Definitions

A policy definition is a **JSON** file used to describe business rules to control access to resources.

## Policy Assignment

The scope of a policy can effect. Assigned to a user, a resource group or management group.

## Policy Parameters

Values you can pass into your Policy definition so your Policies are more flexible for re-use.

## Initiative Definitions

An initiative definition is a collection of policy definitions, that you can assign. eg. A group of policies to enforce **PCI-DSS compliance**

Azure has "built-in" policies you can used right away

Scope	Definition type	Type	Category
Azure subscription 1	All definition types	All types	All categories
Name	Polic...	Type	Definition type
Audit virtual machines without disaster recovery ...	1	Built-in	Policy
Azure Backup should be enabled for Virtual Mac...	121	Built-in	Policy
Cognitive Services accounts should restrict netw...	5	Built-in	Policy
Audit Linux machines that have the specified ap...	29	Built-in	Policy
Azure Cosmos DB allowed locations	2	Built-in	Policy
SQL Managed Instance TDE protector should be ...	790	Built-in	Policy
[Preview]: Enable Data Protection Suite	72	Built-in	Initiative
HITRUST/HIPAA	62	Built-in	Initiative
Kubernetes cluster pod security baseline standar...	62	Built-in	Initiative
[Preview]: Windows machines should meet requi...	62	Built-in	Initiative
Enable Azure Cosmos DB throughput policy	62	Built-in	Initiative
NIST SP 800-53 R4	62	Built-in	Initiative
FedRAMP High	62	Built-in	Initiative
FedRAMP Moderate	62	Built-in	Initiative

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure Policies



Enforces **organizational standards** for **compliance**



# Azure Administrator

Azure Policies

## Non-Compliant Resources





# Viewing Non-Compliant Resources

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Once a policy is assigned it will evaluate for the compliance state periodically

We can see how compliant we are on the **Compliance tab**

The screenshot shows the Azure Policy Compliance blade. On the left, there's a navigation menu with tabs: Overview, Getting started, **Compliance** (which is selected and highlighted in grey), Remediation, Authoring, Assignments, Definitions, Related Services, Blueprints (preview), Resource Graph, and User privacy. The main area displays compliance statistics: Overall resource compliance at 0% (0 out of 1), Non-compliant initiatives at 0 (0 out of 0), Non-compliant policies at 1 (1 out of 1), and Non-compliant resources at 1 (1 out of 1). A table below lists a single non-compliant resource: Audit virtual machine snapshots, which is an Azure subscription 1 and is marked as Non-compliant with 0% (0 out of 1) compliance. A red arrow points from the text "We can see how compliant we are on the **Compliance tab**" to the Compliance tab in the navigation menu. Another red arrow points from the text "eg. VMs should have Disaster Recovery" to the "Non-compliant" status of the listed resource.

Name	Scope	Compliance state	Resource compli..
Audit virtual machine snapshots	Azure subscription 1	<input checked="" type="checkbox"/> Non-compliant	0% (0 out of 1)

eg. VMs should have Disaster Recovery





# Azure Administrator

Azure Policies

## Azure Policy Definition File

(A)  
SUBSCRIBE



# Anatomy of an Azure Policy Definition File

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Display Name** Identifies the policy (128 character limit)

**Type (readonly)**

- Built-in — Maintained by Microsoft
- Custom — Created by you
- Static — Microsoft Owned, A Regulatory Compliance

**Description** Provides the context of the policy

**Metadata**

Optional key value information to store on the policy in the

**Mode**

determines which resource types are evaluated. Changes whether using

Resource Provider or Azure Resource Manager

**Resource Manager**

- All — resource groups, subscriptions, and all resource types
- Indexed — only resource types that support tags and location

**Resource Provider**

- Microsoft.ContainerService.Data (*deprecated*)
- Microsoft.Kubernetes.Data
- Microsoft.KeyVault.Data

```
{  
  "properties": {  
    "displayName": "Management ports of virtual machines should be protected with just-in-time network access control",  
    "policyType": "BuiltIn",  
    "mode": "All",  
    "description": "Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations",  
    "metadata": { "version": "2.0.0", "category": "Security Center" },  
    "parameters": {  
      "effect": {  
        "type": "String",  
        "metadata": {  
          "displayName": "Effect",  
          "description": "Enable or disable the execution of the policy"  
        },  
        "allowedValues": ["AuditIfNotExists", "Disabled"],  
        "defaultValue": "AuditIfNotExists"  
      }  
    },  
    "policyRule": {  
      "if": {  
        "field": "type",  
        "equals": "Microsoft.Compute/virtualMachines"  
      },  
      "then": {  
        "effect": "[parameters('effect')]",  
        "details": {  
          "type": "Microsoft.Security/assessments",  
          "name": "805651bc-6ecd-4c73-9b55-97a19d0582d8",  
          "existenceCondition": {  
            "field": "Microsoft.Security/assessments/status.code",  
            "in": ["Healthy"]  
          }},  
          "id": "/providers/Microsoft.Authorization/policyDefinitions/b0f33259-77d7-4c9e-aac6-3aabcfae693c",  
          "type": "Microsoft.Authorization/policyDefinitions",  
          "name": "b0f33259-77d7-4c9e-aac6-3aabcfae693c"  
        }  
      }  
    }  
}
```





# Anatomy of an Azure Policy Definition File

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Parameters

Value you can pass into the policy to allow the policy to be more flexible. A parameter has the following properties

- **name** the name of the parameter
- **type** string, array, object, boolean, integer, float, or datetime.
- **metadata** used by Azure to display friendly information
  - **description**
  - **displayName**
  - **strongType** (optional, multi-select list)
  - **assignPermissions**
- **defaultValue** (optional)
- **allowedValues** (optional)

You reference parameters by using **field and in**

```
{  
  "field": "location",  
  "in": "[parameters('allowedLocations')]"  
}
```

```
{  
  "properties": {  
    "displayName": "Management ports of virtual machines should be protected with just-in-time network access control",  
    "policyType": "BuiltIn",  
    "mode": "All",  
    "description": "Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations",  
    "metadata": { "version": "2.0.0", "category": "Security Center" },  
    "parameters": {  
      "effect": {  
        "type": "String",  
        "metadata": {  
          "displayName": "Effect",  
          "description": "Enable or disable the execution of the policy"  
        },  
        "allowedValues": [ "AuditIfNotExists", "Disabled" ],  
        "defaultValue": "AuditIfNotExists"  
      }  
    },  
    "policyRule": {  
      "if": {  
        "field": "type",  
        "equals": "Microsoft.Compute/virtualMachines"  
      },  
      "then": {  
        "effect": "[parameters('effect')]",  
        "details": {  
          "type": "Microsoft.Security/assessments",  
          "name": "805651bc-6ecd-4c73-9b55-97a19d0582d0",  
          "existenceCondition": {  
            "field": "Microsoft.Security/assessments/status.code",  
            "in": [ "Healthy" ]  
          }  
        }  
      }  
    }  
  },  
  "id": "/providers/Microsoft.Authorization/policyDefinitions/b0f33259-77d7-4c9e-aac6-3aabcfae693c",  
  "type": "Microsoft.Authorization/policyDefinitions",  
  "name": "b0f33259-77d7-4c9e-aac6-3aabcfae693c"  
}
```



# Anatomy of an Azure Policy Definition File

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Policy Rule

consists of **If** and **Then** blocks.

In the **If** block, you define one or more conditions that specify when the policy is enforced.

You can apply logical operators to these conditions to precisely define the scenario for a policy.

```
{  
  "if": {  
    <condition> | <logical operator>  
  },  
  "then": {  
    "effect": "deny | audit | append | auditIfNotExists | deployIfNotExists | disabled"  
  }  
}
```



```
{  
  "properties": {  
    "displayName": "Management ports of virtual machines should be protected with just-in-time network access control",  
    "policyType": "BuiltIn",  
    "mode": "All",  
    "description": "Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations",  
    "metadata": { "version": "2.0.0", "category": "Security Center" },  
    "parameters": {  
      "effect": {  
        "type": "String",  
        "metadata": {  
          "displayName": "Effect",  
          "description": "Enable or disable the execution of the policy"  
        },  
        "allowedValues": ["AuditIfNotExists","Disabled"],  
        "defaultValue": "AuditIfNotExists"  
      }  
    },  
    "policyRule": {  
      "if": {  
        "field": "type",  
        "equals": "Microsoft.Compute/virtualMachines"  
      },  
      "then": {  
        "effect": "[parameters('effect')]",  
        "details": {  
          "type": "Microsoft.Security/assessments",  
          "name": "805651bc-6ecd-4c73-9b55-97a19d0582d8",  
          "existenceCondition": {  
            "field": "Microsoft.Security/assessments/status.code",  
            "in": ["Healthy"]  
          }  
        }  
      }  
    },  
    "id": "/providers/Microsoft.Authorization/policyDefinitions/b0f33259-77d7-4c9e-aac6-3aabcfae693c",  
    "type": "Microsoft.Authorization/policyDefinitions",  
    "name": "b0f33259-77d7-4c9e-aac6-3aabcfae693c"  
  }  
}
```





# Anatomy of an Azure Policy Definition File

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Policy Rule — Policy Effect

```
{  
    "if": {  
        <condition> | <logical operator>  
    },  
    "then": {  
        "effect": "deny | audit | append | auditIfNotExists | deployIfNotExists | disabled"  
    }  
}
```

- **Deny** — The resource creation/update fails due to policy.
- **Audit** — Creates a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
- **Append** — Adds additional parameters/fields to the requested resource during creation or update. A common example is adding tags on resources such as Cost Center or specifying allowed IPs for a storage resource.
- **Audit If Not Exists** — Creates a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
- **Deploy If Not Exists** — Executes a template deployment when a specific condition is met. For example, if SQL encryption is enabled on a database, then it can run a template after the DB is created to set it up a specific way.
- **Disabled** — The policy rule is ignored (disabled). Often used for testing.





# Azure Administrator

Azure Policies

## Configure Azure Policy



Follow Along

The screenshot shows the Azure Policy Definitions interface. At the top, there's a search bar and navigation links for 'Policy definition' and 'Initiative definition'. A sidebar on the left lists sections: Overview, Getting started, Compliance, Remediation, Authoring (with 'Assignments' selected), Definitions, Exemptions, Related Services, Blueprints (preview), Resource Graph, and User privacy. The main content area displays a list of policy definitions under the heading 'Definitions'. Each item has a small preview icon and a link. The first few items are: 'Microsoft Azure Foundations Benchmark 1.0', 'Enable Monitoring in Azure Security Center', '[Preview]: Australian Government ISM PROTECT', and 'UK OFFICIAL and UK NHS'. At the bottom right, there's a 'BENCHMARKS' section with icons for 'PCI v3.2.1:2018', 'Canada Federal FIPS 140-2', 'Enable Azure Monitor for VMs', and 'Enable Azure Monitor for Virtual Machine Scale Sets'.

Name
Microsoft Azure Foundations Benchmark 1.0
[Preview]: Deploy prerequisites to enable Guest OS monitoring
OS Microsoft Azure Foundations Benchmark 1.0
Enable Monitoring in Azure Security Center
[Preview]: Australian Government ISM PROTECT
UK OFFICIAL and UK NHS
[Preview]: SWIFT CSP-CSCF v2020
[Preview]: Azure Security Benchmark
Kubernetes cluster pod security restricted standard
PCI v3.2.1:2018
Canada Federal FIPS 140-2
Enable Azure Monitor for VMs
Enable Azure Monitor for Virtual Machine Scale Sets



# Azure Administrator

Azure Policies



## Azure Policies CheatSheet

(A)  
SUBSCRIBE

# Azure Policies *CheatSheet*



Azure Policy enforce organizational standards and to assess **compliance** at-scale

- Policies do not restrict access, they only observe for compliance.

Once a policy is assigned it will evaluate for the compliance state periodically

The rules of a policy are describe in a JSON file and is known as a **policy definition**

Policy definition can be grouped together which is known as a **policy initiative** (formally known as a policy set)



# Azure Administrator

Azure Resource Manager



## Introduction to Azure Resource Manager





# Introduction to Azure Resource Manager

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Resource Manager (ARM) is a service that allows you to **manage** Azure resources.

Azure Resource Manager is a collection of services in the Azure Portal, **so you can't simply type** in "Azure Resource Manager"



The screenshot shows the Azure Portal's search interface. A search bar at the top contains the text "azure resource manager". Below the search bar, a list of services is displayed under the heading "Services". The services listed are: Azure Cosmos DB, Azure Database for MySQL servers, Azure Resource Mover, Azure Arc, Azure Databricks, Azure Lighthouse, Azure Migrate, Azure OSS, Azure Quantum, and Azure Sentinel. Each service entry includes a small blue circular icon with a white symbol representing the service.

It is a management layer that allows you to:

- Create, Update, Delete Resources
- Apply Management features eg. Access Controls, Locks, Tags
- Writing Infrastructure as Code (IaC) via JSON templates.

The specific features we are going to look at that make up the ARM layer are the following:

- |                      |                                     |
|----------------------|-------------------------------------|
| • Subscriptions      | • Resource Tags                     |
| • Management Groups  | • Access Control (IAM)              |
| • Resource Groups    | • Role-Based Access Controls (RABC) |
| • Resource Providers | • Azure Policies                    |
| • Resource Locks     | • ARM Templates                     |
| • Azure Blueprints   |                                     |



Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure Resource Manager



A **deployment and management service** for Azure  
Enables you to **create, update, and delete** resources in your Azure account



# Azure Administrator

Azure Resource Manager

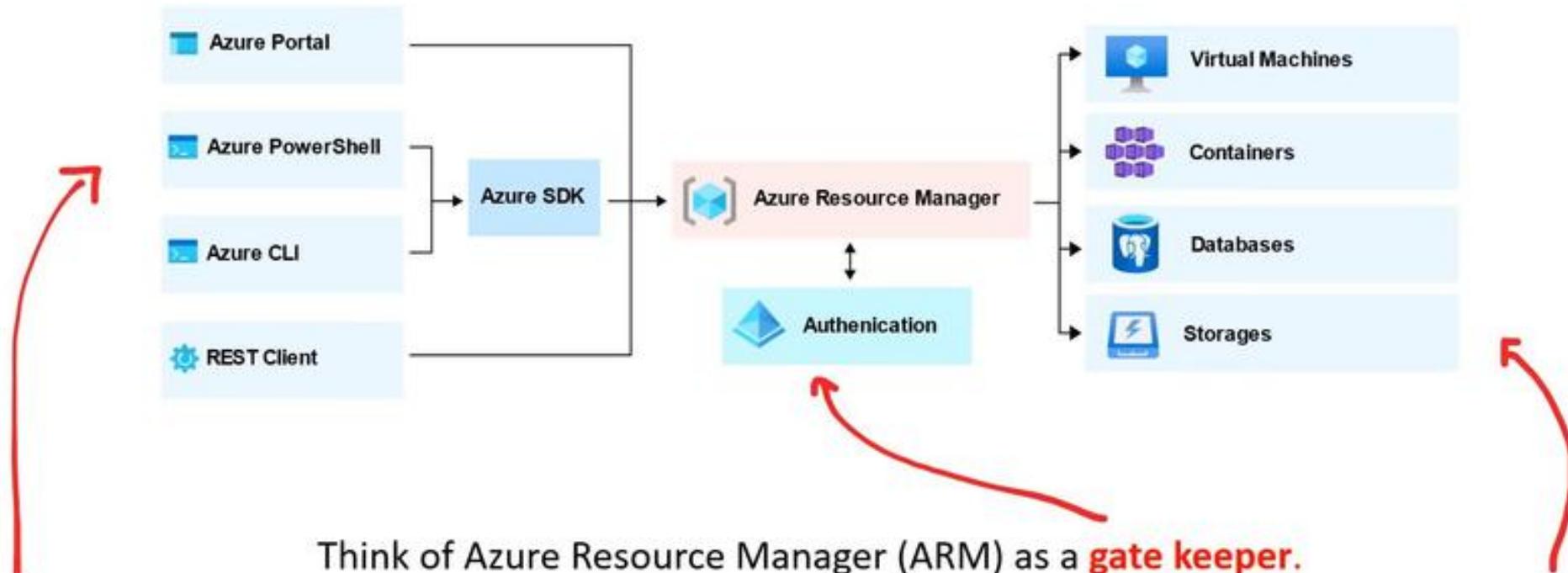
## [] Use Cases

(A)  
SUBSCRIBE



# Azure Resource Manager – Use Case

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)



Think of Azure Resource Manager (ARM) as a **gate keeper**.

All **requests** flow through ARM and it decides whether that request can be performed on a **resource**.





# Azure Administrator

Azure Resource Manager

## [] Scoping

(A)  
SUBSCRIBE



# Azure Resource Manager – Scoping

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is scope?

Scope is a **boundary of control** for azure resources. It is a way to **govern** your resource by placing resources

- within a logical grouping
- and also applying logical restrictions in the form of rules.



### Management Groups

A logical grouping of multiple subscriptions



### Subscriptions

grants you access to Azure services based on a billing and support agreement



### Resource Groups

A logical grouping of multiple resources



### Resources

An azure service eg. Azure VMs

*We'll revisit scope when we look at Role-Based Access Controls (RBAC)*





# Azure Administrator

Azure Resource Manager



## Subscriptions

(<sup>A</sup>)  
SUBSCRIBE



# Subscriptions

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

Before you can do anything in your Azure account. You'll need to have a subscription.

An Azure Account can have **multiple subscriptions** and the most common three are:

- Free Trial
- Pay-As-You-Go
- Azure for Students

eg. If you wanted Developer support you  
Would add a Developer Support Subscription

The screenshot shows three subscription options in the Azure portal:

- Free Trial**: Full access to all services. Explore any service that you want. [Learn more](#). **Select offer**
- Pay-As-You-Go**: This flexible pay-as-you-go plan involves no up-front costs, and no long term commitment. You pay only for the resources that you use. [Learn more](#). **Select offer**
- Azure for Students**: Innovate, explore and drive your career with Azure credits plus popular free products for 12 months. [Learn more](#). **Select offer**

At the subscription level you'll  
have the ability to set:

- Resource Tags
- **Access Controls**
- Resources Groups
- And more ...

The screenshot shows the 'Access control (IAM)' section for 'Azure subscription 1'.

**Subscription**

Search (Cmd+F) + Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Security Events Cost Management Cost analysis Cost alerts Budgets

Number of role assignments for this subscription: 1 / 2000

Role assignments (1 items (1 Users))

Name	Type	Role	Scope
Andrew Brown andrew@exampr...	User	Owner	This resource



# Azure Administrator

Azure Resource Manager



## Management Groups



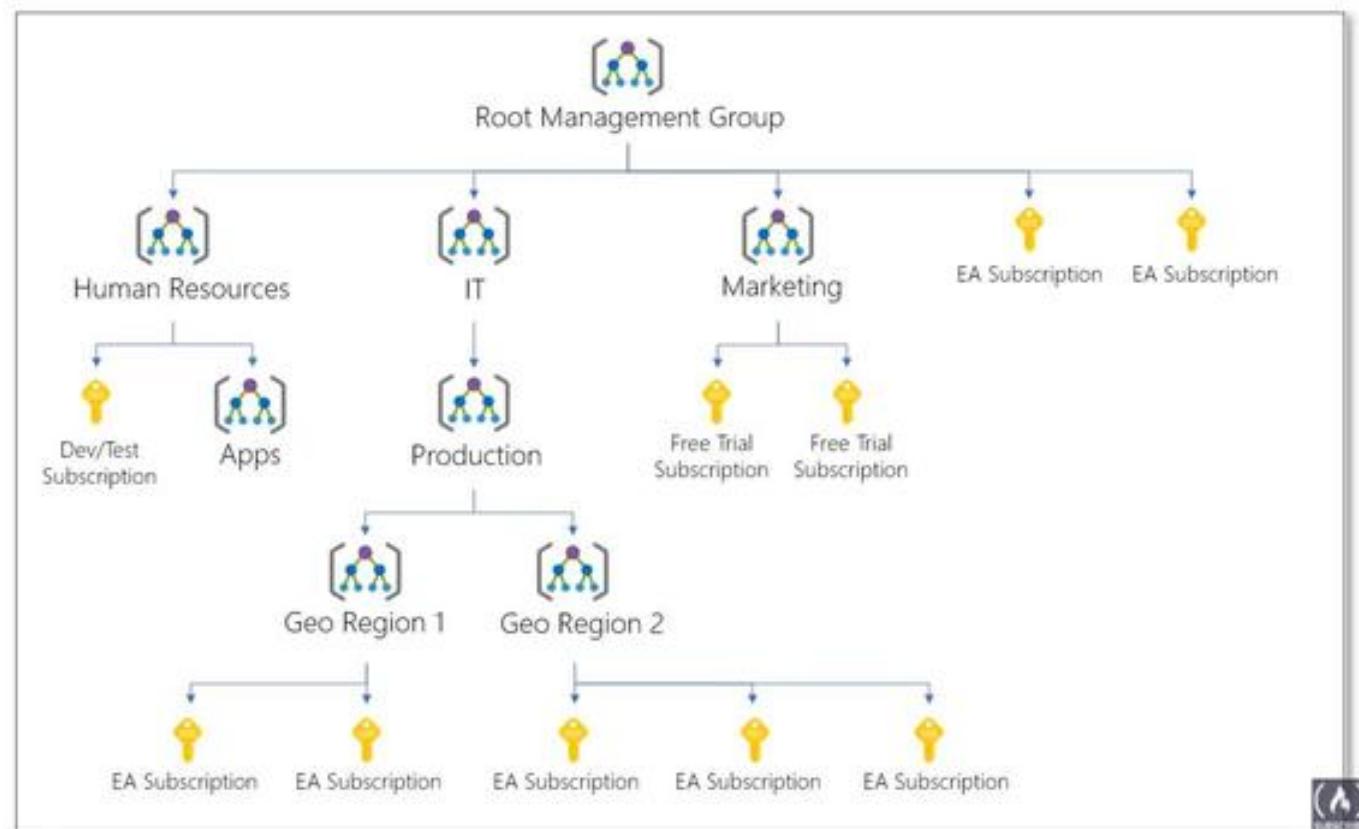
# Azure Management Groups

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

Managing multiple subscriptions (accounts) into a hierachal structure.

Each directory is given a single top-level management group called the "Root" management group.

All subscriptions within a management group automatically inherit the conditions applied to the management group.





# Azure Administrator

Azure Resource Manager

## [RG] Resource Groups





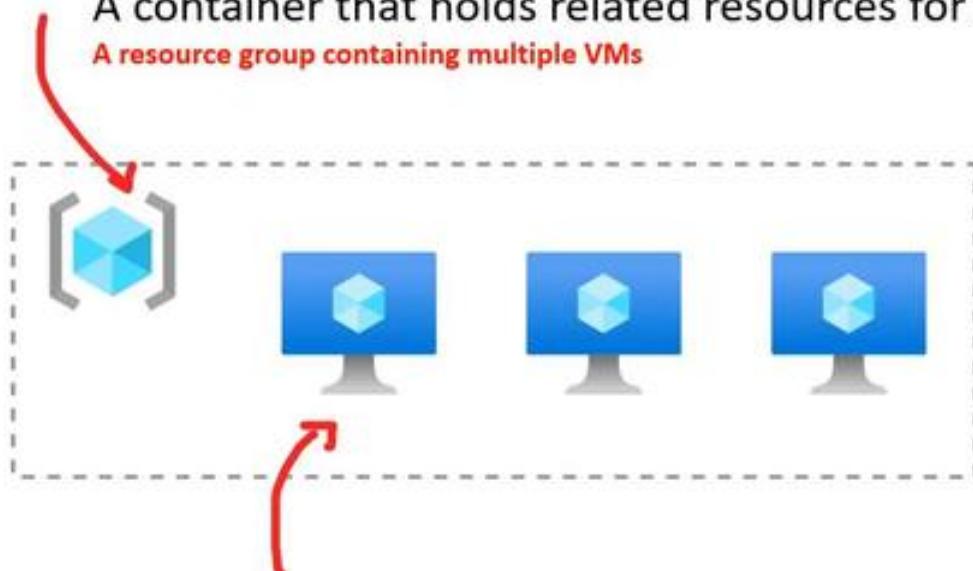
# Resources Groups

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Resource Group

A container that holds related resources for an Azure solution

**A resource group containing multiple VMs**



## Resource

A manageable item that is available through Azure

**An individual Virtual Machine (VM)**

## Resource Provider

A service that supplies Azure resources.

**eg. Microsoft.Compute**





# Azure Administrator

Azure Resource Manager



## Resource Providers

(A)  
SUBSCRIBE

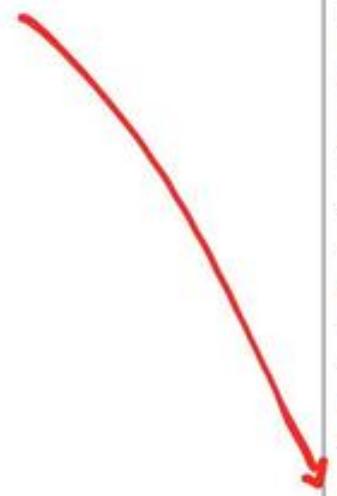


# Resources Providers

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

In order to use Azure resources you have to **register Resource Providers**  
Many Resource Providers are registered by default for you with your Subscription.

You can register Resource Providers  
under your subscription



Azure subscription 1   Resource providers		
Subscription		
Billing		Status
	Microsoft.ClassicStorage	<input type="radio"/> NotRegistered
	Microsoft.ClassicSubscription	<input checked="" type="radio"/> Registered
	Microsoft.CodeSpaces	<input type="radio"/> NotRegistered
	Microsoft.CognitiveServices	<input type="radio"/> NotRegistered
	Microsoft.Commerce	<input checked="" type="radio"/> Registered
	Microsoft.Compute	<input type="radio"/> NotRegistered
	Microsoft.ConnectedCache	<input type="radio"/> NotRegistered
	Microsoft.Consumption	<input checked="" type="radio"/> Registered
	Microsoft.ContainerInstance	<input type="radio"/> NotRegistered
	Microsoft.ContainerRegistry	<input type="radio"/> NotRegistered
	Microsoft.ContainerService	<input type="radio"/> NotRegistered
	Microsoft.ContainerManagement	<input checked="" type="radio"/> Registered
	Microsoft.CostManagement	<input type="radio"/> NotRegistered





# Azure Administrator

Azure Resource Manager



## Resource Tags

(A)  
SUBSCRIBE



# Resource Tags

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

A tag is a **key and value pair** that you can assign to azure resources.

Name ⓘ	Value ⓘ	Resource
Env	: Production	Storage account
Project	: Enterprise	Storage account
	:	Storage account



## Tag Examples

Dept = Finance

Status = Approved

Team = Compliance

Environment = Production

Project = Enterprise

Location = West US

Tags allow you to organize your resources in the following ways:

- **Resource management**
  - specific workloads, environments eg. Developer Environments
- **Cost management and optimization**
  - Cost tracking, Budgets, Alerts
- **Operations management**
  - Business commitments and SLA operations eg. Mission-Critical Services
- **Security**
  - Classification of data and security impact
- **Governance and regulatory compliance**
- **Automation**
- **Workload optimization**





# Azure Administrator

Azure Resource Manager

## [] Resource Locks

(Λ)  
SUBSCRIBE



# Resource Locks

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

As an admin, you may need to **lock a subscription, resource group, or resource** to **prevent other users from accidentally deleting or modifying critical resources.**

In the **Azure Portal** you can set the following lock levels.

**CannotDelete (Delete)**

authorized users can still read and modify a resource, but they can't delete the resource.

**ReadOnly (Read-only)**

authorized users can read a resource, but they can't delete or update the resource





# Azure Administrator

Azure Resource Manager



# Azure Blueprints

(A)  
SUBSCRIBE



# Azure Blueprints

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Blueprints enable **quick creation** of **governed subscriptions**.

Compose artifacts based on common or organization-based patterns into re-usable blueprints.

The service is designed to help with *environment setup*

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed **Azure Cosmos DB**  
Blueprint objects are replicated to multiple Azure regions.



## ARM Templates vs Azure Blueprints

Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with an ARM template.

### ARM Template

- ARM templates are stored either locally or in source control.
- There's no active connection or relationship to the ARM template

### Azure Blueprints

- relationship between the blueprint definition (*what should be deployed*) and the blueprint assignment (*what was deployed*)
- can also upgrade several subscriptions at once that are governed by the same blueprint

Azure Blueprints supports **improved tracking and auditing of deployments**





# Azure Administrator

Azure Resource Manager

## [] Moving Resources



Follow Along

Microsoft Azure     |P| Search resources, services, and documentation

Home > Resource groups > the-federation-of-planets >

### Move resources

Resources to move

Select all

Dilithium

Move these resources to:

Resource group \*  
the-klingon-empire

I understand that tools and scripts associated with moved resources will not work until I update them.

UBLISHING     SUBSCRIBE



# Azure Administrator

Azure Resource Manager



## ARM CheatSheet

# Azure Resource Manager *CheatSheet*

Exam

Pro

Azure Resource Manager (ARM) is a service that allows you to **manage** Azure resources.

It is a management layer that allows you to: Create, Update, Delete Resources

- Apply Management features eg. Access Controls, Locks, Tags
- Writing Infrastructure as Code (IaC) via JSON templates.

ARM is a service layer that **spans multiple features and services**: Subscriptions, Management Groups, Resource Groups ,Resource Providers, Resource Locks, Azure Blueprints, Resource Tags, Access Control (IAM), Role-Based Access Controls (RABC), Azure Policies, ARM Templates

Think of Azure Resource Manager (ARM) as a **gate keeper**.

- All **requests** flow through ARM and it decides whether that request can be performed on a **resource**.

Scope is a **boundary of control** for azure resources. It is a way to **govern** your resource by placing resources within a logical grouping and also applying logical restrictions in the form of rules.

- **Management Groups** A logical grouping of multiple subscriptions
  - **Subscriptions** grants you access to Azure services based on a billing and support agreement
    - **Resource Groups** A logical grouping of multiple resources
      - **Resources** An azure service eg. Azure VMs

An Azure Account can have **multiple subscriptions** and the most common three are: Free Trial, Pay-As-You-Go, Azure for Students

**Resource Providers** a list of possible services with an Azure, some services are *registered* by default and other needs to explicitly registered

**Resource Tags** is a **key and value pair** that you can assign to azure resources

Resource Locks prevent users from accidentally modifying or deleting resources at the Subscriptions, Resource Group or Resource scope

- **CannotDelete (Delete)** authorized users can still read and modify a resource, but they can't delete the resource.
- **ReadOnly (Read-only)** authorized users can read a resource, but they can't delete or update the resource

Blueprints enable **quick creation** of **governed subscriptions**.

- Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with an ARM template.
- relationship between the blueprint definition (what *should be deployed*) and the blueprint assignment (what *was deployed*)





# Azure Administrator

ARM Templates

## Introduction to ARM Templates





# ARM Templates

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is Infrastructure As Code? (IaC)

the process of **managing and provisioning** computer data centers (eg, Azure) through machine-readable **definition files** (eg. JSON files) rather than physical hardware configuration or interactive configuration tools.

You write a script that will setup cloud services for you.

IaCs can either be:

- **Declarative** — You defined exactly what you want, and you get exactly that
- **Imperative** — You define what you generally want, and the service will guess what you want

**ARM templates** are **JSON files that define azure resources** you want to provision and azure services you want to configure.

With ARM templates you can:

- **ARM templates** are declarative. (you get exactly what you define)
- stand up, tear down or share entire architectures in minutes
- Reduce configuration mistakes
- Know exactly what you have defined for a stack to establish an architecture baseline for compliance





# ARM Templates

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

With ARM templates you can:

- **ARM templates** are declarative. (you get exactly what you define)
- stand up, tear down or share entire architectures in minutes
- Reduce configuration mistakes
- Establish an architecture baseline for compliance
- **Modularity** Break up your architecture in multiple files and reuse them
- **Extensibility** Add PowerShell and Bash scripts to your templates
- **Testing** You can use the ARM template tool kit (arm-ttk)
- **Preview Changes** Before you create infrastructure via template, see what it will create
- **Built-In Validation** Will only deploy your template if it passes
- **Tracked Deployments** Keep track of changes to architecture over time
- **Policy as Code** Apply Azure policies to ensure you remain compliant
- **Microsoft Blueprints** (establishes relationship between resource and the template)
- **CI/CD integration**
- **Exportable Code** (exporting the current state of a resource groups and resources)
- **Authoring Tools** Visual Studio Code has advanced features for authoring ARM templates





# Azure Administrator

ARM Templates

## ARM Template Skeleton





# ARM Template – Skeleton

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Skeleton

The general structure of an ARM template

**\$schema** describes the properties that are available within a template

**contentVersion** the version of the template.

You can provide any value for this element

**apiProfile** Use this value to avoid having to specify API versions for each resource in the template

**parameters** values you can pass along to your template

**variables** you transform parameters or resource properties using function expressions

**functions** User-defined functions available within the template

**resources** the azure resources you'll want to deploy or update

```
{  
  "$schema":  
    "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
  "contentVersion": "1.0.0",  
  "apiProfile": "",  
  "parameters": { },  
  "variables": { },  
  "functions": [ ],  
  "resources": [ ],  
  "outputs": { }  
}
```

**outputs** values that are returned after deployment





# Azure Administrator

ARM Templates

## ARM Template Resources





# ARM Template – Resources

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Resource

An Azure Resource you want to provision

### **type**

Type of the resource

Follows the format of {ResourceProvider}/ResourceType

### **apiVersion**

Version of the REST API to use for the resource

Each resource provider published its own API versions,

### **name**

Name of the resource

### **location**

Most resources have a location property

The region where the resource will be deployed

### **Other Properties**

Other properties we can use to configure the resource

Will vary per resource type

```
{  
    "$schema":  
        "https://schema.management.azure.com/schemas/2019-  
        04-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "resources": [  
        {  
            "type": "Microsoft.Storage/storageAccounts",  
            "apiVersion": "2019-04-01",  
            "name": "{provide-unique-name}",  
            "location": "eastus",  
            "sku": {  
                "name": "Standard_LRS"  
            },  
            "kind": "StorageV2",  
            "properties": {  
                "supportsHttpsTrafficOnly": true  
            }  
        }  
    ]  
}
```



# Azure Administrator

ARM Templates

## ARM Template Parameters





# ARM Template – Parameters

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Parameters

Allows you to pass variables to your ARM template

**type** the expected data type of the inputed value

- **string, securestring, int, bool, object, secureObject, and array.**

**defaultValue** if not value is provided it will be set to this value

**allowedValues** an array of allowed values

**minValue** the minimal possible value

**maxValue** the maximum possible value

**minLength** the maximum length of characters or array

**maxLength** the maximum length of characters or array

**description** the description that will be displayed to the in the Azure Portal

Setting a parameter

Accessing a parameter

```
{  
  "$schema":  
    "https://schema.management.azure.com/schemas/2019-  
    04-01/deploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "parameters": {  
    "storageName": {  
      "type": "string",  
      "minLength": 5,  
      "maxLength": 20  
    }  
  },  
  "resources": [  
    {  
      "type": "Microsoft.Storage/storageAccounts",  
      "apiVersion": "2019-04-01",  
      "name": "[parameters('storageName')]",  
      "location": "eastus",  
      "sku": {  
        "name": "Standard_LRS"  
      },  
      "kind": "StorageV2",  
      "properties": {  
        "supportsHttpsTrafficOnly": true  
      }  
    }  
  ]  
}
```





# Azure Administrator

ARM Templates

## ARM Template Functions





# ARM Template – Functions

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Functions

Allows you to apply transformations to your ARM variables

- Template Functions — built-in functions
- Used-Defined Functions — custom functions you create

Functions are called using **parentheses eg. ()**:

```
{ "condition": "[equals(parameters('newOrExisting'), 'new')]" }
```



## Template Functions

- **Array:** array, concat, contains, createArray, empty, first, intersection, last, length, min, max, range, skip, take, union
- **Comparison:** coalesce, equals, less, lessOrquals, greater, greaterOrEqual
- **Date:** dateTimeAdd, utcNow
- **Deployment:** deployment, environment, **parameters, variables**
- **Logical:** and, or, if, not, or
- **Numeric:** add, copyIndex, div, float, int, min, max, mod, mul, sub
- **Object:** contains, empty, intersection, json, length, union
- **Resource:** extensionResourceId, ListAccountSas, listKeys, listSecrets, list\*, picZones, providers, reference, resourceGroup, resourceId, subscription, subscriptionResourceId, tenantResourceId
- **String:** base64, base64ToJson, base64ToString, concat, contains, dataUri, DataUriToString, empty, endsWith, first, format, guid, indexOf, last, lastIndexOf, length, newGuid, padLeft, replace, skip, split, startsWith, string, substring, take, toLower, toUpper, trim, uniqueString, uri, uriComponent, uriComponentToString





# Azure Administrator

ARM Templates

## ARM Template Variables





# ARM Template – Variables

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Variables

Template variables are used to simplify your arm templates.

You transform parameters and resource properties using functions  
and then assign them into a reusable variable



```
"variables": {  
    "storageName": "[concat(toLower(parameters('storageNamePrefix')),uniqueString(resourceGroup().id))]"  
},
```

To call a variable you use the **variable()** function



```
"resources": [  
    {  
        "type": "Microsoft.Storage/storageAccounts",  
        "name": "[variables('storageName')]",  
        ...  
    }  
]
```





# ARM Template – Variables

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

## Nested Variables

You can use json object to have nested variables to scope your variables for multiple use cases.

Scoping/Nesting variables **based on environment**

```
"variables": {  
    "environmentSettings": {  
        "test": {  
            "instanceSize": "Small",  
            "instanceCount": 1  
        },  
        "prod": {  
            "instanceSize": "Large",  
            "instanceCount": 4  
        }  
    }  
},
```

Using params to **choose the environment**

```
"parameters": {  
    "environmentName": {  
        "type": "string",  
        "allowedValues": [  
            "test",  
            "prod"  
        ]  
    }  
},
```

"[variables('environmentSettings')[parameters('environmentName')].instanceSize]"

Referencing nested variables eg. Variables()[] .property





# Azure Administrator

ARM Templates

## ARM Template Output





# ARM Template – Outputs

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

## Outputs

Returns values from deployed resources, so you can use them programmatically

You specific **the type and value** under outputs

```
"outputs": {  
    "resourceID": {  
        "type": "string",  
        "value": "[resourceId('Microsoft.Network/publicIPAddresses', parameters('publicIPAddresses_name'))]"  
    }  
}
```

You can use the Azure API via **CLI**, PowerShell or SDK to fetch outputs

```
az deployment group show \  
  -g <resource-group-name> \  
  -n <deployment-name> \  
  --query properties.outputs.resourceID.value
```





# Azure Administrator

ARM Templates

## Launch an ARM Template



Follow Along

Microsoft Azure     [Search resources, services, and docs \(S + F\)](#)

Home > Create a CDN Profile, a CDN Endpoint and a Web App >

Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ⌂ Load file ⌂ Download

```
1<parameters>
2  WorflinuxOSVersion: {
3    "type": "string",
4    "defaultValue": "14.04.2-LTS"
5  },
6  "WorflinuxPassword": {
7    "type": "securestring"
8  },
9  "WorflinuxOSVersion": {
10   "type": "string",
11   "defaultValue": "14.04.2-LTS"
12   "allowedValues": [
13     "12.04.5-LTS",
14     "14.04.2-LTS",
15     "15.04"
16   ]
17 },
18  "WorflinuxType": {
19    "type": "string",
20    "defaultValue": "Standard_LRS"
21   "allowedValues": [
22     "standard_LRS",
23     "standard_ZRS",
24     "standard_GRS",
25     "standard_RAGRS",
26     "Premium_LRS"
27   ]
28 },
29  "Worf": {
30    "type": "object"
31  },
32  "Worf": {
33    "type": "object"
34  },
35  "Worf": {
36    "type": "object"
37  },
38  "Worf": {
39    "type": "object"
40  }
41 },
42 "resources": [
43   {
44     "type": "Microsoft.Network/networkInterfaces",
45     "name": "[concat('Worflinux', uniqueId())]",
46     "location": "[resourceGroup().location]",
47     "tags": {
48       "Name": "Worflinux"
49     },
50     "properties": {
51       "ipConfigurations": [
52         {
53           "name": "IPConfig1",
54           "properties": {
55             "privateIPAllocationMethod": "Dynamic",
56             "subnet": {
57               "id": "[resourceId('Microsoft.Network/virtualNetworks', 'Worf').subnets[0].id]"
58             }
59           }
60         }
61       ],
62       "networkSecurityGroup": {
63         "id": "[resourceId('Microsoft.Network/networkSecurityGroups', 'Worf')]"
64       }
65     }
66   },
67   {
68     "type": "Microsoft.Compute/virtualMachines",
69     "name": "[concat('Worflinux', uniqueId())]",
70     "location": "[resourceGroup().location]",
71     "tags": {
72       "Name": "Worflinux"
73     },
74     "properties": {
75       "hardwareProfile": {
76         "vmSize": "Standard_DS1_v2"
77       },
78       "osProfile": {
79         "computerName": "Worflinux",
80         "adminUsername": "root",
81         "adminPassword": "[parameters('WorflinuxPassword')]",
82         "linuxConfiguration": {
83           "osType": "Ubuntu",
84           "disablePasswordAuthentication": false,
85           "ssh": {
86             "publicKeys": [
87               {
88                 "keyData": "[listKeys(resourceId('Microsoft.KeyVault/vaults', 'Worf'), '2015-06-15').keys[0].value]"
89               }
90             ]
91           }
92         }
93       },
94       "storageProfile": {
95         "imageReference": {
96           "uri": "https://marketplace.azureedge.net/api/images/marketplaceImageContext?imageId=10000000000000000000000000000000&version=1&language=en-US&size=1280x720&format=png&scale=100&type=ThumbnailImage&blobType=Image&blobContainerName=marketplace-image-thumbs&blobName=10000000000000000000000000000000_1.png",
97           "offer": "Ubuntu Server 16.04 LTS (HVM) - Standard"
98         },
99         "osDisk": {
100          "caching": "None",
101          "createOption": "FromImage"
102        }
103      }
104    }
105  }
106 ]
```

Save Discard



# Azure Administrator

ARM Templates



## ARM Template CheatSheet



# ARM Templates *CheatSheet*

Exam  Pro

Infrastructure As Code (IaC) is the process of managing and provisioning computer data centers (eg, Azure) through machine-readable definition files (eg. JSON files) rather than physical hardware configuration or interactive configuration tools.

IaCs can either be:

- **Declarative** — You defined exactly what you want, and you get exactly that
- **Imperative** — You define what you generally want, and the service will guess what you want

ARM templates are JSON files that define azure resources you want to provision and azure services you want to configure.

ARM templates are declarative. (you get exactly what you define)

An ARM template is made of the following JSON structure:

- **\$schema** describes the properties that are available within a template
- **contentVersion** the version of the template. You can provide any value for this element
- **apiProfile** Use this value to avoid having to specify API versions for each resource in the template
- **parameters** values you can pass along to your template
- **variables** you transform parameters or resource properties using function expressions
- **functions** User-defined functions available within the template
- **resources** the azure resources you'll want to deploy or update
  - **type** Type of the resource
  - **apiVersion** Version of the REST API to use for the resource, Each resource provider published its own API versions
  - **name** Name of the resource
  - **Location** Most resources have a location property, The region where the resource will be deployed
  - **Other Properties** Other properties we can use to configure the resource. Will vary per resource type
- **outputs** values that are returned after deployment





# Azure Administrator



## Introduction to Storage Accounts

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure Storage Accounts



Contains all of your Azure Storage data objects:

**blobs, files, queues, tables, and disks**



# Introduction to Storage Accounts

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Storage offers **several types of storage** accounts.

Each with **different features** and **their own pricing models**

- General-purpose v1 (legacy)
- General-purpose v2
- BlobStorage (legacy)
- BlockBlobStorage
- FileStorage

Storage accounts vary with the following features:

**Supported Services** (What can I put in this storage account?)

Blob, File, Queue, Table, **Disk**, and Data Lake Gen2

**Performance Tiers** (how fast will my read and writes be?)

Standard and Premium

**Access Tiers** (how often do I need quick access to files?)

Hot, Cool, Archive

**Replication** (How many redundant copies should be made and where?)

LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS

**Deployment model** (Who should deploy the supported services?)

Resource Manager, Classic

**Storage type** and **Account Kind** means the same thing

Account kind ⓘ **BlobStorage** ▾

 **Containers**  
Scalable, cost-effective storage for unstructured data  
[Learn more](#)

 **File shares**  
Serverless SMB and NFS file shares  
[Learn more](#)

 **Tables**  
Tabular data storage  
[Learn more](#)

 **Queues**  
Effectively scale apps according to traffic  
[Learn more](#)





# Azure Administrator



## Storage Comparsion





# Introduction to Storage Accounts

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Type	Service	Performance Tiers	Access Tiers	Replication	Deployment Models
General-purpose V2	Blob, File, Queue, Table, Disk, Data Lake Gen 2	Standard, Premium	Hot, Cool, Archive	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Resource Manager
General-purpose V1	Blob, File, Queue, Table, Disk	Standard, Premium	N/A	LRS, GRS, RA-GRS	Resource Manager <b>Classic</b>
BlockBlobStorage	Blob (block, append)	Premium	N/A	LRS, ZRS	Resource Manager
FileStorage	File	Premium	N/A	LRS, ZRS	Resource Manager
BlobStorage	Blob (Block, append)	Standard	Hot, Cool, Archive	LRS, GRS, RA-GRS	Resource Manager





# Azure Administrator



## Core Storage Services



# Core Storage Services

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure has 5 core storage services

blob

Services

Storage accounts

disk

Services

Disks

Disk Accesses

Disks (classic)



## Azure Blob

A massively scalable **object store** for text and binary data.  
Also includes support for big data analytics through Data Lake Storage Gen2



## Azure Files

Managed **file shares** for cloud or on-premises deployments



## Azure Queues

A **NoSQL store** for schemaless storage of structured data.



## Azure Tables

A **messaging store** for reliable messaging between application components



## Azure Disks

**Block-level storage** volumes for Azure VMs





# Azure Administrator



## Performance Tiers



# Performance Tiers (Blob Storage)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are **2 types** of performance tiers for storage accounts: Standard and Premium



Performance  Standard  Premium

IOPS stands for Input/Output Operations Per Second

The higher the IOPS the faster a drive can read and write

## Premium Performance

- Stored on Solid State Drives (**SSDs**)
- Optimize for low-latency
- Higher throughput
- Use cases:
  - Interactive workloads
  - Analytics
  - AI or ML
  - Data transformation



## Standard Performance

- Stored on Hard Disk Drives (**HDDs**)
- Varied performance based on access tier (Hot, Cool, Archive)  
Use cases:
  - Backup and disaster recovery
  - Media content
  - Bulk data processing



An SSD **has no moving parts** and data is distributed randomly. This is why it can read and write so fast.

An HDD **has moving parts**, an arm that needs to read and write data sequential to a disk. It is very good at writing or reading large amounts of data that is close together





# Azure Administrator



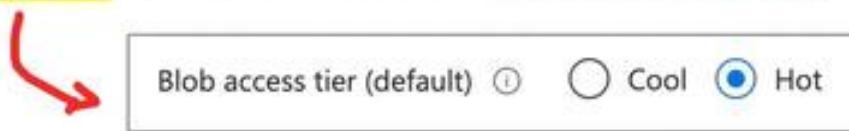
## Access Tiers



# Access Tiers (Blob Storage)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are **3 types** of access tiers for **Standard storage**: Cool, Hot and Archive



## Hot

- Data that's accessed frequently.
- Highest storage cost, lowest access cost

### Use Case

- Data that's in active use or expected to be accessed frequently.
- Data that's staged for processing and eventual migration to the cool access tier

## Cool

- Data that's infrequently accessed and stored for at least 30 days.
- Lower storage cost, higher access cost

### Use Case

- Short-term backup and disaster recovery datasets
- Older media content not viewed frequently anymore but is expected to be available immediately when accessed
- Large data sets that need to be stored cost effectively while more data is being gathered for future processing.

## Archive

- Data that's rarely accessed and stored for at least 180 days
- Lowest storage cost, highest access cost

### Use Case

- Long-term backup, secondary backup, and archival datasets
- Original (raw) data that must be preserved, even after it has been processed into final usable form.
- Compliance and archival data that needs to be stored for a long time and is hardly ever accessed.





# Access Tiers (Blob Storage)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Account Level Tiering

Any blob that doesn't have an explicitly assigned tier infers the tier from the Storage Account access tier setting.

## Blob-Level Tiering

You can upload a blob to the tier of your choice.

Changing tiers happens instantly with the exception from moving out of archive

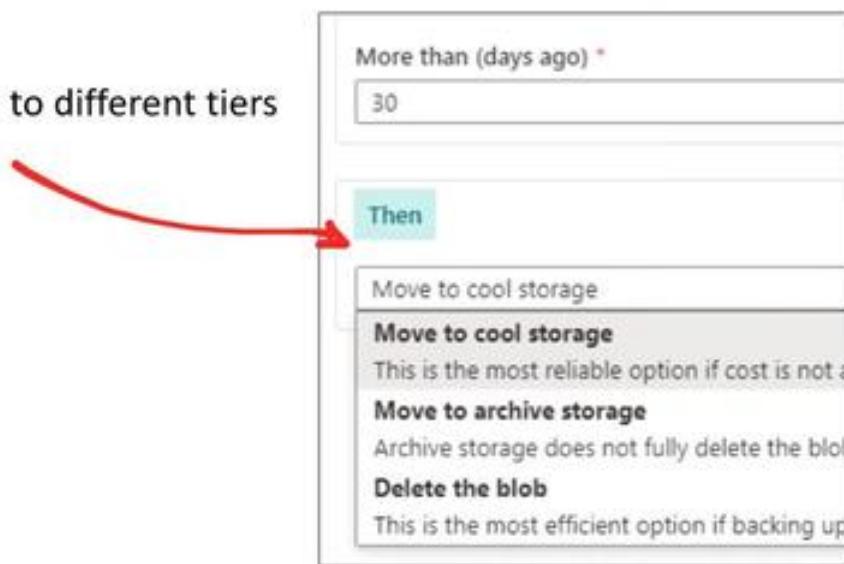
## Rehydrating a Blob

When moving a blob out of archive into another tier it can take several hours. This is known as “rehydrating”

## Blob Lifecycle Management

You can create rule-based policies to transition data to different tiers

Eg. After 30 days move to cool storage



The screenshot shows a configuration dialog for a lifecycle rule. It has two main sections: 'More than (days ago) \*' (set to 30) and 'Then'. Under 'Then', there are three options: 'Move to cool storage' (selected), 'Move to archive storage', and 'Delete the blob'. Each option has a descriptive subtitle below it.

More than (days ago) *	30
Then	
Move to cool storage	This is the most reliable option if cost is not a concern.
Move to archive storage	Archive storage does not fully delete the blob.
Delete the blob	This is the most efficient option if backing up is not a concern.





# Access Tiers (Blob Storage)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

When a blob is uploaded or moved to another tier  
It's charged at the new tier's rate **immediately** upon tier change.



When moving from a **cooler tier**:

The operation is billed as a **write operation** to the destination tier.

Where the write operation (per 10,000) and data write (per GB) charges of the destination tier apply.



When moving from a **hotter tier**

The operation is billed as a read from the source tier

Where the **read operation** (per 10,000) and data retrieval (per GB) charges of the source tier apply

Early deletion charges for any blob moved out of the cool or archive tier may apply as well

## Cool and archive early deletion

Any blob that is moved into the cool tier (GPv2 accounts only) is subject to a cool early deletion period of 30 days.

Any blob that is moved into the archive tier is subject to an archive early deletion period of 180 days. This charge is prorated.





# Azure Administrator



## Replication Data Redundancy



# Replication and Data Redundancy

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

When you create a Storage Account you need to choose a **Replication Type**

Replication ⓘ

Geo-redundant storage (GRS) ▾



The greater level of redundancy the more expensive the cost of replication



Replication stores multiple copies of your data so that it is **protected from:**

- planned events
- transient hardware failures
- network or power outages
- massive natural disasters

## Primary Region Redundancy

- Locally Redundant Storage (LRS)
- Zone-redundant storage (ZRS)

Disaster Recovery and Failovers

## Secondary Region Redundancy

- Geo redundant storage (GRS)
- Geo-zone-redundant storage (GZRS)

Disaster Recovery and Failovers

## Secondary Region Redundancy with Read Access

- Read-access geo-redundant storage (RA- GRS)
- Read-access geo-redundant storage (RA-GZRS)

Read Replicas





## Azure Administrator



# **Locally redundant storage and Zone-redundant storage**



# Replication and Data Redundancy

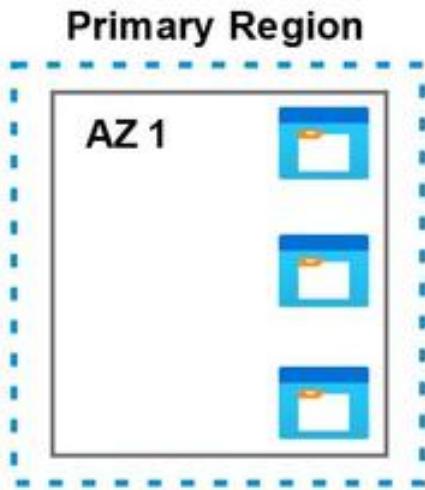
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Redundancy in the Primary Region

- Data is replicated **3 times** in the primary region
- There are **two options** for storing in the primary region

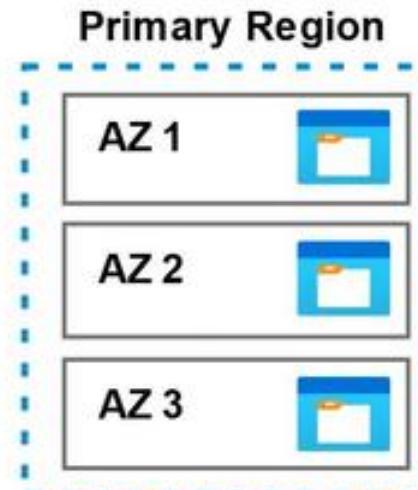
### Locally Redundant Storage (LRS)

- Copies data **synchronously** in primary region
- 99.99999999% (11 nines) durability
- **Cheapest option**



### Zone-redundant storage (ZRS)

- Copies data **synchronously across 3 AZs** in primary region
- 99.999999999% (12 9's) durability





# Azure Administrator



## Geo-Redundant Storage and Geo-Zone-Redundant Storage



# Replication and Data Redundancy

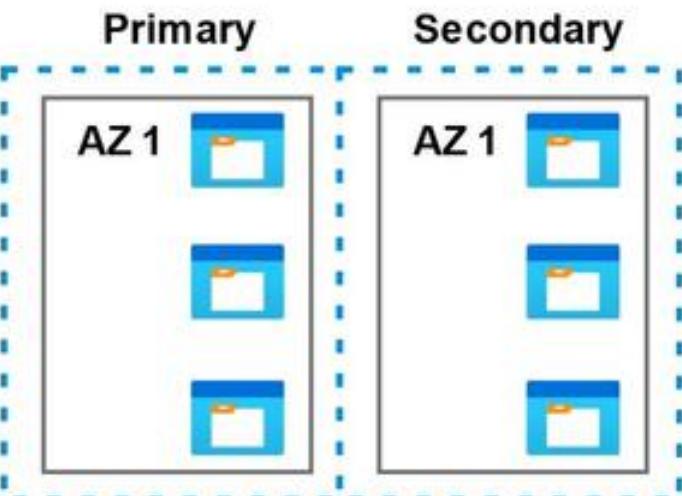
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Redundancy in the Secondary Region

- Replicate to a secondary region in case of primary regional disaster
- The secondary region is determined based on your primary's pair region
- Secondary region isn't available for read or write access (except in event of failover)

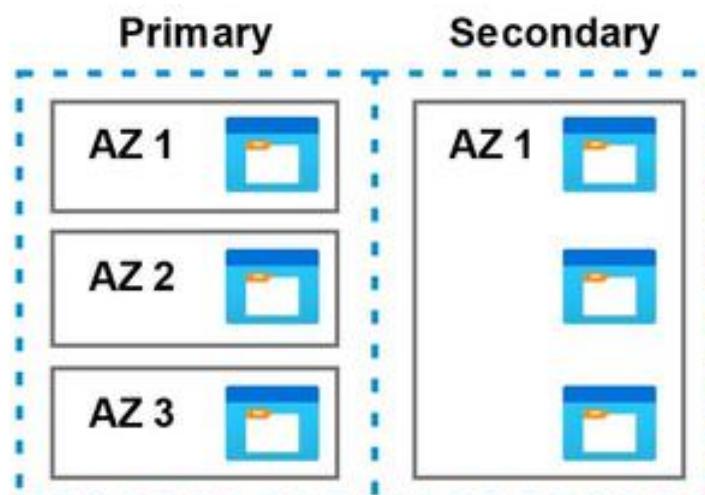
### Geo Redundant Storage (GRS)

- Copies data **synchronously** in primary region
- Copies data **asynchronously** to another region
- 99.999999999999% (16 9's) of durability



### Geo-Zone-redundant storage (GZRS)

- Copies data **synchronously** across 3 AZs in a physical region
- Copies data **asynchronously** to another region
- 99.999999999999% (16 9's) of durability





# Azure Administrator



**Read-Access Geo Redundant Storage and  
Read-Access Geo-Zone-redundant Storage**



# Replication and Data Redundancy

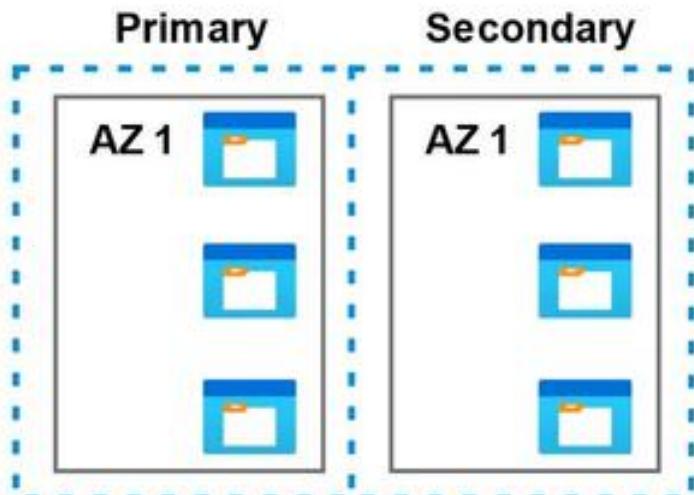
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Redundancy in the Secondary Region with Read Access

- Data is replicated **synchronously** to primary region
- Your data will be “in-sync” with your primary and you’ll have **read access**.

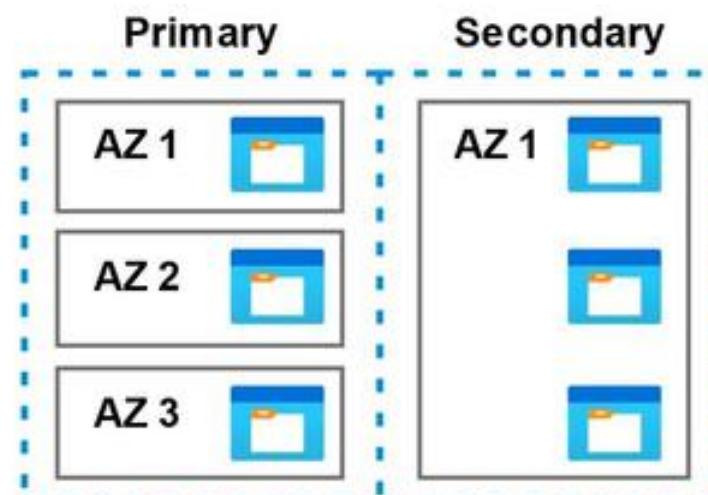
### Read-Access Geo Redundant Storage (RA-GRS)

- Copies data **synchronously** in primary region
- Copies data **synchronously** to another region
- 99.999999999999% (16 9's) of durability



### Read-Access Geo-Zone-redundant storage (RA-GZRS)

- Copies data **synchronously** across 3 AZs in a physical region
- Copies data **synchronously** to another region
- 99.999999999999% (16 9's) of durability





# Azure Administrator



## Introduction to Azure Blob

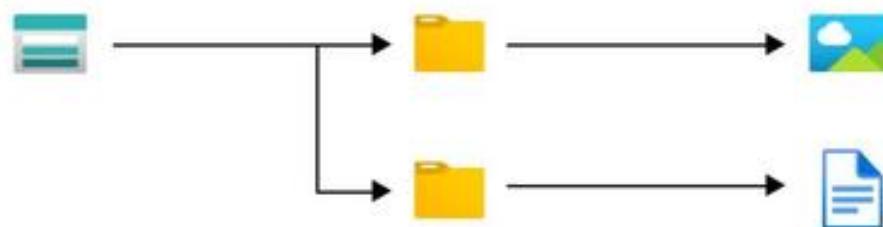


# Azure Blob

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Blob storage is a **object-store** that is optimized for **storing massive amounts of unstructured data**.  
Unstructured data is data that doesn't adhere to a particular data model or definition, such as text or binary data.

Azure Blobs are composed of the components:



Storage Account

Containers

Blobs

a unique namespace in Azure for your data

<http://mystorageaccount.blob.core.windows.net>

similar to a folder in a file system

The actual data being stored





# Azure Administrator



## Azure Blob Types



# Azure Blob

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Storage supports **3 types** of blobs:



## 1. Block blobs

- store text and binary data
- made up of blocks of data that can be managed individually
- store up to about 4.75 TiB of data



## 2. Append blobs

- Optimized for append operations
- ideal for scenarios such as logging data from virtual machine

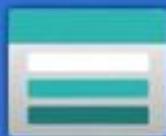


## 3. Page blobs

- store random access files up to 8 TB in size.
- store virtual hard drive (VHD) files and serve as disks for Azure virtual machine



# Azure Administrator



## Azure Blob Moving Data





# Azure Blob

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are **multiple ways** to move data into Azure Blob Storage

<b>AzCopy</b>	Easy-to-use command-line tool for Windows and Linux
<b>Azure Storage Data Movement library</b>	.NET library (uses AzCopy underneath)
<b>Azure Data Factory</b>	An ETL service by Azure
<b>Blobfuse</b>	Virtual file system driver. Access data through Linux file system
<b>Azure Data Box</b>	A rugged device used to physically transport data to Azure
<b>Azure Import/Export service</b>	A service where you ship your physical disks for data transfer onto Azure



# Azure Administrator



## Introduction to Azure Files





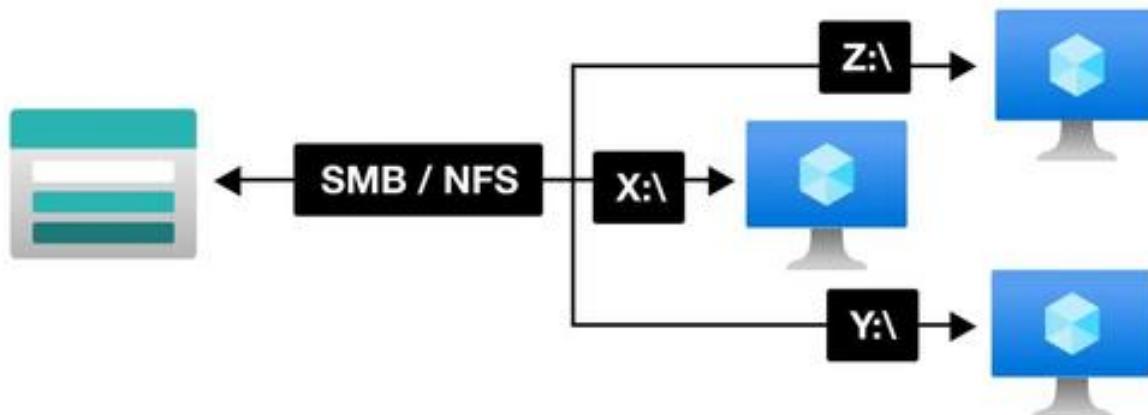
# Azure Files

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Files is a fully managed **file share** in the cloud.

A file share is a **centralized server for storage** that allows **multiple connections**.

*It's like having one big shared drive that everyone (Virtual Machines) can work on at the same time.*



To connect to the file share a **network protocol** is used:

- Server Message Block (SMB)
- Network File System (NFS)

When a connection is established the file share's filesystem will be accessible in the specific directory within your own directory tree. This is known as **mounting**





# Azure Administrator



## Azure Files Use Cases





# Azure Files – Use Cases

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Use Cases

- Completely **replace or supplement** on-premises file servers Network Attach Storage (NAS) devices
- **Lift-and-Shift** your on-premise storage to the cloud via Classic Lift or Hybrid Lift
  - “Lift-and-Shift” means when you move workloads without rearchitecting, eg. importing local VMs to the cloud
  - Classic Lift — where both the application and its data are moved to Azure
  - Hybrid Lift — where the application data is moved to Azure Files, and the application continues to run on-premises
- **Simplify cloud development**
  - Shared application settings — Multiple VMs and developer workstations need to access the same config files.
  - Diagnostic share — All VMs log to the file share, developers can mount and debug all logs in a centralized place
  - Dev/Test/Debug — Quickly share tools for developer needed for local environments
- **Containerization**
  - You can use Azure Files to persist volumes for stateful containers

Why use Azure files instead of setting up your own File Share server?

- **Shared Access** — Already setup to work with standard networking protocols SMB and NFS
- **Fully managed** — Its kept up to date with security patches, designed to scale
- **Scripting and Tooling** — You can automate the management and creation of file shared with Azure API and PowerShell
- **Resiliency** — Built to be durable and always working





# Azure Administrator



## Azure Files Feature





# Azure Files

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Backups

You can backup your file share with **shared snapshots**

- They are read-only
- Incremental (they only contain as much data as has changed since the previous snapshot)
- You can have up to **200 snapshots** per file share
- You can retain backups for **up to 10 years**
- Backups are stored within your file share (if you delete your file share you will delete your backups)

## Soft Delete

You can prevent accidental deletion by turning on Soft Delete (Storage will be marked for deletion and retained for a period of time before final delete occurs)

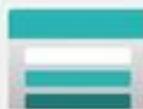
## Advanced Threat Protection (ATP)

An additional layer of security intelligence that provides alerts when it detects anomalous activity on your storage account

## Store Tiers:

- **Premium** — Store on SSD with single-digit milliseconds for most IO operation
- **Transaction optimized** — Store on HDD with transaction heavy workloads that don't need the latency offered by premium file shares (historically this tier has been called **standard**)
- **Hot** — optimized for general purpose file sharing scenarios such as **team shares** and **Azure File Sync**.
- **Cool** — Stored on HDD for cost-efficient storage optimized for online archive storage scenario





# Azure Files

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Types of Storage

- **General purpose version 2 (GPv2)** — deployed on to HDD
- **FileStorage** — deployed onto SSD

## Identity

- **On-Premise:** — Azure Storage can be joined to an on-premise Active Directory Domain Service
- **Managed** — Azure Storage can be joined to Microsoft managed Active Directory Domain Service
- **Store Account Key** — A username (storage account name) and password (account key) can be used to mount

## Networking

- Azure Files are accessible inside or outside your AWS Account from anywhere via storage account **public endpoint**.
- SMB connects to **port 445**, your organization may need to unblock this port so you can mount your file share

## Encryption

- Azure Files is **encrypted-at-rest** using Azure Storage Service Encryption (SSE)
- Azure Files is **encrypted-in-transit** with SMB 3.0+ with encryption or HTTPS





# Azure Administrator



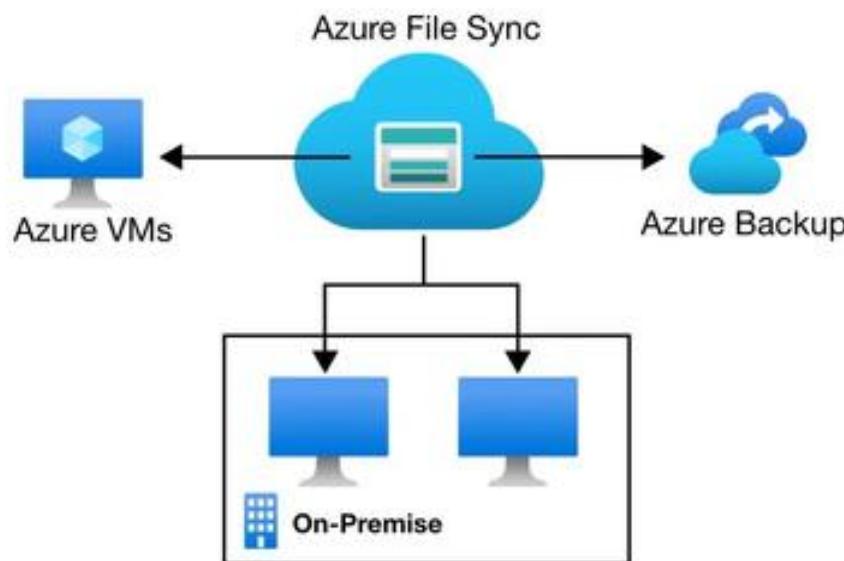
# Azure File Sync



# Azure File Sync

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure File Sync is a service that allows you to **cache** Azure file shares on an **on-premises Windows Server** or **cloud VM**.



- You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS
- You can have as many caches as you need across the world.





# Azure Administrator



# Azure Storage Explorer

(A)  
SUBSCRIBE



# Azure Storage Explorer

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

A **standalone app** that makes it easy to work with Azure Storage data on Windows, macOS, and Linux.  
You can create Blob containers, upload files, create snapshots of Disk, and more!

The screenshot shows the Microsoft Azure Storage Explorer application running on a Mac OS X desktop. The window title is "Microsoft Azure Storage Explorer". The interface has two main panes: an "EXPLORER" pane on the left and a "Details" pane on the right.

**EXPLORER Pane:** This pane displays a hierarchical tree view of storage resources. It includes sections for "Quick Access", "Local & Attached" (which lists "Storage Accounts", "Cosmos DB Accounts (Deprecated)", "Data Lake Storage Gen1 (Preview)", and "Azure subscription 1 (andrew@exampro.co)"), and "Disks" (listing "ExamPro", "NetworkWatcherRG", and "VstsRG-teacherseal-2beb"). Under the "Azure subscription 1" node, there is a "Storage Accounts" section with "exampro32kidsfdisk" listed. Below this, under "exampro32kidsfdisk", there are "Blob Containers" and "myfiles" is selected. Other options like "File Shares", "Queues", and "Tables" are also shown under the storage account.

**Details Pane:** This pane shows a table of "Active blobs (default)" for the "myfiles" container. The table has columns: Name, Access Tier, Access Tier Last Modified, Last Modified, Blob Type, Content Type, Size, Status, Remaining Days, Deleted Time, and L. One row is visible, showing a blob named "choose-carefully.png" with the following details:

Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content Type	Size	Status	Remaining Days	Deleted Time	L
choose-carefully.png	Hot (internet)		11/7/2020, 9:47:07 PM	Block Blob	image/png	415.6 KB	Active			

At the bottom of the Details pane, it says "Showing 1 to 1 of 1 cached items".



# Azure Administrator



# AZCopy



# AZCopy

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

AZCopy is a **command-line utility** that you can use to copy blobs or files to or from a storage account.

## 1. Its an **executable file** you download

### Download AzCopy

First, download the AzCopy V10 executable executable file, so there's nothing to install.

- Windows 64-bit (zip)
- Windows 32-bit (zip)
- Linux x86-64 (tar)
- macOS (zip)

## 2. You will need to have the level of authorization via attached roles:

To download

- Storage Blob Data Reader

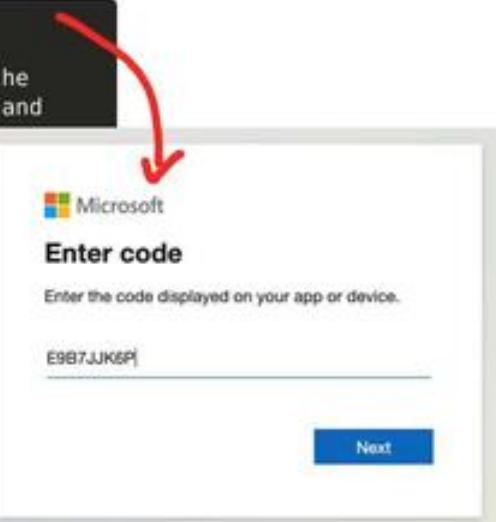
To upload:

- Storage Blob Data Contributor
- Storage Blob Data Owner

## 3. You gain access either via:

1. Azure Active Directory (AD)
2. Shared Access Signature (SAS)

```
~: azcopy login  
To sign in, use a web browser to open the  
page https://microsoft.com/devicelogin and  
enter the code E9B7JK6P to authenticat
```



## 4. Use the Copy command to **upload** and **download**

```
azcopy copy \  
'C:\StarTrek\jodri.txt' \  
'https://enterprise.blob.core.windows.net/mycontainer/jodri.txt'
```

```
azcopy copy \  
'https://enterprise.blob.core.windows.net/mycontainer/jodri.txt' \  
'C:\StarTrek\jodri.txt'
```





# Azure Administrator



# Azure Import Export Service

# Azure Import/Export Service

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Used to securely **import large amounts of data** to Azure Blob storage and Azure Files **by shipping disk drives** to an Azure datacenter.

You have 2 options for shipping drives on import:

- Use your own disk drives
- Use **Microsoft** provided drives



Microsoft ships up to 5 encrypted solid-state disk drives (SSDs) known as **Azure Data Box Disk** with a 40 TB total capacity per order, to your datacenter through a regional carrier.

You can quickly configure **Azure Data Box Disk** drives, copy data to disk drives over a USB 3.0 connection, and ship the disk drives back to Azure.

To prepare your drive you'll need to use the command-line **WAImportExport tool** to

- Prepare your disk drives that are shipped for import.
- Copying your data to the drive.
- Encrypts the data on the drive with AES 256-bit BitLocker.
- Generate the drive **journal files** used during import creation.
- Helps identify numbers of drives needed for export jobs.

There are two versions of **WAImportExport**

- Version 1 for import/export into Azure Blob storage.
- Version 2 for importing data into Azure files.

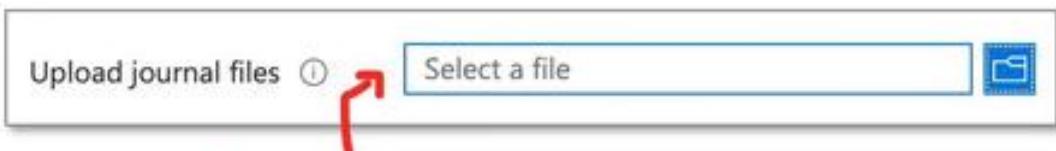
**WAImportExport tool** is only compatible with 64-bit Windows



# Azure Import/Export Service

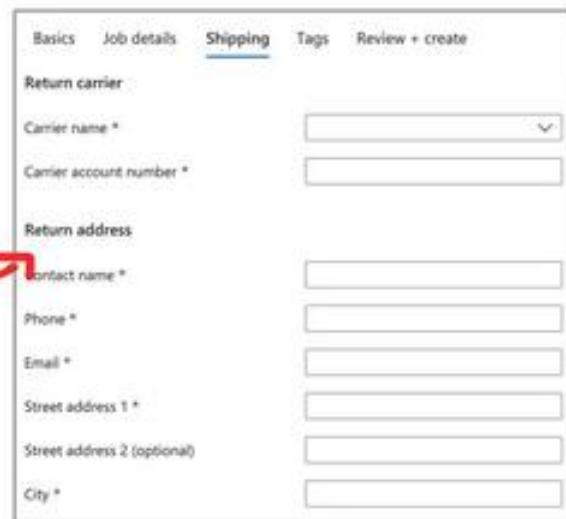
Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Once you have prepared your drives and generated a journal files you can create an Import Job



The **journal file** stores basic information such as:

- drive serial number
- encryption key
- storage account details.
- You'll specify Region and Storage Account
- You'll provide shipping information



The screenshot shows the "Shipping" tab of a form. The tabs at the top are "Basics", "Job details", "Shipping" (which is underlined in blue), "Tags", and "Review + create". Below the tabs are two sections: "Return carrier" and "Return address". The "Return carrier" section contains fields for "Carrier name \*" (with a dropdown arrow) and "Carrier account number" (with an input field). The "Return address" section contains fields for "Contact name \*" (with an input field), "Phone \*" (with an input field), "Email" (with an input field), "Street address 1 \*" (with an input field), "Street address 2 (optional)" (with an input field), and "City \*" (with an input field).

For **export jobs** you:

- You can only export from Azure Blob
- You can ship up to 10 empty drives to Azure per job,
- You create an export job and the data is loaded onto those drives and shipped back to you



# Azure Administrator



# Shared Access Signature

# Shared Access Signatures

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

A shared access signature (SAS) is a URI that grants restricted access rights to **Azure Storage** resources.

Share the URI to grant clients temporary access to specific set of permissions

Types of shared access signatures

## Account-level SAS

- access to resources in **one or more** of the storage services

## Service-level SAS

- access to single the storage account by using the storage account key

## User delegation SAS

- Access to storage account using Azure AD credentials
- Limited only to Blob and Containers
- Microsoft considers this method best practice for accessing via SAS

A shared access signature comes into different formats:

## Ad hoc SAS

- the start time, expiry time, and permissions are part of the URI
- Any type of SAS can be an ad hoc SAS

## Service SAS with stored access policy:

- A stored access policy is defined on a resource container (limited to blob container, table, queue, or file share)
- The stored access policy can be associated to multiple SAS to manage constraints



# Shared Access Signatures

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

The URI Format itself:

- **Blob URI:** <https://myaccount.blob.core.windows.net/mycontainer/myblob.txt>
- **sv (Storage services version)** which version of the storage services to use
- **st (Start Time)** the time the SAS becomes valid
- **se (Expiration Time)** the time when the SAS becomes invalid eg. Container (c) or Blob (b)
- **sr (Storage Resource)** if the resource is a blob, queue
- **sp (Permissions)** what operations can be performed against the storage resource eg. Read (r) and Write (w)
- **sig (Signature)** used to authenticate access a SHA256 algorithm

```
https://myaccount.blob.core.windows.net/mycontainer/myblob.txt  
?sv=2014-02-14  
&st=2014-12-23T22%3A18%3A26Z  
&se=2014-12 23T22%3A23%3A26Z  
&sr=b  
&sp=rw  
&sig=Za7816bf8X01cfea414%40We5dae2Y23b00361a39617%a9c
```



# Shared Access Signatures

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

You can **generate** SAS via

- Azure SDK
- Azure **Portal**



The screenshot shows the 'examprostorageaccount | Shared access signature' configuration page. The left sidebar lists various storage account settings, with 'Shared access signature' currently selected and highlighted. The main pane contains configuration options for generating a SAS token, including:

- Allowed services:** Blob, File, Queue, Table (all checked)
- Allowed resource types:** Service (checked), Container, Object (unchecked)
- Allowed permissions:** Read, Write, Delete, List, Add, Create, Update, Process (all checked)
- Blob versioning permissions:** Enables deletion of versions (checked)
- Start and expiry date/time:** Start: 11/08/2020, End: 11/08/2020, Timezone: (UTC-05:00) Eastern Time (US & Canada)
- Allowed IP addresses:** for example, 168.1.5.65 or 168.1.5.65-168.1.5.70
- Allowed protocols:** HTTPS only (selected)
- Preferred routing tier:** Basic (default) (selected)
- A note: Some routing options are disabled because the endpoints are not published.
- Signing key:** key1
- Generate SAS and connection string** button





# Azure Administrator



## Use AZCopy to copy files to Storage Accounts



### Follow Along

```
Microsoft Azure
Home > MicrosoftStorageAccount-20210410095355 > fajo
fajo | Containers
Storage account
Search (Ctrl+F)
+ Container Change access level
Overview Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events
Name
Kivafajo
Bash
andrew@Azure:~/clouddrive$ ls -la
total 25558
drwxrwxrwx 2 andrew andrew 0 Apr 17 18:42 .
drwxr-xr-x 3 root root 4096 Apr 18 13:54 ..
-rw-rw-r-- 1 andrew andrew 26119314 Apr 18 14:05 azcopy
drwxrwxrwx 2 andrew andrew 0 Apr 17 18:42 .
-rw-rw-r-- 1 andrew andrew 47402 Apr 18 14:04 kivas-fajo.jpg
andrew@Azure:~/clouddrive$ chmod u+x azcopy
andrew@Azure:~/clouddrive$ ls -la
total 25558
drwxrwxrwx 2 andrew andrew 0 Apr 17 18:42 .
drwxr-xr-x 3 root root 4096 Apr 18 13:54 ..
-rw-rw-r-- 1 andrew andrew 26119314 Apr 18 14:05 azcopy
drwxrwxrwx 2 andrew andrew 0 Apr 17 18:42 .
(4) SUBSCRIBE
```



# Azure Administrator



## Create a File Share with Azure Files



Follow Along

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with icons for Home, Compute, Storage, Network, and more. The main area displays the 'kivas' Virtual Machine details. The VM summary shows it's running, located in Central US (Zone 1), part of an Azure subscription, and has an availability zone. Below the summary, there's a 'File' section with a 'Create' button and other options. A terminal window is open at the bottom, showing the following command-line session:

```
kivashell:~$ rm -rf /etc/subcredentials
rm: cannot remove '/etc/subcredentials': Permission denied
kivashell:~$ sudo rm -rf /etc/subcredentials
kivashell:~$ sudo chmod +w /etc/subcredentials
kivashell:~$ sudo bash -c "echo 'username:kivas' >> /etc/subcredentials/kivashell:~$ sudo bash -c "echo 'password=2zdg4t654poy0ifH06sf0NlyGat
kivashell:~$ "
```

At the bottom right of the terminal window, there's a 'WSL UI' icon and a '(A)' icon.



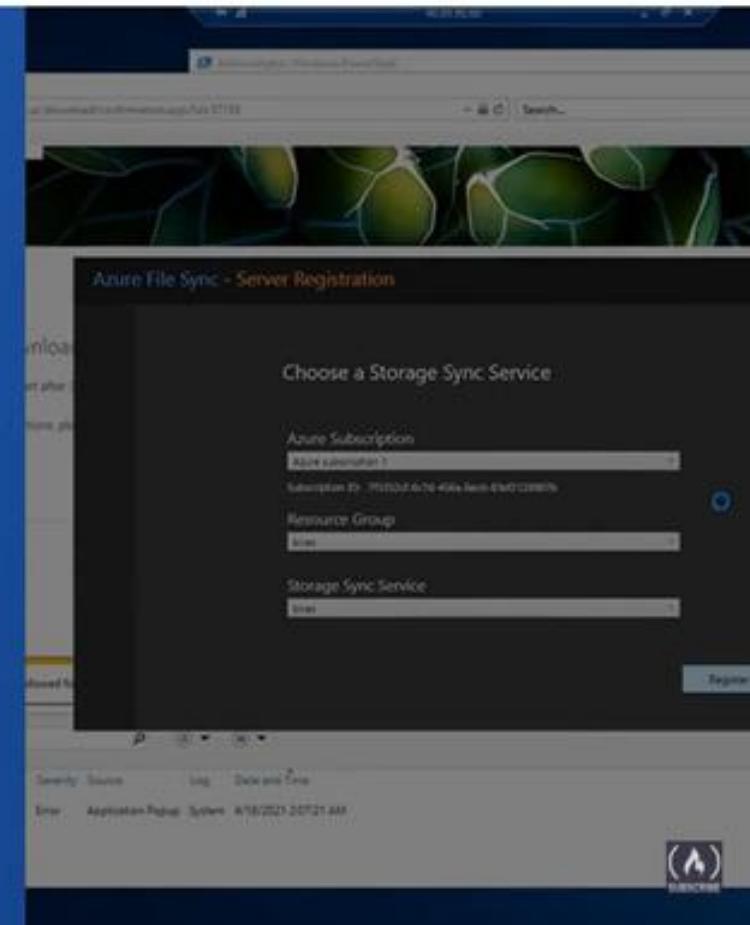
# Azure Administrator



## Setup Azure Files Sync



Follow Along





# Azure Administrator



## Storage Accounts CheatSheet



# Storage Accounts *CheatSheet*

Exam Pro

Azure has 5 core storage services:

1. **Azure Blob** A massively scalable **object store** for text and binary data. Includes support for big data analytics via Data Lake Storage Gen2
2. **Azure Files** Managed **file shares** for cloud or on-premises deployments
3. **Azure Queues** A **NoSQL store** for schemaless storage of structured data.
4. **Azure Tables** A **messaging store** for reliable messaging between application components
5. **Azure Disks** **Block-level storage** volumes for Azure VMs

For Blob Storage there are **2 types** of performance tiers for storage accounts: **Standard** and **Premium**

- **Standard Performance** Stored on Hard Disk Drives (**HDDs**)
- **Premium Performance:** Stored on Solid State Drives (**SSDs**)
  - Varied performance based on access tier (Hot, Cool, Archive)

Azure Storage supports **3 types** of blobs:

1. **Block blobs** store text and binary data, made up of blocks of data that can be managed individually, store up to about 4.75 TiB of data
2. **Append blobs** Optimized for append operations, ideal for scenarios such as logging data from virtual machine
3. **Page blobs** store random access files up to 8 TB in size, store virtual hard drive (VHD) files and serve as disks for Azure virtual machine

For Blob Storage there are **3 types** of access tiers for **Standard storage**: Cool, Hot and Archive

- **Hot** Data that's accessed frequently. Highest storage cost, lowest access cost
- **Cool** Data that's infrequently accessed and stored for at least 30 days., Lower storage cost, higher access cost
- **Archive** Data that's rarely accessed and stored for at least 180 days. Lowest storage cost, highest access cost

**Account Level Tiering** Any blob that doesn't have an explicitly assigned tier infers the tier from the Storage Account access tier setting.

**Blob-Level Tiering** You can upload a blob to the tier of your choice. Changing tiers happens instantly except when moving out of archive

**Rehydrating a Blob** When moving a blob out of archive into another tier it can take several hours. This is known as "**rehydrating**"



# Storage Accounts *CheatSheet*



**Blob Lifecycle Management** You can create rule-based policies to transition data to different tiers Eg. After 30 days move to cool storage When a blob is uploaded or moved to another tier. It's charged at the new tier's rate **immediately** upon tier change.

When moving from a **cooler tier**:

- The operation is billed as a **write operation** to the destination tier.
- Where the write operation (per 10,000) and data write (per GB) charges of the destination tier apply.

When moving from a **hotter tier**

- The operation is billed as a read from the source tier
- Where the **read operation** (per 10,000) and data retrieval (per GB) charges of the source tier apply
- Early deletion charges for any blob moved out of the cool or archive tier may apply as well

**Cool and archive early deletion**

- Any blob that is moved into the cool tier (GPv2 accounts only) is subject to a cool early deletion period of 30 days.
- Any blob that is moved into the archive tier is subject to an archive early deletion period of 180 days. This charge is prorated.

There are **multiple ways** to move data into Azure Blob Storage:

- |  |   |
|--|---|
| • <b>AzCopy</b>                              | Easy-to-use command-line tool for Windows and Linux                       |
| • <b>Azure Storage Data Movement library</b> | .NET library (uses AzCopy underneath)                                     |
| • <b>Azure Data Factory</b>                  | An ETL service by Azure   |
| • <b>Blobfuse</b>                            | Virtual file system driver. Access data through Linux file system         |
| • <b>Azure Data Box</b>                      | A rugged device used to physically transport data to Azure                |
| • <b>Azure Import/Export service</b>         | A service where you ship your physical disks for data transfer onto Azure |



# Storage Accounts *CheatSheet*



When you create a Storage Account you need to choose a **Replication Type**

## Primary Region Redundancy (Disaster Recovery and Failovers)

- Locally Redundant Storage (LRS)
  - Copies data **synchronously** in primary region
  - **Cheapest option**
- Zone-redundant storage (ZRS)
  - Copies data **synchronously across 3 AZs** in primary region

## Secondary Region Redundancy (Disaster Recovery and Failovers)

- Geo redundant storage (GRS)
  - Copies data **synchronously** in primary region
  - Copies data **asynchronously** to another region
- Geo-zone-redundant storage (GZRS)
  - Copies data **synchronously across 3 AZs** in a physical region
  - Copies data **asynchronously** to another region

## Secondary Region Redundancy with Read Access (Read Replicas)

- Read-access geo-redundant storage (RA- GRS)
  - Copies data **synchronously** in primary region
  - Copies data **synchronously** to another region
- Read-access geo-redundant storage (RA-GZRS)
  - Copies data **synchronously** in primary region
  - Copies data **synchronously** to another region



# Storage Accounts *CheatSheet*

Exam Pro

Azure Files is a fully managed **file share** in the cloud. A file share is a **centralized server for storage** that allows **multiple connections**.

To connect to the file share a **network protocol** is used: Server Message Block (SMB), Network File System (NFS)

When a connection is established the file share's filesystem will be accessible in the specific directory within your own directory tree.

- This is known as **mounting**

You can backup your file share with **shared snapshots**

- read-only, Incremental, up to **200 snapshots** per file share, retain backups for **up to 10 years**
- Backups are stored within your file share (if you delete your file share you will delete your backups)

**Soft Delete** prevent accidental deletion by turning on Soft Delete (marked for deletion, retained for a period of time before final delete occurs)

**Store Tiers:**

- **Premium** — Store on to SSD with single-digit milliseconds for most IO operation
- **Transaction optimized** — Store on HDD with transaction heavy workloads that don't need the latency offered by premium file shares (historically this tier has been called **standard**)
- **Hot** — optimized for general purpose file sharing scenarios such as **team shares** and **Azure File Sync**.
- **Cool** — Stored on HDD for cost-efficient storage optimized for online archive storage scenario

**Types of Storage:** General purpose version 2 (GPv2) — deployed on to HDD and **FileStorage** — deployed onto SSD

**Identity:** On-Premise or Managed via AD DS or **Store Account Key** username (storage account name) and password (account key)

Azure Files are accessible inside or outside your AWS Account from anywhere via storage account **public endpoint**.

- SMB connects to **port 445**, your organization may need to unblock this port so you can mount your file share

**Encryption**

- Azure Files is **encrypted-at-rest** using Azure Storage Service Encryption (SSE)
- Azure Files is **encrypted-in-transit** with SMB 3.0+ with encryption or HTTPS

**Azure File Sync** is a service that allows you to **cache** Azure file shares on an **on-premises Windows Server** or **cloud VM**.



# Storage Accounts *CheatSheet*



**Azure Import/Export Service** is used to securely import large amounts of data to Azure Blob Storage and Azure Files

- You have 2 options for shipping drives on import:
  - Use your own disk drives
  - Use **Microsoft** provided drives
- Microsoft ships up to 5 encrypted solid-state disk drives (SSDs) known as **Azure Data Box Disk** with a 40 TB total capacity per order, to your datacenter through a regional carrier

To prepare you drive you'll need the to use the command-line **WAImportExport** tool to

- Prepare your disk drives that are shipped for import.
- Copying your data to the drive.
- Encrypts the data on the drive with AES 256-bit BitLocker.
- Generate the drive journal files used during import creation.
- Helps identify numbers of drives needed for export jobs

There are two version of **WAImportExport**

- Version 1 for import/export into Azure Blob storage.
- Version 2 for importing data into Azure files.

**WAImportExport** tool is only compatible with 64-bit Windows

For **export** jobs you:

- You can only export from Azure Blob
- You can ship up to 10 empty drives to Azure per job,
- You create an export job and the data is loaded onto those drives and shipped back to you



# Storage Accounts *CheatSheet*



A shared access signature (SAS) is a URI that grants restricted access rights to **Azure Storage** resources.

Share the URI to grant clients temporary access to specific set of permissions

Types of shared access signatures

## Account-level SAS

- access to resources in **one or more** of the storage services

## Service-level SAS

- access to single the storage account by using the storage account key

## User delegation SAS

- Access to storage account using Azure AD credentials
- Limited only to Blob and Containers
- Microsoft considers this method best practice for accessing via SAS

A shared access signature comes into different formats:

## Ad hoc SAS

- the start time, expiry time, and permissions are part of the URI
- Any type of SAS can be an ad hoc SAS

## Service SAS with stored access policy:

- A stored access policy is defined on a resource container (limited to blob container, table, queue, or file share)
- The stored access policy can be associated to multiple SAS to manage constraints



# Azure Administrator



## Introduction to Virtual Machine



Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure Virtual Machines



Choose an OS, Compute, Memory and Storage  
and launch a **server** in minutes



# Introduction to Azure VMs

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Virtual Machines (VMs) is a highly configurable server.

Virtualization let you run a server **without having to buy and maintain the physical hardware** that runs it



Virtual Machines still require maintenance such as:

- applying OS system patches
- Installing and configuring packages

## Some things you should know:

- The **size** of the virtual machine is determined by the Image
  - The image defines the combination of vCPUs, Memory and Storage Capacity
- The current limit on a per subscription basis is **20 VMs per region**.
- Azure VMs are billed at an **hourly rate**
- A single instance VMs has an availability of 99.9% (when all storage disks are premium)
- Two instances deployed in Availability Set will give you 99.95% availability
- You can attach multiple Managed Disk to your Azure VMs

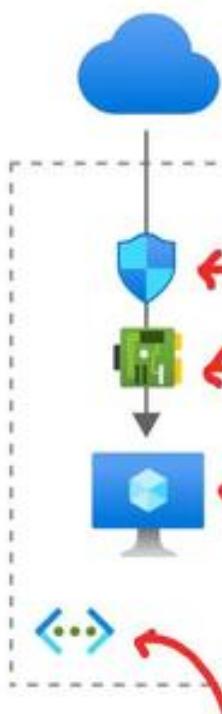




# Introduction to Azure VMs

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

When you **launch** an Azure Virtual Machine other networking components will be either created or associated to your Virtual Machine.



- Network Security Group (NSG)** — attached to the NIC, virtual firewall with rules around ports and protocols
- Network Interface (NIC)** — a device that handle ip protocols and network communication
- Virtual Machine instance** — The actual running server
- Public IP Address** — The address that you will use publicly access your VM

**Virtual Network (VNet)** — The network where your VM will reside

Resource	Type	Status	Operation details
MyNewVirtualMachine	Microsoft.Compute/virtualMachines	OK	<a href="#">Operation details</a>
mynewvirtualmachine839	Microsoft.Network/networkInterfaces	Created	<a href="#">Operation details</a>
MyNewVirtualMachine_group-vnet	Microsoft.Network/virtualNetworks	OK	<a href="#">Operation details</a>
MyNewVirtualMachine-nsg	Microsoft.Network/networkSecurityGroups	OK	<a href="#">Operation details</a>
MyNewVirtualMachine-ip	Microsoft.Network/publicIpAddresses	OK	<a href="#">Operation details</a>





# Azure Administrator



## VM Operation Systems



# Azure VMs – Operation Systems

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is an Operation System (OS)?

The OS is the program that manages all other programs in a computer.

The most commonly known operations systems are Windows ,macOS, and Linux



When you launch a Virtual Machine you need to choose an Image which has a specific Operation System.

Microsoft works closely with partners to ensure the images available are updated and optimized for an Azure runtime. Most of these images can be found in the **Azure Marketplace**



- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux
- Ubuntu Server
- Debian
- FreeBSD
- Azure Marketplace - Flatcar Container Linux
- RancherOS
- Bitnami Library for Azure
- Mesosphere DC/OS on Azure
- Docker images
- CloudBees Jenkins Platform



You can **Bring Your Own Linux** by creating a Linux Virtual Hard Disk (VHD)

*(Hyper-V virtual hard disk (VHDX) format isn't supported in Azure, only fixed VHD)*





# Azure Administrator



## Cloud Init



# Cloud-Init

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Cloud-init** is the industry standard multi-distribution method for cross-platform **cloud instance initialization**. It is supported across all major public cloud providers, provisioning systems for private cloud infrastructure, and bare-metal installations.

## What is Cloud Instance Initialization?

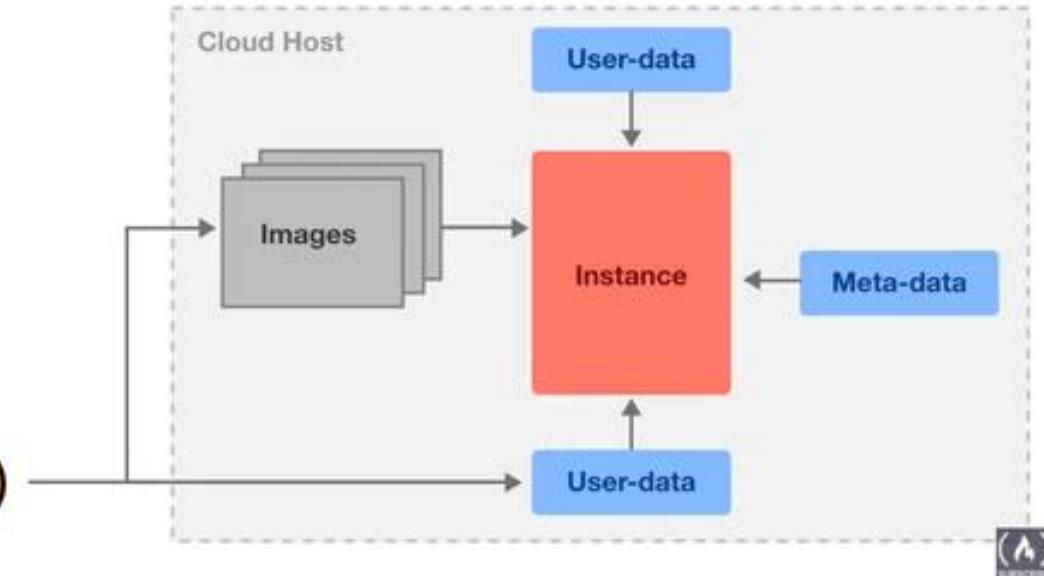
The process of preparing an instance with configuration data for the operation system and runtime environment.

Cloud instances are initialized from a disk image and instance data:

- Meta-data
- **User-data**
- Vendor-data

**User Data** is a script that you want to run when an instance first boots up. eg. Install Apache web-server

Azure Virtual Machines supports for cloud-init across most Linux Distros that support it.





# Azure VMs – Sizes

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure VMs come in a variety of sizes that are also optimized for specific use cases.

Azure VMs are grouped into:

- **Types** eg. General Purposes, Compute Optimized
- **Sizes** eg . B, Dsv3 (also called Series or SKU Family)

**General Purpose** Balanced CPU-to-Memory ratio. Testing and development, small to medium databases, and low to medium traffic web servers.

SKUs: B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dv4, Dsv4, Ddv4, Ddsv4

**Compute Optimized** High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and app servers.

SKUs: F, Fs, Fsv2

**Memory Optimized** High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics

SKUs: Esv3, Ev3, Easv4, Eav4, Ev4, Esv4, Edv4, Edsv4, Mv2, M, DSv2, Dv2

**Storage Optimized** High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.

SKUs: Lsv2

**GPU** Specialized VMs for heavy graphic rendering and video editing, model training and inferencing (ND) with deep learning.

Available with single or multiple GPUs.

SKUs: NC, NCv2, NCv3, NCasT4\_v3 (Preview), ND, NDv2 (Preview), NV, NVv3, NVv4

**High performance compute** Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

SKUs: HB, HBv2, HC, H

*There are previous series of Virtual Machines sizes not shown here like Basic A*





# Azure VMs – Sizes

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

The type of image may limit you to specific VM sizes

Image \*

Ubuntu Server 18.04 LTS - Gen1

Browse all public and private images

Size \*

Standard\_B1s - 1 vcpu, 1 GiB memory (CA\$9.72/month)

Select size

You can explore sizes and then sort and filter based on a variety of options such as **cost**

Showing 375 VM sizes.   Subscription: Azure subscription 1   Region: East US   Current size: Standard_B1s   Image: Ubuntu Server 18.04 LTS   <a href="#">Learn more about VM sizes</a>									
VM Size ↑↓	Family ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Temp storage (GiB) ↑↓	Premium disk ↑↓	Cost/month ↑↓	
Most used by Azure users									
DS1_v2	General purpose	1	3.5	4	3200	7	Supported	CA\$68.21	
D2s_v3	General purpose	2	8	4	3200	16	Supported	CA\$89.70	
B2s	General purpose	2	4	4	1280	8	Supported	CA\$38.87	
<b>B1s </b>	General purpose	1	1	2	320	4	Supported	CA\$9.72	
B2ms	General purpose	2	8	4	1920	16	Supported	CA\$77.74	
B1ms	General purpose	1	2	2	640	4	Supported	CA\$19.34	
B1ls	General purpose	1	0.5	2	160	4	Supported	CA\$4.86	
DS2_v2	General purpose	2	7	8	6400	14	Supported	CA\$136.42	
B4ms	General purpose	4	16	8	2880	32	Supported	CA\$155.11	
D4s_v3	General purpose	4	16	8	6400	32	Supported	CA\$179.40	
DS3_v2	General purpose	4	14	16	12800	28	Supported	CA\$273.78	
D8s_v3	General purpose	8	32	16	12800	64	Supported	CA\$358.81	





# Azure Administrator



# Azure Compute Unit



# Azure Compute Units

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Azure Compute Unit (ACU)** provides a way of comparing compute (CPU) performance across Azure SKUs.

ACU is currently standardized on a **Small (Standard\_A1)** VM with the value of **100**

All other SKUs then represent approximately how much faster that SKU can run a standard benchmark

SKU Family	ACU / vCPU	vCPU : Core
A1 – A4	100	1:1
D1 - D14	160 - 250	1:1



D1-d14 are **60% to 150%** more performant than the A1-A4





# Azure Administrator



# VM MobileApp

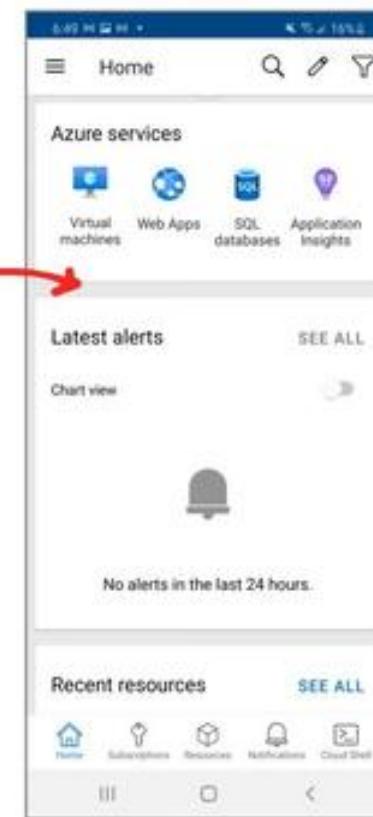
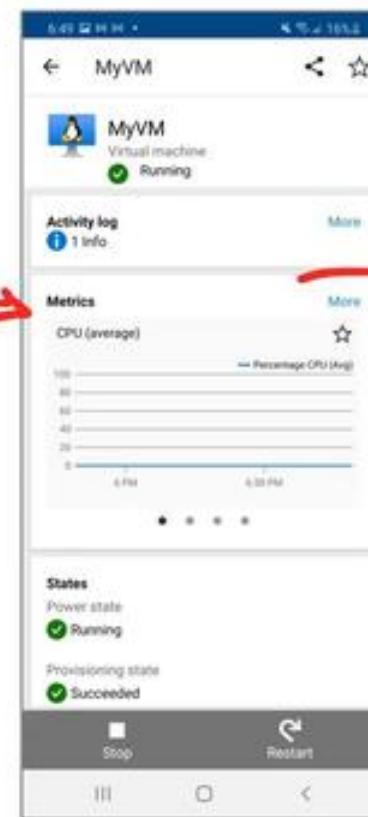




# Monitor VMs via Azure Mobile App

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

You can install the **Azure Mobile App**, and you can monitor your VMs on the go.





# Azure Administrator



## VM Generations





# Hyper-V and Generation 1 vs 2

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)



Hyper-V is Microsoft's **hardware virtualization product**.

It lets you **create and run a software version of a computer**, called a *virtual machine*

Each virtual machine acts like a complete computer, running an operating system and programs.



Hyper-V is just like Virtual Box

There are two generations of Hyper-V VMs:

**Generation 1** - support most guest operating systems

**Generation 2** - support most 64-bit versions of Windows and more current versions of Linux and FreeBSD operating systems

Azure has Generation 1 and Generation 2 VMs which are similar **but not exactly the same** as Hyper-V Generations

The most important difference between Azure Gen 1 and Gen 2:

Gen 1

- **BIOS-based** architecture

Gen 2

- **UEFI-based** boot architecture (improved boot and installation times)
- Secure Boot verifies the boot loader is signed by a trusted authority
- Larger boot volume up to 64 TB

Hyper-V VMs are packaged into Virtual Hard Disk formats: VHD or VHDX files





# Azure Administrator



## 3 Ways To Connect via SSH, RPD, Bastion





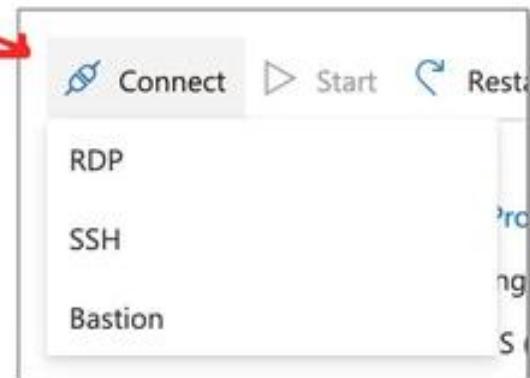
# SSH, RDP and Bastions

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are **3 ways to connect** to your **Virtual Machines**

**Secure Shell (SSH)** is a protocol to establish a secure connection between a client and server.

- This is how you can remotely connect to your Azure VM via terminal
- SSH happens on Port 22 via TCP
- RSA Key Pairs are commonly used to authorize access



**Remote Desktop Protocol (RDP)** is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.

- This is how you can remotely connect to Windows Server via Visual Desktop
- RDP happens on Port 3389 via TCP and UDP

## Bastion

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. It provides **secure** and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. A bastion is a hardened instance that is monitored. Users connect to this VM which then establishes a connection to the target instance. Sometimes known as jump box since you have one extra security step.





# Azure Administrator



## Secure Shell Protocol





# Secure Shell (SSH)

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

It is very common to use **SSH key pairs** as a mean to authenticate to your VMs.

**SSH Key Pairs** is when you **generate out** two keys:

- A Private Key
- A Public Key

The private key should remain on your local system and not be shared with others.

The public key is stored on VM.

**When you go to SSH** you provide your private key and its matched against the public key to authenticate you.

```
~> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/data/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/data/.ssh/id_rsa.
Your public key has been saved in /home/data/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:Up6KjbnEV4Hgfo75YM393QdQsK3Z0aTNBz0DoirrW+c data@yar
The key's randomart image is:
+---[RSA 2048]---+
| .. .oo.. |
| . . . . o.X. |
| . . o. ..+ B |
| . o.o .+ ... |
| ..o.S o.. |
| . %o= . |
| @.B... . |
| o.=. o . . . |
| .oo E. . . . |
+---[SHA256]---+
```

```
ssh -i ~/.ssh/id_rsa.pub azureuser@10.111.12.123
```





# Azure Administrator



# Remote Desktop Protocol



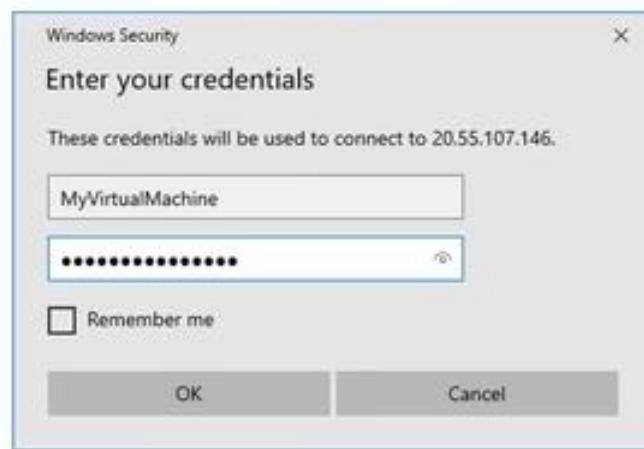
# Remote Desktop Protocol (RDP)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

In order to RDP into your Windows Server you'll need to **download the RDP file.**

The Remote Desktop Client is already installed in Windows 10.

If you are macOS you can download the Microsoft Remote Desktop From the Apple Store.



RDP    SSH    BASTION

Connect with RDP

IP address \*

Public IP address (20.55.107.146) ▾

Port number \*

3389

**Download RDP File**

MyWindowsVM.rdp

Once you open the RDP file you will use the Username and Password during the creation of your VM in the Azure Portal





# Azure Administrator



# Azure Bastion





# Azure Bastion

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Bastion is an **intermediate hardened instance** you can use to connect to your target server via SSH or RDP  
It will provision a web-based RDP client or SSH Terminal

**Some devices cannot run an RDP Client such as Google Chromebook**  
and so Azure Bastion is one of the only ways to allow you to do that

When you create an Azure Bastion  
You need to add a Subnet to your VNet  
called **AzureBastionSubnet** with at least a  
size of /27 (32 addresses)



The screenshot shows the 'Address space' and 'Subnets' sections of the Azure portal. In the 'Address space' section, a checkbox for '10.2.0.0/27' is selected, highlighted with a purple border and a checkmark. In the 'Subnets' section, a new subnet is being created with the name 'AzureBastionSubnet' and the address range '10.2.0.0/27', also highlighted with a purple border and a checkmark.

Address range	Addresses
<input type="checkbox"/> 10.1.0.0/16	10.1.0.0 - 10.1.255.255 (65536 addresses)
<input checked="" type="checkbox"/> 10.2.0.0/27	10.2.0.0 - 10.2.0.31 (32 addresses)

Subnet name	Address range
<input type="checkbox"/> default	10.1.0.0/24
<input type="checkbox"/> AzureBastionSubnet	10.2.0.0/27





# Azure Bastion

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

If you have a Windows Server which requires RDP, and have a Bastion in the same VNet  
You just enter in your Username and Password as you normally would

**Connect using Azure Bastion**  
Azure Bastion Service enables you to securely and seamlessly RDP & SSH to your VMs from the Azure portal, without the need of any additional client/agent or any piece of software. [Learn more](#)

Using Bastion: **MyBastion**, Provisioning State: **Succeeded**

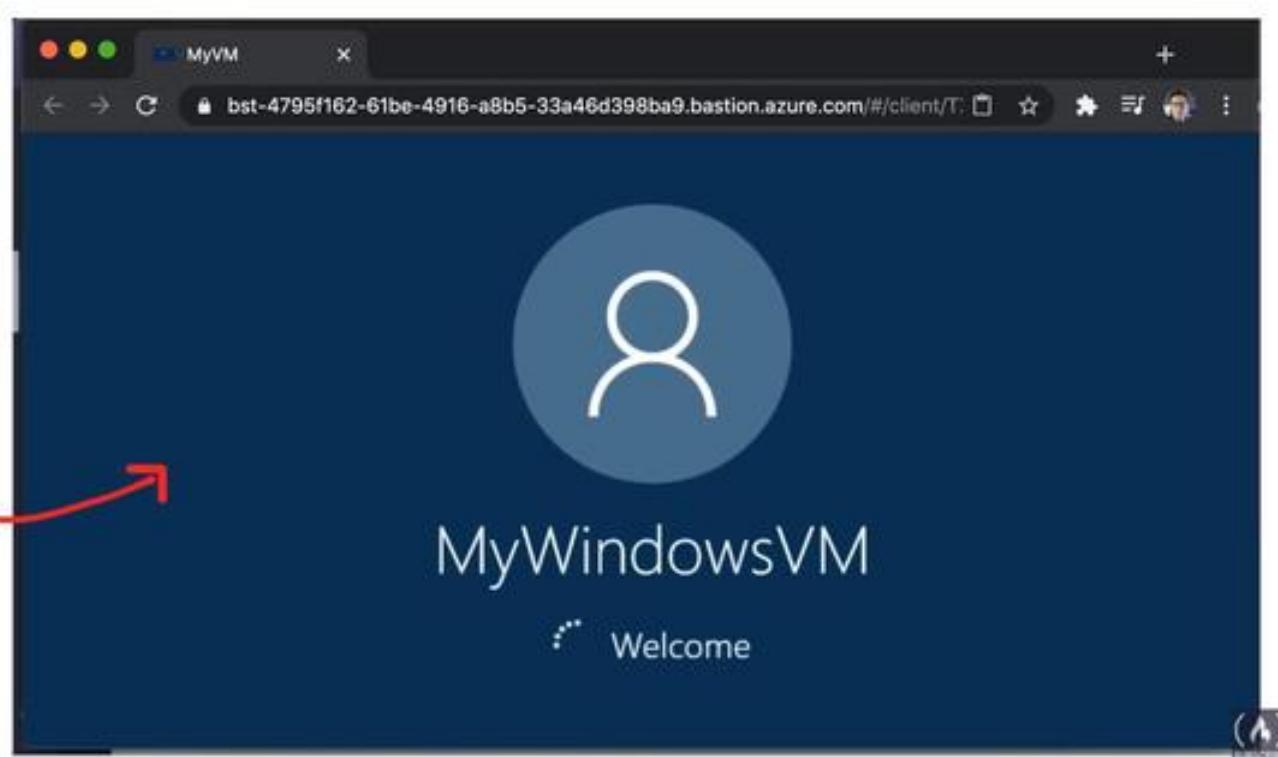
Please enter username and password to your virtual machine to connect using Bastion.

Open in new window

Username \*

Password \*

**Connect**





# Azure Bastion

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

If you have a Linux server you can SSH with the Bastion.

You can use SSH Private Key or Password that you set when you created your VM

**Connect using Azure Bastion**  
Azure Bastion Service enables you to securely and seamlessly RDP exposing a public IP on the VM, directly from the Azure portal, without software. [Learn more about Azure Bastion](#).

Open in new window

Username \*

Authentication Type \*   
 Password  SSH Private Key  SSH Private Key from Local File

Local File \*

Advanced

**Connect**

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1031-azure x86\_64)

\* Documentation: <https://help.ubuntu.com>  
\* Management: <https://landscape.canonical.com>  
\* Support: <https://ubuntu.com/advantage>

System information as of Thu Nov 12 21:27:05 UTC 2020

System load: 0.18	Processes: 116
Usage of /: 4.5% of 28.90GB	Users logged in: 0
Memory usage: 20%	IP address for eth0: 10.1.0.6
Swap usage: 0%	

0 packages can be updated.  
0 updates are security updates.

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/\*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo\_root" for details.

MyWindowsVM@MyVM:~\$



# Azure Administrator



## Windows Vs Linux





# Windows vs Linux Servers

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

You can launch both **Windows and Linux** services on Azure VMs



## Windows

- You need a Windows License (or your Windows account with by unactivated)
- You can bring your own license via Hybrid License
- You set a user name and password
- You have to use a much larger instances to run Windows at least a B2
- It's a full desktop environments



## Linux

- Most versions of Linux require no type of license.
- You set either a username and password or create an ssh-key pair
- You can utilize smaller VM sizes because you're not running a full desktop experience
- Unix and Linux based system traditionally are terminal based environments





# Azure Administrator



## Update Management





# Update Management

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Update Management** allows you to **manage and install operating system updates and patches** for both **Windows** and **Linux** virtual machines that are deployed in Azure, on-premises, or in other cloud providers

When you launch an Azure VM you can go to **Operations** and turn on **Guest + Host Updates**. This will install the Microsoft Monitoring Agent (MMA) that will be used to monitor your instances

The screenshot shows the Azure portal's 'Operations' blade. On the left, there is a list of services: Bastion, Auto-shutdown, Backup, Disaster recovery, and Guest + host updates. The 'Guest + host updates' item is highlighted with a red arrow pointing to the right. On the right, a separate window titled 'Guest OS updates' is open, showing the 'Update management' section. It includes a brief description: 'Update management in Azure Automation machines. You can quickly assess the for your servers.' followed by a 'Learn more' link and a 'Go to Update management' button.



Azure Automations is the underlying service that is installed the agent.

- Update Management will perform a scan for update compliance
- A compliance scan is by default, **performed every 12 hours** on a **Windows** and **every 3 hours** on a **Linux**
- It can take between **30 minutes and 6 hours** for the dashboard to display updated data from managed computers.



In Azure Automation, you can enable the Update Management, Change Tracking and Inventory, and Start/Stop VMs during off-hours features for your servers and virtual machines. These features have a dependency on a **Log Analytics** workspace, and therefore require linking the workspace with an Automation account.





# Azure Administrator

Availability Follow Along



## Create a Bastion



**Follow Along**

The screenshot shows the Azure portal interface. At the top, there's a search bar and a navigation bar with 'Virtual Machines' selected. Below that, a list item for 'WindowsServer-2011-20210321114643' is shown under the 'enterprise-d' category. A note says 'To improve security, enable just-in-time access on this VM.' Below this, there are tabs for 'SSH' and 'BASTION'. Under the 'BASTION' tab, there's a section titled 'Connect with RDP' with fields for 'Address' (public IP address 20.83.48.58) and 'Port number'. A progress bar indicates 'Configuring remote session...'. At the bottom, there are buttons for 'download RDP File' and 'connect!', along with links for 'Test your connection' and 'Troubleshoot RDP connectivity issues'. In the bottom right corner, there's a '(A)' icon with the word 'SUBSCRIBE'.



# Azure Administrator

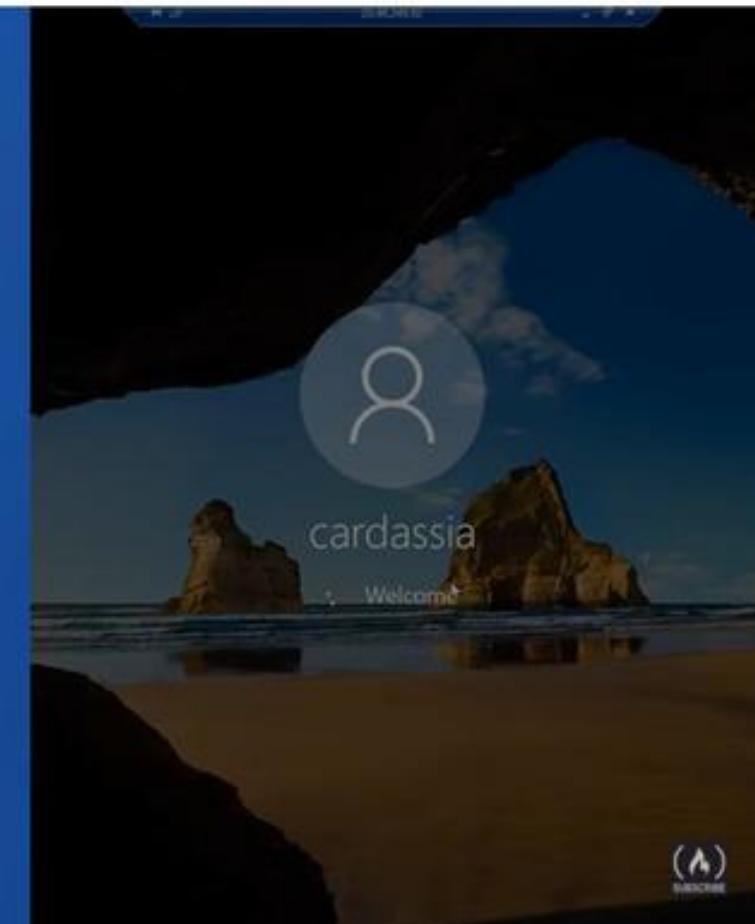
Availability Follow Along



## Create a Windows VM and RDP



### Follow Along





# Azure Administrator

Availability Follow Along



## Create a Linux VM and SSH



Follow Along

Microsoft Azure     ⓘ Search resources, services, and docs (24)

Home > Virtual machines > Create a virtual machine >

### Select a VM size

Search by VM size...     Display cost: Monthly     vCPUs: All     RAM (GB): All

Showing 215 VM sizes     Subscription: Azure subscription 1     Region: Central US     Current

VM Size	Family	vCPUs	RAM (GB)
D11_v2	General purpose	1	3.5
D2s_v3	General purpose	2	8
D2s	General purpose	2	4
D1s	General purpose	1	1
B2ms	General purpose	2	8
B1ms	General purpose	1	2
B1s	General purpose	1	0.5
D52s_v2	General purpose	2	7
B4ms	General purpose	4	16
D4s_v3	General purpose	4	16
D52s_v2	General purpose	4	14
D8s_v3	General purpose	8	32

Most used by Azure users     The most used sizes by users in Az

> D-Series v4     The latest generation D family sizes

Select     Prices presented are estimates in your local currency that include only Azure product costs. Learn more



# Azure Administrator

Availability Follow Along



## Follow Along VM Monitoring



Follow Along

Search resources, services, and data across your Azure environment

jadzia-dax | Configuration management (Preview) - Virtual machine

Properties

Lock

Operations

- Actions
- Auto-shutdown
- Backup
- Disaster recovery
- Guest + host updates
- Inventory
- Change tracking
- Configuration management (Preview)
- Policies
- Run command

Monitoring

- Insights
- Alerts
- Metrics
- Diagnostic settings
- Logs

Enable commitment control and compliance of this VM with Configuration.

This service is included with Azure virtual machines and Azure DevTest Labs. You only pay for logs stored in Log Analytics.

This service requires a Log Analytics workspace and an Automation account. You can use your existing workspace and account or let us create a new workspace and account for use.

Log Analytics workspace location: East US 2

Log Analytics workspace: Workspace-c72bc342-7d94-4...

Automation account subscription: Azure Automation 3

Automation account: Automation 3

(A) SUBSCRIBE



# Azure Administrator



## VM CheatSheets



# Virtual Machines *CheatSheet*



Azure Virtual Machines (VMs) allows you to create Linux and Windows virtual machines

The size of the virtual machine is determined by the Image

- The image defines the combination of vCPUs, Memory and Storage Capacity

The current limit on a per subscription basis is **20 VMs per region**.

Azure VMs are billed at an **hourly rate**

A single instance VMs has an availability of 99.9% (when all storage disks are premium)

Two instances deployed in Availability Set will give you 99.95% availability

You can attach multiple Managed Disk to your Azure VMs

When you *launch* an Azure Virtual Machine other networking components will be either created or associated to your Virtual Machine.

- Network Security Group (NSG), Network Interface (NIC), Public IP Address, VNet

You can **Bring Your Own Linux** by creating a Linux Virtual Hard Disk (VHD)

Azure VMs come in a variety of sizes that are also optimized for specific use cases.

- **General Purpose , Compute Optimized, Memory Optimized, Storage Optimized, GPU, High performance compute**

Azure Compute Unit (ACU) provides a way of comparing compute (CPU) performance across Azure SKUs.

ACU is currently standardized on a **Small (Standard\_A1)** VM with the value of **100**

All other SKUs then represent approximately how much faster that SKU can run a standard benchmark

You can install the **Azure Mobile App**, and you can monitor your VMs on the go.

Hyper-V is Microsoft's **hardware virtualization product**.

- It lets you **create and run a software version of a computer**, called a *virtual machine*

There are two generations of Hyper-V VMs:

**Generation 1** - support most guest operating systems

**Generation 2** - support most 64-bit versions of Windows and more current versions of Linux and FreeBSD operating systems

Hyper-V VMs are packaged into Virtual Hard Disk formats: VHD or VHDX files



# Virtual Machines *CheatSheet*

Exam Pro

There are **3 ways to connect** to your Virtual Machines

**Sure Shell (SSH)** to connect via a terminal or SSH client eg. PuTTY

- SSH happens on **Port 22** via TCP
- RSA Key Pairs are commonly used to authorize access

**Remote Desktop Protocol (RDP)** a graphical interface to connect to another computer over a network connection

- This is how you can remotely connect to Windows Server via Virtual Desktop
- RDP happens on **Port 3389** via TCP and UDP

**Azure Bastion** a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal

- Supports both SSH or RDP, useful when you only have browser like a chromebook, or do not have permission to configure or install software

**Update Management** allows you to **manage and install operating system updates and patches** for both **Windows** and **Linux** virtual machines that are deployed in Azure, on-premises, or in other cloud providers

- Update Management will perform a scan for update compliance
- A compliance scan is by default, **performed every 12 hours** on a **Windows** and **every 3 hours** on a **Linux**
- It can take between **30 minutes and 6 hours** for the dashboard to display updated data from managed computers.





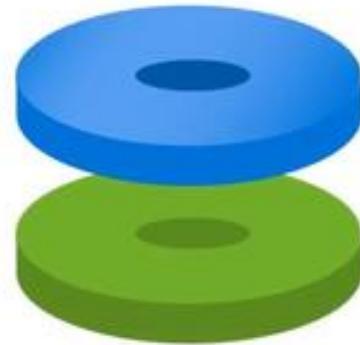
# Azure Administrator



## Introduction to Azure Disks

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure Disks



A virtual hard drive in the cloud  
**Block-level storage volumes** for SSD and HDD



# Introduction to Azure Disks

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Managed Disks are **block-level storage volumes** that are managed by Azure and used with Azure VMs



Managed disks **are like a physical disk** in an on-premises server **but, virtualized.**

You specify **size, type** and other **configurations** without worrying about the underlying hardware

- Managed disks are designed for 99.999% availability.
- Azure creates **three replicas** of your data, allowing for high durability
- You can create up to 50,000 VM **disks** of a type in a subscription per region
- Allowing you to create up to 1,000 VMs in a virtual machine scale set using a Marketplace image.
- Managed disks are integrated with **availability sets**
- Managed disks support **Availability Zones**
- **Azure Backup** can be used to create a backup job with time-based backups and backup retention policies.
- You can use **Azure role-based access control (RBAC)** to assign specific permissions for a managed disk to one or more users.
- You can **directly import** your Virtual Hard drive Disks (VHD) into Azure Disks
- You can use **Azure Private Links** to ensure traffic between Azure Disks and VMs stay within the Microsoft network





# Azure Administrator



## Disk Encryption



# Azure Disks – Encryption

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Azure Managed Disks** supports 2 types of encryption:

- Server Side Encryption (SSE)
- Azure Disk Encryption (ADE)

## Server Side Encryption (SSE)

provides encryption-at-rest and safeguards your data to meet your organizational security and compliance commitments.  
enabled **by default** for all managed disks, snapshots, and images

*Temporary disk are not encrypted by server-side encryption unless you enable encryption at host*

Keys can be managed two ways:

1. Platform-managed keys — Azure manages your keys
2. Customer-managed keys — You manage your keys

## Azure Disk Encryption (ADE)

allows you to **encrypt the OS and Data** disks used by an IaaS Virtual Machine

- For Windows encryption is done by **BitLocker**
- For Linux encryption is done by **DM-Crypt**





# Azure Administrator



## Disk Roles

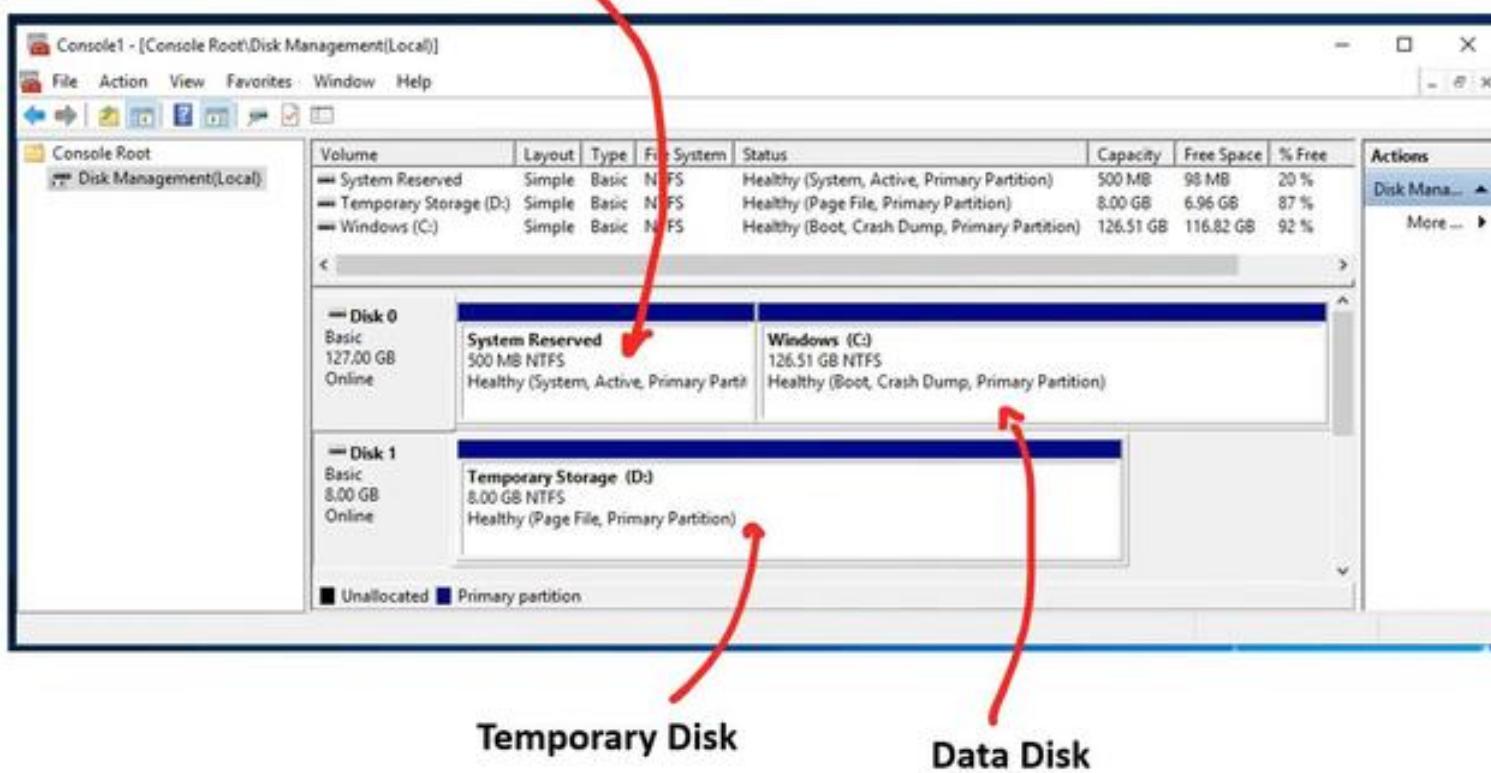


# Azure Disks – Disk Roles

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are 3 main disk roles in Azure, the **data disk**, the **OS disk**, the **temporary disk**  
Its possible to see these three roles via remote access your VM (Windows 10 Pro below)

**OS Disk**





# Azure Disks – Disk Roles

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

There are 3 main disk roles in Azure, the **data disk**, the **OS disk**, the **temporary disk**

## Data Disk

- a managed disk that's attached to a virtual machine to store application data, or other data you need to keep
- registered as SCSI drives and are labeled with a letter that you choose
- has a maximum capacity of 32,767 gibibytes (GiB)
- The size of the VM determines how many data disks you can attach and the type of storage you can use

## OS Disk

- Every virtual machine has one attached operating system disk.
- That OS disk has a pre-installed OS, which was selected when the VM was created.
- This disk contains the boot volume.
- This disk has a maximum capacity of 4,095 GiB

## Temporary Disk

- Most VMs contain a temporary disk, which is not a managed disk.
- provides short-term storage for applications and processes, and is intended to only store data such as page or swap files.
- Data on the temporary disk may be lost during a maintenance event or when you redeploy a VM.
- During a successful standard reboot of the VM, data on the temporary disk will persist.
- The temporary disk is typically /dev/sdb and on Linx and Windows VMs the temporary disk is D: by default.
- not encrypted by SSE unless you enable encryption at host.





# Azure Administrator



## Managed Disk Snapshots Managed Custom Image





# Managed Disk Snapshots and Managed Custom Image

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

A **managed disk snapshot** is a **read-only crash-consistent full copy of a managed disk** that is stored as a standard managed disk by default.

- Snapshots are point in time recovery
- Snapshots exist independent of the source disk and can be used to create new managed disks
- Snapshots are billed based on the used size. (If you have a 64 GB drive and only use 10 GB you're only billed the 10GB)
- You can see the used size of your snapshots by looking at the Azure usage report.

A **managed custom image** allow you to create an image (a copy) of your disk from your VM. This image contains **all managed disks** associated with a VM, including both the OS and data disks.

A snapshot **doesn't have awareness of any disk except the one it contains**.

This makes it problematic to use in scenarios that require the coordination of multiple disks, such as striping.

Snapshots would need to be able to coordinate with each other and this is currently not supported.

This is where you would want to use a **Managed Custom Image**





# Azure Administrator



## Disk Types



# Azure Disks – Disk Types

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure offers **4 tiers** of disks:

## 1. Ultra Disks

- deliver high throughput, high I/OPS, and consistent low latency disk storage for Azure VMs
- dynamically change the performance of the disk, without the need to restart your VM
- suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads
- can only be used as **data disks** (use a Premium SSD for OS Disk)
- Only supported with very specific VM series

## 2. Premium SSD

- high-performance and low-latency disk support for Azure VMs with input/output (IO)-intensive workloads
- suitable for mission-critical production applications
- only be used with VM series that are premium storage-compatible
- Guaranteed IOPS, and throughput of that disk (Standard tiers don't have IOPS guarantees)
- designed to provide low single-digit millisecond latencies and target IOPS and throughput described in the preceding table 99.9% of the time





# Azure Disks – Disk Types

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## 3. Standard SSD

- cost-effective storage option optimized for workloads that need consistent performance at lower IOPS levels
- Compared to standard HDDs, standard SSDs deliver better availability, consistency, reliability, and latency.
- Suitable for Web servers, low IOPS application servers, lightly used enterprise applications, and Dev/Test workloads
- designed to provide single-digit millisecond latencies and the IOPS and throughput up to the limits described in the preceding table 99% of the time
- IOPS and throughput may vary sometimes depending on the traffic patterns
- Available on all Azure VMs

## 4. Standard HDD

- reliable, low-cost disk support for VMs running latency-insensitive workloads
- available on all Azure VMs
- Latency, IOPS, and Throughput of Standard HDD disks may vary more widely as compared to SSD-based disks
- designed to deliver write latencies under 10ms and read latencies under 20ms for most IO operations
- Available in all Azure regions and can be used with all Azure VMs





# Azure Disks – Disk Types

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

	Ultra Disk	Premium SSD	Standard SSD	Standard HDD
Scenario	SSD	SSD	SSD	HDD
Max Disk Size	~65K GiB	~32.7K GiB	~32.7K GiB	~32.7K GiB
Max Throughput	2,000 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPs	160,000	20,000	6,000	2,000



# Azure Administrator



## Bursting



# Azure Disks – Bursting

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Disk Bursting** is the ability to **boost disk storage IOPS and MB/s performance** for a period of time on both VMs and disks.

Bursting allows you to handle unexpected disk traffic.

This allows you to get more use out of your disk, avoid to permanently upgrading to a more performance disk.

Bursting on Disks and VMs are independent from one another  
If you have bursting disk you don't need a bursting VM

## Burstable VMs

- Lsv2 series (All Regions)
- Ds3 series (West Central US)
- Esv3 series (West Central US)

*Bursting is enabled by default for virtual machines that support it.*

## Burstable Disk

- Premium SSDs for disk sizes P20 and smaller (All Regions)

*Bursting is enabled by default for disks that support it.*





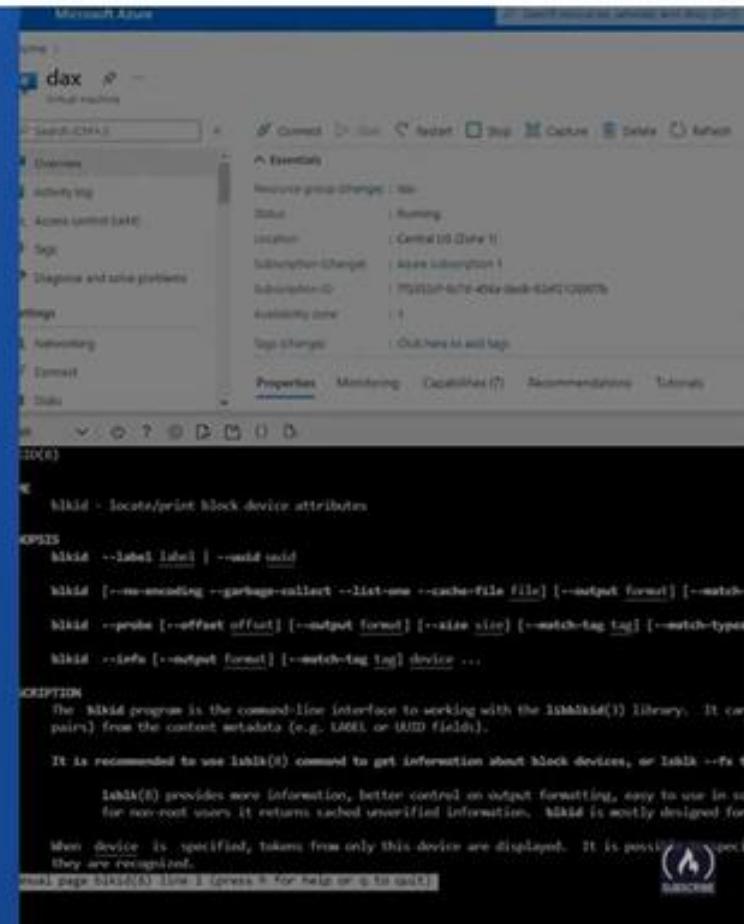
# Azure Administrator



## Attaching, Partitioning and Mounting a Disk



Follow Along



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with options like 'Essentials', 'Activity Log', 'Access Control (IAM)', 'Logs', 'Diagnose and solve problems', 'Networking', 'Compute', and 'Storage'. The main area displays a virtual machine named 'dax'. The 'Storage' tab is selected, showing a single disk named 'Central OS Disk 1'. The 'Status' section indicates the disk is 'Running' and part of 'Central OS Disk 1'. Below this, there's a command-line interface for the 'blkid' tool, which is used to locate/print block device attributes. The help text for 'blkid' includes options for labeling, UUID, encoding, garbage collection, listing, output format, offset, probe, size, tag, and info. It also notes that 'blkid' is the command-line interface to working with the libblkid() library. The 'DESCRIPTION' section explains that libblkid() provides more information, better control over output formatting, and is easier to use than blkid(8) for non-root users. It returns cached unverified information. The 'NOTES' section states that when a device is specified, tokens from only this device are displayed. It is possible to specify multiple devices. The 'SEE ALSO' section links to blkid(8), libblkid(3), and blkid(8). A 'SUBSCRIBE' button is at the bottom right.

```
blkid - Locate/print block device attributes
blkid --label [label] | --uuid [uuid]
blkid [-c encoding] --garbage-collect --list-one --cache-file [file] [--output [format]] [-w [watcher]]
blkid --probe [-o [offset]] [--output [format]] [-s [size]] [--match-tag [tag]] [--match-type [type]]
blkid --info [-o [format]] [--match-tag [tag]] [device ...]
```

**DESCRIPTION**

The `blkid` program is the command-line interface to working with the `libblkid()` library. It can parse from the content metadata (e.g. UUID or UUID fields).

It is recommended to use `libblkid()` command to get information about block devices, or `lsblk` to see what they are connected.

`libblkid()` provides more information, better control on output formatting, easy to use in scripts for non-root users. It returns cached unverified information. `blkid` is mostly designed for interactive use.

When `device` is specified, tokens from only this device are displayed. It is possible to specify multiple devices.

SEE ALSO

- `blkid(8)`, `libblkid(3)`, `blkid(8)` for help on `blkid`.

SUBSCRIBE



# Azure Administrator



## Azure Disks CheatSheet



# Azure Disks *CheatSheet*

Exam

Pro

Azure Managed Disks are **block-level storage volumes** that are managed by Azure and used with Azure VMs

Managed disks are designed for 99.999% availability.

Azure creates **three replicas** of your data, allowing for high durability

You can create up to 50,000 VM **disks** of a type in a subscription per region

Allowing you to create up to 1,000 VMs in a virtual machine scale set using a Marketplace image.

Managed disks are integrated with **availability sets**

Managed disks support **Availability Zones**

Azure **Backup** can be used to create a backup job with time-based backups and backup retention policies.

You can use Azure **role-based access control** (RBAC) to assign specific permissions for a managed disk to one or more users.

You can **directly import** your Virtual Hard drive Disks (VHD) into Azure Disks

You can use Azure **Private Links** to ensure traffic between Azure Disks and VMs stay within the Microsoft network

Azure Managed Disks supports 2 types of encryption:

- Server Side Encryption (SSE) enabled **by default** for all managed disks, snapshots, and images
  - Temporary disk are not encrypted by server-side encryption unless you enable encryption at host
  - Keys can be managed two ways:
    - Platform-managed keys — Azure manages your keys
    - Customer-managed keys — You manage your keys
- Azure Disk Encryption (ADE) allows you to **encrypt the OS and Data** disks used by an IaaS Virtual Machine
- For Windows encryption is done by **BitLocker**
- For Linux encryption is done by **DM-Crypt**



# Azure Disks *CheatSheet*



There are 3 main disk roles in Azure, the **data disk**, the **OS disk**, the **temporary disk**

## Data Disk

- a managed disk that's attached to a virtual machine to store application data, or other data you need to keep
- registered as SCSI drives and are labeled with a letter that you choose
- has a maximum capacity of 32,767 gibibytes (GiB)
- The size of the VM determines how many data disks you can attach and the type of storage you can use

## OS Disk

- Every virtual machine has one attached operating system disk.
- That OS disk has a pre-installed OS, which was selected when the VM was created.
- This disk contains the boot volume.
- This disk has a maximum capacity of 4,095 GiB

## Temporary Disk

- Most VMs contain a temporary disk, which is not a managed disk.
- provides short-term storage for applications and processes, and is intended to only store data such as page or swap files.
- Data on the temporary disk may be lost during a maintenance event or when you redeploy a VM.
- During a successful standard reboot of the VM, data on the temporary disk will persist.
- The temporary disk is typically /dev/sdb and on Linux and Windows VMs the temporary disk is D: by default.
- not encrypted by SSE unless you enable encryption at host.

A **managed disk snapshot** is a **read-only crash-consistent full copy of a managed disk** that is stored as a standard managed disk by default.

- Snapshots are point in time recovery
- Snapshots exist independent of the source disk and can be used to create new managed disks
- Snapshots are billed based on the used size. (If you have a 64 GB drive and only use 10 GB you're only billed the 10GB)
- You can see the used size of your snapshots by looking at the Azure usage report.



# Azure Disks *CheatSheet*

Exam Pro

A **managed custom image** create an image (of your disk from you VM. Contains **all managed disks** associated with a VM, OS and data disks.

A snapshot **doesn't have awareness of any disk except the one it contains**.

For a single disk use a **managed disk snapshot**, for multiple disks such as striping use a **managed custom disk**

Azure offers **4 tiers** of disks: Ultra Disks, Premium SSD, Standard SSD, Standard HDD

**1. Ultra Disks** deliver high throughput, high I/OOPS, and consistent low latency disk storage for Azure VMs

- dynamically change the performance of the disk, without the need to restart your VM
- suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads
- can only be used as **data disks** (use a Premium SSD for OS Disk), Only supported with very specific VM series

**2. Premium SSD** high-performance and low-latency disk support for Azure VMs with input/output (IO)-intensive workloads

- suitable for mission-critical production applications
- only be used with VM series that are premium storage-compatible
- Guaranteed IOPS, and throughput of that disk (Standard tiers don't have IOPS guarantees)
- designed to provide low single-digit ms latencies and target IOPS and throughput described in the preceding table 99.9% of the time

**3. Standard SSD** cost-effective storage option optimized for workloads that need consistent performance at lower IOPS levels

- Compared to standard HDDs, standard SSDs deliver better availability, consistency, reliability, and latency.
- Suitable for Web servers, low IOPS application servers, lightly used enterprise applications, and Dev/Test workloads
- designed to provide single-digit ms latencies and the IOPS and throughput up to the limits described in the preceding table 99% of the time
- IOPS and throughput may vary sometimes depending on the traffic patterns, Available on all Azure VMs

**4. Standard HDD** reliable, low-cost disk support for VMs running latency-insensitive workloads

- available on all Azure VMs
- Latency, IOPS, and Throughput of Standard HDD disks may vary more widely as compared to SSD-based disks
- designed to deliver write latencies under 10ms and read latencies under 20ms for most IO operations
- Available in all Azure regions and can be used with all Azure VMs





# Azure Administrator

Azure Application Gateway



## Introduction to Azure Application Gateway



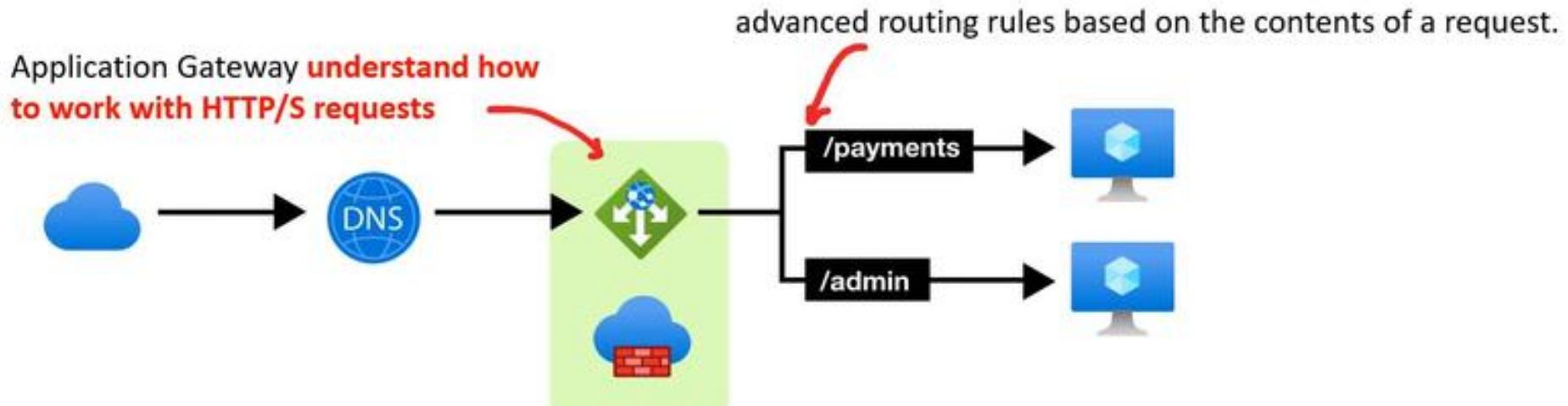


# Introduction to Application Gateway

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Application Gateway is **application-level routing** and **load balancing** service.

Application Gateway operates on **OSI Layer 7** also known as the Application Layer.



Azure Web Application Firewall (WAF) policies can be attached to an Application Gateway to provide additional security





# Introduction to Application Gateway

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)



You need to configure a **Frontends**

- **Private IP** will create an Internal Load Balancer
- **Public IP** will create an Public/External Load Balancer

Frontend IP address type   Public  Private  Both

You need to configure a **Backends**

- You'll need to create Backend pools
  - A backend pool is a collection of resources to which your application gateway can send traffic.
  - A backend pool can contain
    - virtual machines
    - virtual machines scale sets
    - IP addresses
    - domain names
    - App Service

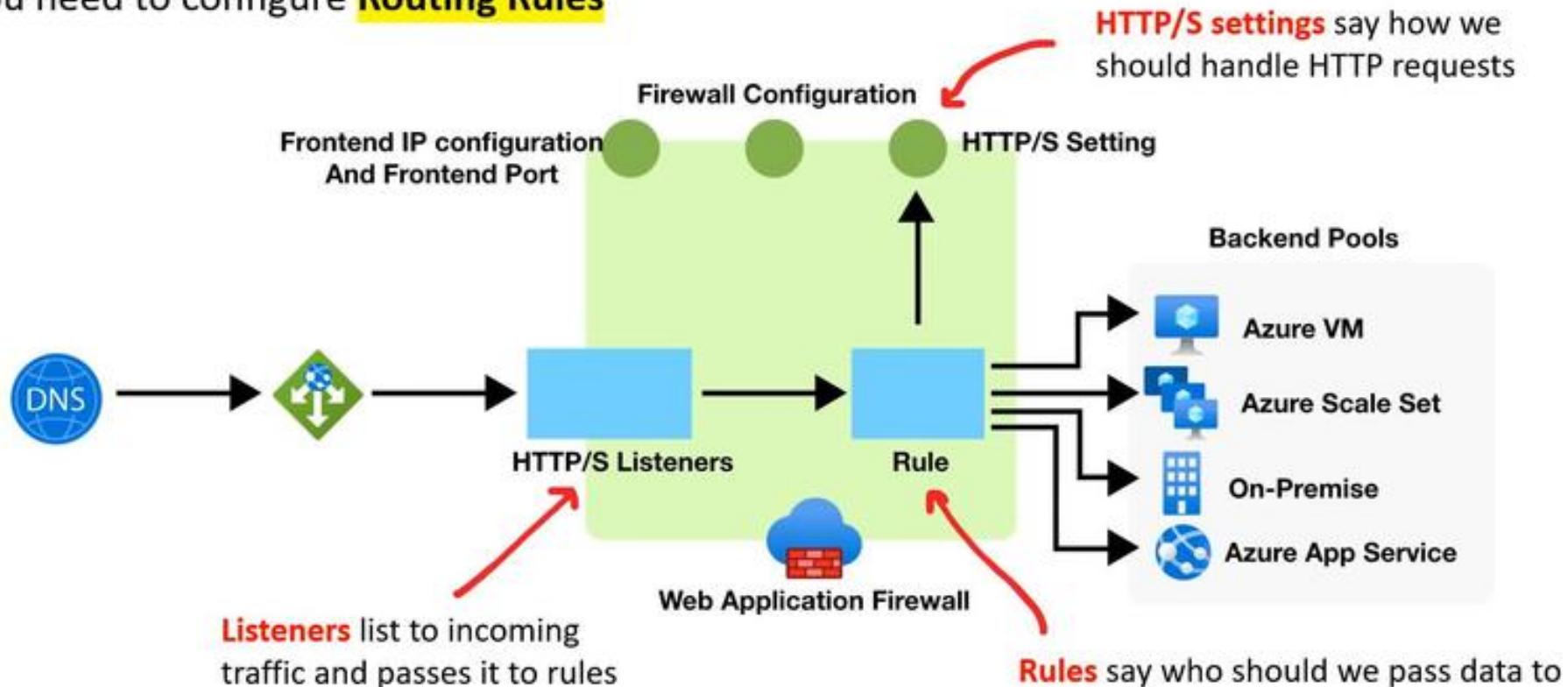




# Introduction to Application Gateway

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

You need to configure **Routing Rules**





# Azure Administrator

Azure Application Gateway



## Routing Rules





# Application Gateway – Routing Rules

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Listeners

A listener “listens” on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

There are 2 types of listeners:



Listener type  Basic  Multi site

1. Basic — forward all requests for any domain to backend pools
  2. Multi-site — forward requests to different backend pools based on **host header** and **host name**
- requests are matched according to the **order of the rules** and the type of listener
    - Add your basic listeners last otherwise it will capture all requests

## Backend targets

Chooses where a route should go either **Backend Pool** or **Redirection**



Target type  Backend pool  Redirection

## HTTP Settings

To create a rule for Backend Pool you need to create HTTP Setting.

This allows to define how we want to handle cookies, connection draining, port request time out and more..





# Application Gateway – Routing Rules

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Backend Port

the port where the back-end servers listen to incoming traffic

## Cookie-based affinity

Use cookies to keep a user session on the same server

## Connection draining

gracefully remove backend pool members during planned service updates

## Request Timeouts

the number of seconds that the application gateway will wait to receive a response from the backend pool before it returns a “connection timed out” error message.

## Override backend path

allows you to override the path in the URL so that the requests for a specific path can be routed to another path

## Override Hostname

Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header

### Add a HTTP setting

HTTP settings name \*

MyHTTPSettings

HTTP  HTTPS

Backend port \*

80

#### Additional settings

Cookie-based affinity

Enable  Disable

Connection draining

Enable  Disable

Request time-out (seconds) \*

20

Override backend path

Yes  No

#### Host name

By default, Application Gateway does not change the incoming HTTP host header for the backend. Multi-tenant services like App service or API management rely on a specific endpoint. Change these settings to overwrite the incoming HTTP host header.

Override with new host name

Yes  No

Host name override

Pick host name from backend  Override with specific domain name

e.g. contoso.com

Create custom probes

Yes  No





# Azure Administrator

Azure Application Gateway



## Application Gateway CheatSheet



# Azure Application Gateway *CheatSheet*



Azure Application Gateway is **application-level routing** and **load balancing** service.

Application Gateway operates on **OSI Layer 7** also known as the Application Layer.

- **Azure Web Application Firewall (WAF)** policies can be attached to an Application Gateway to provide additional security

An Application Gateway is composed of Frontends, Routing Rules and Backends:

- Frontends you choose an address type
  - **Private IP** will create an Internal Load Balancer
  - **Public IP** will create an Public/External Load Balancer
- Backends you create Backend Pools
  - Backend pools
    - A backend pool is a collection of resources to which your application gateway can send traffic.
    - A backend pool can contain , VMs, VM scale sets, IP addresses, domain names, App Service
- **Routing Rules** are composed of **Listeners**, **Backend targets**, **HTTP Settings**
  - **Listeners** “listens” on a specified port and IP address for traffic that uses a specified protocol.
    - If the listener criteria are met, the application gateway will apply this routing rule.
    - There are 2 types of listeners:
      - Basic — forward all requests for any domain to backend pools
      - Multi-site — forward requests to different backend pools based on **host header** and **host name**
      - requests are matched according to the **order of the rules** and the type of listener
        - Add your basic listeners last otherwise it will capture all requests
  - **Backend targets** Chooses where a route should go either **Backend Pool** or **Redirection**
    - To create a rule for Backend Pool you need to create **HTTP Setting**.
      - defines how we want to handle cookies, connection draining, port request time out and more.





# Azure Administrator

Scale Sets



## Introduction to Scale Sets

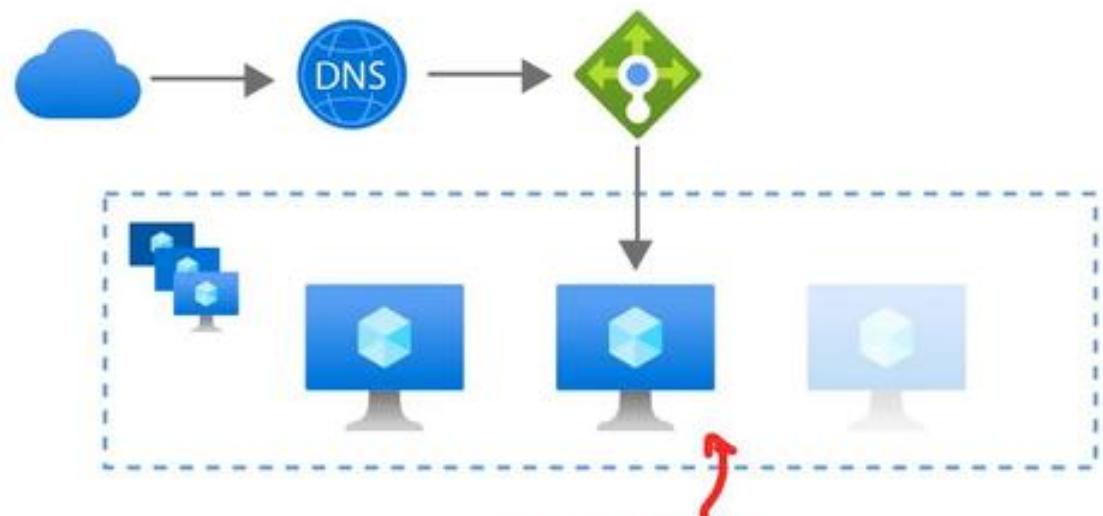




# Azure Scale Sets

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Scale Sets allows you to **automatically increase or decrease** your VM capacity.



- Create Scaling Policies to automatically add or remove based on Host Metrics
- Create Health checks and set a Repair Policy to replace unhealthy instances
- Associate A Load Balancer to distribute VMs across AZs
- You can scale to 100s or even 1000s of VMs using scale sets



# Azure Administrator

Scale Sets



## Associate a Load Balancer





# Azure Scale Sets - Load Balancer

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

A Load Balancer can be **associated** with a Scale Set.

This will allow you to:

- evenly distribute your VMs across multiple Availability Zones to make your application Highly Available.
- Use Load Balancer probe checks for more robust Health checks

Use a load balancer

Yes  No

Load balancing options \*

Select a load balancer \*  [Create new](#)

Select a backend pool \*  [Create new](#)

You have the choice between 2 different load balancers:

1. **Application Gateway** is an **HTTP/HTTPS** web traffic load balancer with URL-based routing, SSL termination, session persistence, and web application firewall.
2. **Azure Load Balancer** supports all **TCP/UDP** network traffic, port-forwarding, and outbound flows.





# Azure Administrator

Scale Sets



## Scaling Policy





# Azure Scale Sets – Scaling Policy

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**A Scaling Policy** determine when a VMs should be added or removed to meet current capacity requirements

## Scale Out

When a instance should be **added** to the Scale Set to **increase** capacity  
eg. When CPU Threshold (%) greater than X for Y minutes add X servers

## Scale In

When a instance should be **removed** to the Scale Set to **decrease** capacity  
eg. When CPU Threshold (%) less than X for Y minutes add X servers

Scaling

Scaling policy  Manual  Custom

Minimum number of VMs \*

Maximum number of VMs \*

Scale out

CPU threshold (%) \*

Duration in minutes \*

Number of VMs to increase by \*  ✓

Scale in

CPU threshold (%) \*

Number of VMs to decrease by \*

*When you are creating a Scale Set you have very limited options for your Scaling Policy*





# Azure Scale Sets – Scaling Policy

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

The screenshot shows the 'Scale rule' configuration dialog. At the top, it says 'Metric source: Current resource (MyScaleSet)'. Below that, 'Resource type' is set to 'Virtual machine scale sets' and 'Resource' is 'MyScaleSet'. The 'Criteria' section includes a 'Time aggregation' dropdown set to 'Average', a 'Metric namespace' dropdown set to 'Virtual Machine Host', and a 'Metric name' dropdown set to 'Network In Total'. There's also a 'Dimension Name' section with an 'Operator' dropdown set to 'All values'. A note below says: 'If you select multiple values for a dimension, autoscale will aggregate the metric across the selected values, not evaluate the metric for each values individually.' On the right, there's a chart titled 'Network In Total (Average)' showing data from 11:00 AM to 11:55 AM. Below the chart are sections for 'Enable metric divide by instance count' (unchecked), 'Operator' (set to 'Greater than' with value '70'), 'Duration (in minutes)' (set to '10'), 'Time grain (in mins)' (set to '1'), and 'Time grain statistic' (set to 'Average'). The 'Action' section includes 'Operation' (set to 'Increase count by' with value '1'), 'Cool down (minutes)' (set to '5'), and 'Instance count' (set to '1'). At the bottom is a blue 'Add' button.

After you create your ScaleSet you have a-lot more options available to configure the rules of your Scaling Policy

#### Built-in Host-based metrics:

- Percentage CPU
- Network In
- Network Out
- Disk Read Bytes
- Disk Write Bytes
- Disk Read Operations/Sec
- Disk Write Operations/Sec
- CPU Credits Remaining
- CPU Credits Consumed

#### Aggregates

- Average
- Minimum
- Maximum
- Total
- Last
- Count

#### Operators

- Greater than
- Greater than or equal to
- Less than
- Less than or equal to
- Equal to
- Not equal to

#### Actions

- Increase count by X
- Increase percent by X%
- Increase count to X
- Decrease count by X
- Decrease percent by X%
- Decrease count to X

If you want more metrics there are 2 ways to collect more information:

1. **App Insights** installs a small instrumentation package in your application that monitors the app and sends telemetry to Azure.
  - When you want application metrics: Page load performance, Session counts
2. **Azure Diagnostic extension** is an agent that runs inside a VM instance. It monitors and saves performance metrics to Azure storage so you can collect more detailed information
  - When you want more detailed Host-based metrics



# Azure Scale Sets – Scaling Policy

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Scale-In Policy** is how determines what VM is removed (deleted) to decrease the capacity of the Scale Set

## Default

- Delete the VM with the highest Instance ID
- Balanced across Availability Zones (AZs) and Fault Domains (ADs)

## Newest VM

- Delete the newest created VM
- Balanced across Availability Zones (AZs)

## Oldest VM

- Delete the oldest VM
- Balanced across Availability Zones (AZs)

Scale-In policy

Scale-in policy

Default - Balance across availabil

**Update Policy** determine how VM instances are brought up-to-date with the latest scale set model

## Automatic

- Increasing with start upgrading immediately in random order

## Manual

- Existing instances must be manually upgraded

## Rolling

- Upgrades roll out in batches with optional pause

Upgrade policy

Upgrade mode \*

Manual - Existing instances mu

**Automatic OS upgrades** can be enabled helps to ease update management by safely and automatically upgrading the OS disk for all instances





# Azure Administrator

Scale Sets



## Health Monitoring

(A)  
SUBSCRIBE



# Azure Scale Sets - Health Monitoring

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Health monitoring can be enabled to determine if your server is **healthy** or **unhealthy**.

There are 2 modes of health monitoring:

1. Application health extension
  - Ping an HTTP request to a specific path and expect a status 200
2. Load Balancer Probe
  - Allow you to check based on TCP, UDP or HTTP requests.

Health

Monitor application health  Enabled

Application health monitor \*  Application health extension

Protocol \*  HTTP

Port number \*  80

Path \*  /

Monitor application health  Enabled

Application health monitor \*  Load balancer probe

Load balancer health probe  (new) healthProbe3b8ed99b-1

[Create new](#)

Automatic repair policy

If an instance is found to be unhealthy the delete it and launch a new instance

Automatic repair policy

Automatic repairs  On  Off

Grace period (min) \*  30





# Azure Administrator

Scale Sets



## Advanced Features



# Azure Scale Sets - Advanced

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Allocation policy

By default Scaling Sets are limited to 100 instances.

You can beyond 100 (up to 1000 instances)



### Allocation policy

Enable scaling beyond 100 instances  No  Yes

Spreading algorithm  Max spreading  Fixed spreading

Fault domain count \*

**Proximity placement groups** allow you to group Azure resources physically closer together in the same region.



### Proximity placement group

Proximity placement group

By default a scale set has a single placement that hold upto 100 VMs.

If a scale set property called *singlePlacementGroup* is set to *false*, then the scale set can be composed of multiple placement groups and has a range of 0-1,000 VMs.





# Azure Administrator

Scale Sets



## Scale Sets CheatSheet



# Scale Sets *CheatSheet*

Exam

Pro

Azure Scale Sets allows you to **automatically increase** or **decrease** your VM capacity.

A Load Balancer can be **associated** with a Scale Set.

- evenly distribute your VMs across multiple Availability Zones to make your application Highly Available.
- Use Load Balancer probe checks for more robust Health checks
- You have the choice between 2 different load balancers:
  1. **Application Gateway** is an **HTTP/HTTPS** web traffic load balancer application firewall.
  2. **Azure Load Balancer** supports all **TCP/UDP** network traffic, port-forwarding, and outbound flows.
- A **Scaling Policy** determine when a VMs should be added or removed to meet current capacity requirements
  - **Scale Out** When a instance should be **added** to the Scale Set to **increase** capacity
  - **Scale In** When a instance should be **removed** to the Scale Set to **decrease** capacity

**Scale-In Policy** is how determines what VM is removed (deleted) to decrease the capacity of the Scale Set

- **Default** Delete the VM with the highest Instance ID, Balanced across Availability Zones (AZs) and Fault Domains (ADs)
- **Newest VM** Delete the newest created VM, Balanced across Availability Zones (AZs)
- **Oldest VM** Delete the oldest VM, Balanced across Availability Zones (AZs)

**Update Policy** determine how VM instances are brought up-to-date with the latest scale set model

- **Automatic** Increasing with start upgrading immediately in random order
- **Manual** Existing instances must be manually upgraded
- **Rolling** Upgrades roll out in batches with optional pause

**Health monitoring** can be enabled to determine if you server is **healthy** or **unhealthy**.

There are 2 modes of health monitoring:

1. Application health extension: Ping an HTTP request to a specific path and except a status 200
2. Load Balancer Probe: Allow you to check based on TCP, UDP or HTTP requests.

**Automatic repair policy** If an instance is found to be unhealthy the delete it and launch a new instance





# Azure Administrator

Azure App Services



## Introduction to Azure App Services



Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure App Service



Quickly **deploy and manage Web apps** on Azure  
without worrying about the underlying infrastructure

*Platform as a Service*





# Introduction to Azure App Service

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure App Service is an **HTTP-based service** for hosting web applications, REST APIs, and mobile back ends.

You can choose your **programming language** and either a **Windows** and **Linux** environment

It is a Platform as Service, so it's the **Heroku equivalent for Azure**.

**Azure App Service takes** care of the following underlying infrastructure

- Security patches for OS and languages
- Load balancing
- Autoscaling
- Automated manager

When you create your app you have to choose a unique name since it becomes a fully qualified domain

deep-space-nine   
.azurewebsites.net

**Azure App Service** makes it easy to implement common Integrations and features such as:

- Azure DevOps (For deployments)
- Github Integration
- Docker Hub Integration
- Package Management
- Easy to setup staging environments
- Custom Domains
- Attaching TLS/SSL Certificates

You pay based on an Azure App Service Plan:

- **Shared Tier** — Free, Shared (Linux not supported)
- **Dedicated Tier** — Basic, Standard, Premium, PremiumV2, PremiumV3
- **Isolated Tier**

Azure App Services can also run docker single or multi-containers 



# Azure Administrator

Azure App Services



## Runtimes





# Azure App Service – Runtimes

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a Runtime Environment?

A runtime software/instructions that are executed *while* your program is running.

A runtime generally means what **programming language** and **libraries** and **framework** you are using.

A runtime for Azure App Services will be a pre-defined **container** that has your programming language and commonly used library for that language installed.

With Azure App Services you choose a runtime.

- .NET
- .NET Core
- Java
- Ruby
- Node.js
- PHP
- Python

Azure App Services will have generally multiple latest versions of a programming language eg. Ruby 2.6, 2.7

It's common for a cloud provider to stop supporting older versions so you keep current and forces customer to keep good security practices by having latest patches



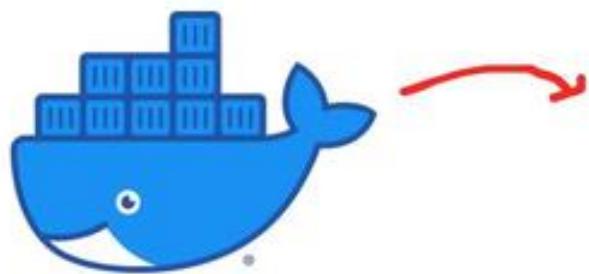


# Azure App Service – Custom Container

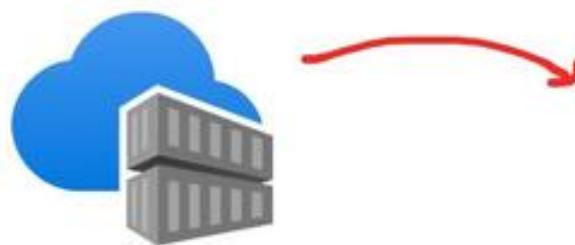
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure App Service allows you defined **custom containers** for **Windows or Linux**

You might want to create your own custom container to use a different runtime or bundle in a packages or software



**Create** your own **Docker** Container  
on your local environment



**Push** the Docker container to  
**Azure Container Registry**



**Deploy** your Container  
Image to **App Service**



# Azure Administrator

Azure App Services



## Deployment Slots



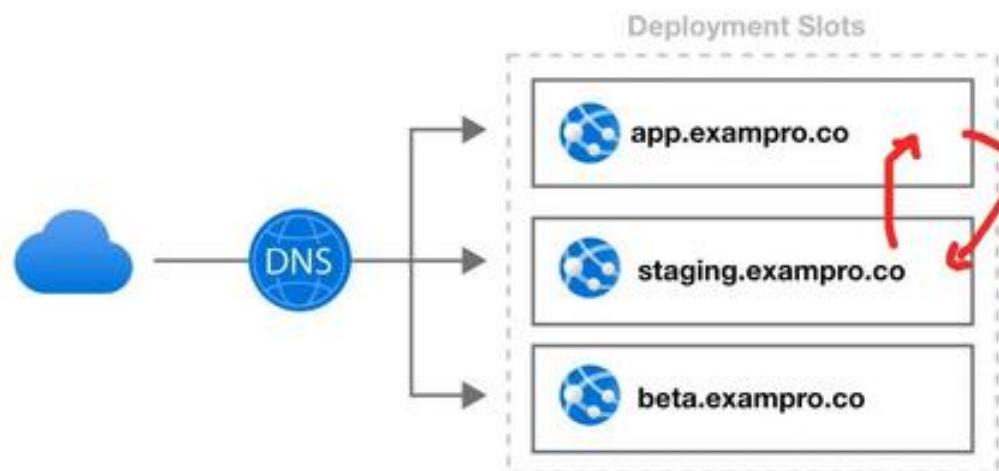


# Azure App Service – Deployment Slots

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Deployment Slots** allow you to create **different environments** of your web-application associated to a different hostname. This is useful when need a staging, or QA environment.

Think of it as a way to quickly clone your production environment for other uses.



You can also **Swap environments** This could be how you perform a Blue/Green deploy.

You can promote our staging to production by swapping, if something goes wrong you could swap them back.





# Azure Administrator

Azure App Services



## App Service Environment





# Azure App Service – App Service Environment

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**App Service Environment (ASE)** is an Azure App Service feature that provides a **fully isolated and dedicated environment** for securely running App Service apps at high scale

This allow you to host:

- Windows web apps
- Linux web apps
- Docker containers
- Mobile apps
- Functions

App Service environments (ASEs) are appropriate for application workloads that require:

- Very high scale
- Isolation and secure network access.
- High memory utilization

Customers can create multiple ASEs within a single Azure region or across multiple Azure regions making ASEs ideal for **horizontally scaling stateless application tiers** in support of **high requests per second (RPS) workloads**.

- ASE comes with its own pricing tier (Isolated Tier)
- ASEs can be used to configure security architecture
- Apps running on ASEs can have their access gated by upstream devices, such as web application firewalls (WAFs)
- App Service Environments can be deployed into Availability Zones (AZ) using zone pinning.

There are **2 deployment types** for an App Service environment (ASE):

1. External ASE
2. ILB ASE

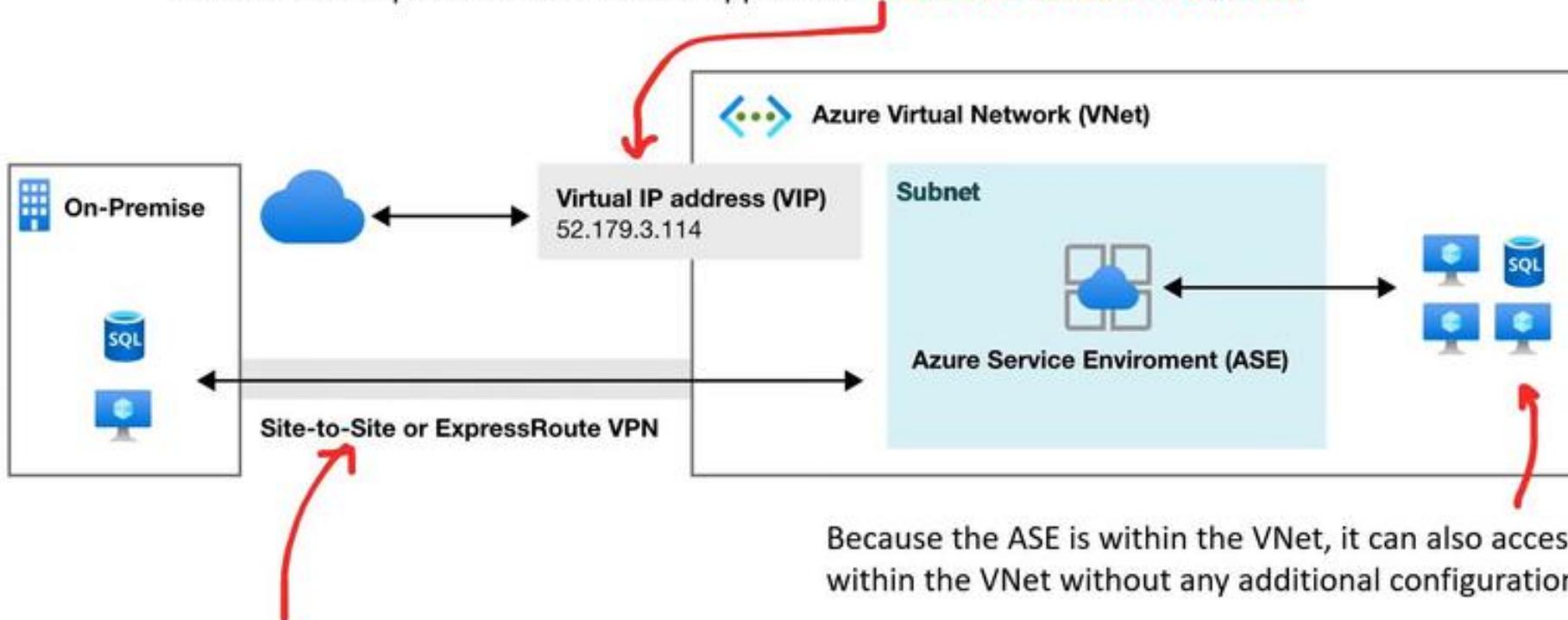




# Azure App Service – App Service Environment

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

External ASE exposes the ASE-hosted apps on an **internet-accessible IP address**.



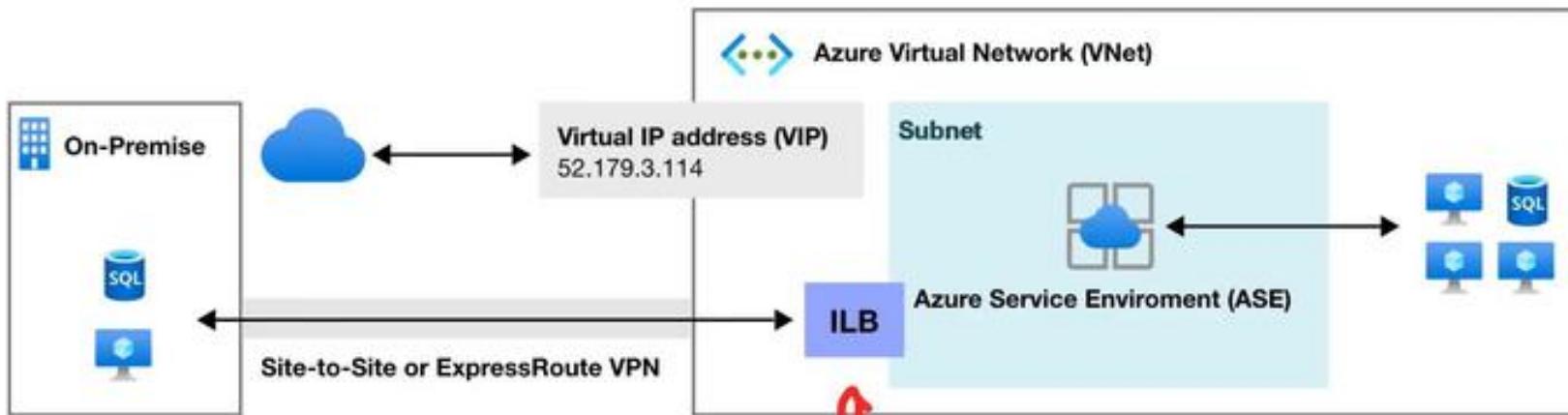
If the VNet is connected to your on-premises network, apps in your ASE also have access to resources there without additional configuration.





# Azure App Service – App Service Environment

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)



ILB ASE exposes the ASE-hosted apps on an IP address inside your VNet.

The internal endpoint is an **internal load balancer (ILB)**



# Azure Administrator

Azure App Services



## Deployment



# Azure App Service – Deployment

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is Deployment?

The action of pushing changes or updates from a local environment or repository into a remote environment.

Azure App Services provides many ways to deploy your applications:

- Run from Package
- Deploy ZIP or WAR (Uses Kudu)
- Deploy via FTP
- Deploy via cloud sync (Dropbox or One Drive)
- Deploy continuously (GitHub, BitBucket, and Azure Repos) uses Kudu and Azure Pipelines
- Deploy using a custom container CI/CD pipeline (Deploy for Docker Hub or Azure Container Registry)
- Deploy from local Git (Kudu build server,)
- Deploy using Github Actions
- Deploy using Github Actions containers
- Deploy with template (ARM templates)





# Azure App Service – Deployment

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Run from a package** is when the files in the package **are not copied to the wwwroot directory**.

Instead, the ZIP package itself gets **mounted** directly as the **read-only** wwwroot directory.

All other deployment methods in App Service have deployed to the following directory:

- **(Windows)** `D:\home\site\wwwroot`
- **(Linux)** `/home/site/wwwroot`

Since the same directory is used by your app at runtime, it's **possible for deployment to fail** because of **file lock conflicts**, and for the app to behave unpredictably because some of the files are not yet updated.





# Azure App Service – Deployment

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**ZIP and WAR file deployment** uses the same **Kudu service** that powers continuous integration-based deployments.



Kudu is the engine behind git deployments in Azure App Service.  
It's an open-source project that can also run outside of Azure

Kudu supports the following functionality for ZIP file deployment:

- Deletion of files left over from a previous deployment
- Option to turn on the default build process, which includes package restore
- Deployment customization, including running deployment scripts
- Deployment logs
- A file size limit of 2048 MB

You can deploy using

- Azure CLI
- Azure API via REST (cURL)
- Azure Portal



```
# Azure CLI
az webapp deployment source config-zip --resource-group <group-name> --name <app-name> --src clouddrive/<filename>.zip

# cURL
curl -X POST -u <deployment_user> --data-binary @"<zip_file_path>" https://<app_name>.scm.azurewebsites.net/api/zipdeploy

# Azure PowerShell
Publish-AzWebapp -ResourceGroupName <group-name> -Name <app-name> -ArchivePath <zip-file-path>
```





# Azure App Service – Deployment

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

You can use (File Transfer Protocol) FTP protocol to upload files.  
You will need your own FTP client. You just drag and upload your files.

Go to the **Deployment Center**

FTP

FTP

Use an FTP connection to access and copy app files.

FTP

FTP

App Service enables you to access your app content through FTP/S. [Learn more](#)

FTPS Endpoint <https://waws-prod-dm1-145.ftp.azurewebsites.windows.net/site/www>

[App Credentials](#) [User Credentials](#)

Application Credentials are auto-generated and provide access only to this specific app or deployment slot. These credentials can be used with FTP, Local Git and WebDeploy. They cannot be configured manually, but can be reset anytime. [Learn more](#)

Username [deep-space-nine\\\$deep-space-nine](#)

Password [Show](#)

[Reset Credentials](#)

Get the FTP credentials for your FTP client





# Azure App Service – Deployment

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

You can use **Dropbox** or **OneDrive** to deploy using a cloud sync.



**Dropbox** is third-party cloud storage service



OneDrive is Microsoft's cloud storage service

You go to Deployment Center, configure for Dropbox or OneDrive.

When you turn on Sync it will create a folder in your drop cloud drive:

**OneDrive**: Apps\Azure Web Apps

**Dropbox**: Apps\Azure

This will sync with your **/home/site/wwwroot**, so you just update files in that folder.





# Azure Administrator

Azure App Services



## Azure App Service Plan





# Azure App Service Plan

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure App Service Plan defines **how you pay and what resources are available** to you.

There are **3 pricing tiers** for App Service Plan:

## Shared Tiers

There are **2 shared**: Free, Shared

### Free Tier provides:

- 1 GB of disk space
- up to 10 apps on a single shared instance
- No SLA for availability
- Each app has a compute quota of 60 minutes per day

### Shared Tier provides

- up to 100 apps on a single shared instance
- No SLA for availability
- Each app has a compute quota of 240 minutes per day

*Shared Tiers does not support Linux-based instances*

The screenshot shows the Azure App Service Plan configuration page. At the top, there are three tabs: 'Dev / Test' (selected), 'Production', and 'Isolated'. Below the tabs, a message states: 'The first Basic (B1) core for Linux is free for the first 30 days!'. A section titled 'Recommended pricing tiers' contains two options: 'F1' (highlighted with a red box and a blue border) and 'B1'. The F1 tier details are: 1 GB memory, 60 minutes/day compute, and Free. The B1 tier details are: 100 total ACU, 1.75 GB memory, A-Series compute equivalent, and 16.82 CAD/Month (Estimated). A link 'See additional options' is shown below the B1 tier. To the right, under 'Included hardware', it lists 'Memory' (Memory available to run applications deployed and running in the App Service plan) and 'Storage' (1 GB disk storage shared by all apps deployed in the App Service plan).

Tier	Memory	Compute	Cost
F1	1 GB	60 minutes/day	Free
B1	1.75 GB	A-Series equivalent	16.82 CAD/Month (Estimated)

**Included hardware**

Every instance of your App Service plan will include the following hardware configuration:

- Memory**: Memory available to run applications deployed and running in the App Service plan.
- Storage**: 1 GB disk storage shared by all apps deployed in the App Service plan.





# Azure App Service Plan

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure App Service Plan defines **how you pay and what resources are available** to you.

There are **3 pricing tiers** for App Service Plan:

## Dedicated Tiers

Basic, Standard, Premium, PremiumV2, PremiumV3

## Basic

- More disk space
- Unlimited apps
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage

The screenshot shows the Azure App Service Plan pricing tiers. At the top, there are three categories: Dev / Test (for less demanding workloads), Production (for most production workloads), and Isolated (Advanced networking and scale). Below these are two sections: 'Recommended pricing tiers' and 'Additional pricing tiers'. The 'Recommended pricing tiers' section highlights the B1 tier, which is described as 'The first Basic (B1) core for Linux is free for the first 30 days!'. The B1 tier includes 100 total ACU, 1.75 GB memory, A-Series compute equivalent, and 16.82 CAD/Month (Estimated). The 'Additional pricing tiers' section shows B2 and B3, which have higher resource requirements and costs. Below these sections are 'Included features' (Custom domains / SSL, Manual scale) and 'Included hardware' (Azure Compute Units (ACU), Memory, Storage).

Tier	ACU	Memory	Compute Equivalent	Cost
B1	100	1.75 GB	A-Series	16.82 CAD/Month (Estimated)
B2	200	3.5 GB	A-Series	32.70 CAD/Month (Estimated)
B3	400	7 GB	A-Series	65.41 CAD/Month (Estimated)

**Included features**

- Custom domains / SSL
- Manual scale

**Included hardware**

- Azure Compute Units (ACU)
- Memory
- Storage





# Azure App Service Plan

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure App Service Plan defines **how you pay and what resources are available** to you.

There are **3 pricing tiers** for App Service Plan:

The screenshot shows the Azure App Service Plan pricing tiers. At the top, there are three main categories: Dev / Test (For test and learning workloads), Production (For most production workloads), and Isolated (Advanced networking and scale). Below these are two sections: Recommended pricing tiers and Additional pricing tiers. The Additional pricing tiers section is highlighted with a red box and a red arrow from the slide. It contains three boxes: P1V1 (100 total ACU, 5.25 GB memory, B-Series compute equivalent, 86.72 CAC/Month (Estimated)), P2V2 (200 total ACU, 10.5 GB memory, D-Series compute equivalent, 173.50 CAC/Month (Estimated)), and P3V3 (400 total ACU, 14 GB memory, D3-Series compute equivalent, 413.00 CAC/Month (Estimated)). Below the tiers, there are sections for Included features and Included hardware. The included features include Custom domains / SSL, Auto scale, Staging slots, Daily backups, and Traffic manager. The included hardware includes Azure Compute Units (ACU), Memory (Memory per instance), and Storage (200 GB disk storage shared by all apps deployed in the App Service plan).

## Dedicated Tiers

Basic, Standard, Premium, PremiumV2, PremiumV3

### Basic

- More disk space
- Unlimited apps
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage

### Standard

- scale out to three dedicated instances
- SLA of 99.95% availability
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage





# Azure App Service Plan

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure App Service Plan defines **how you pay and what resources are available** to you.

There are **3 pricing tiers** for App Service Plan:

## Dedicated Tiers

Basic, Standard, Premium, PremiumV2, PremiumV3

### Basic

- More disk space
- Unlimited apps
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage

### Standard

- scale out to three dedicated instances
- SLA of 99.95% availability
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage

### Premium

- scale to 10 dedicated instances
- availability SLA of 99.95%
- multiple levels of hardware

The screenshot shows the Azure App Service Plan pricing tiers. It highlights the PremiumV3 tier, which includes 400 total ACU, 7 GB memory, and 32 vCPUs. The page also shows other tiers like P1V2 and P2V2, and additional tiers like S1, S2, and S3. It details included features such as custom domains, auto-scale, staging slots, daily backups, and traffic manager, as well as included hardware like Azure Compute Units, memory, and storage.

Tier	ACU	Memory	vCPUs
P1V2	100	3.5 GB	2 vCPU
P2V2	400	7 GB	4 vCPU
P3V3	800	14 GB	8 vCPU
P1V3	100	3.5 GB	2 vCPU
P2V3	200	7 GB	4 vCPU
P3V3	400	14 GB	8 vCPU
S1	100	1.75 GB	1 vCPU
S2	200	3.5 GB	2 vCPU
S3	400	7 GB	4 vCPU





# Azure App Service Plan

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure App Service Plan defines **how you pay and what resources are available** to you.

There are **3 pricing tiers** for App Service Plan:

## Isolated Tier

- dedicated Azure virtual network
- Full network and compute isolation
- scale out to 100 instances
- availability SLA of 99.95%

The screenshot shows the Azure App Service Plan pricing tiers. It highlights the 'Isolated' tier, which is described as having advanced networking and scale. The 'Isolated' tier is shown with a dashed border around its icon and title. Below the tiers, there's a table comparing three pricing tiers: Dev/Test, Production, and Isolated. The Isolated tier is highlighted with a blue background. The table includes columns for total ACU, memory, and price per month. The 'Included features' and 'Included hardware' sections are also visible.

Tier	Total ACU	Memory	Price (CAD/Month)
Dev / Test	210	3.5 GB	355.07 CAD/Month (Estimated)
Production	420	7 GB	710.14 CAD/Month (Estimated)
<b>Isolated</b>	<b>690</b>	<b>14 GB</b>	<b>1420.29 CAD/Month (Estimated)</b>

**Included features**  
Every app hosted on this App Service plan will have access to these features:

- Single tenant system
- Isolated network
- Private app access
- Scale to a large number of instances
- Traffic manager

**Included hardware**  
Every instance of your App Service plan will include the following hardware configuration:

- Azure Compute Units (ACU)
- Memory
- Storage





# Azure Administrator

Azure App Services



## WebJobs





# Azure App Service – WebJobs

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**WebJobs** is a feature of Azure App Service that enables you to run a program or script in the same instance as a web app, API app, or mobile app.

There is **no additional cost** to use WebJobs.

*WebJobs is not yet supported for App Service on Linux.*

Type ⓘ

Continuous

Continuous

Triggered

Scale ⓘ

Multi Instance

Multi Instance

Single Instance

**The following file types are supported:**

- .cmd, .bat, .exe (using Windows cmd)
- .ps1 (using PowerShell)
- .sh (using Bash)
- .php (using PHP)
- .py (using Python)
- .js (using Node.js)
- .jar (using Java)

Triggers ⓘ

Scheduled

CRON Expression \* ⓘ

Ex: 0 0/2 \* \* \*

## WebJobs Types

- Continuous — run continually until stopped
  - Supports debugging
- Triggered — run only when **triggered**
  - (expose a webhook that can be called to enable scenarios like scheduling)
  - Doesn't support debugging

## WebJobs Scale (Only for Continuous)

- Multi Instance — will scale your WebJob across all instances of your App Service plan
- Single Instance — will only keep a single copy of your WebJob running regardless of App Service plan instance count





# Azure Administrator

Azure App Services



## Configure and Deploy Azure App Service



Follow Along

The screenshot shows the 'Spec Picker' interface for selecting an App Service plan. It features two main sections: 'Dev / Test' (selected) and 'Production'. The 'Dev / Test' section is described as 'For less demanding workloads' and notes that the first Basic (B1) core for Linux is free for the first 30 days. Below this, 'Recommended pricing tiers' are listed:

Tier	Total ACU	Memory	Compute Equivalent
P1V2	210 total ACU	3.5 GB memory	Dv2-Series compute equivalent 103.72 CADV/Month (Estimated)
P2V2	420 total ACU	7 GB memory	Dv2-Series compute equivalent 206.50 CADV/Month (Estimated)
P1V3	Premium V3 is not supported for this scale unit. Please consider redeploying or cloning your app. <a href="#">Click for more info</a>		
P2V3	Premium V3 is not supported for this scale unit. Please consider redeploying or cloning your app. <a href="#">Click for more info</a>		
P3V2	Premium P3V2 is not supported for this scale unit. Please consider redeploying or cloning your app. <a href="#">Click for more info</a>		

Below the tiers, 'Included features' are listed:

- Custom domains / SSL: Configure and purchase custom domains with IPv4 and IP SSL bindings.
- Auto scale: Up to 20 instances. Subject to availability.

On the right, 'Included hardware' is mentioned, noting that every instance of the App Service plan will have access to the specified configuration.



# Azure Administrator

Azure App Services



## Trigger a Deploy via Github Actions



### Follow Along

Microsoft Azure

Home > Microsoft.Web-WebApp-Portal-eceeb0c4-bd0d > voyager-delta-flyer

voyager-delta-flyer | Deployment Center

App Service

Search (Ctrl+F)

Logs Settings FTPS credentials

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Security Events (preview)

Deployment

- Quickstart
- Deployment slots
- Deployment Center
- Deployment Center (Classic)

Settings

- Configuration
- Authentication / Authorization
- Authentication (preview)

Time

Friday, March 19, 2021 (4)

Date	Time
03/19/2021	1:17:33 PM -0400
03/19/2021	1:16:29 PM -0400
03/19/2021	1:13:13 PM -0400

(A) SUBSCRIBE



# Azure Administrator

Azure App Services



## Create Deployment Slots



Follow Along

The screenshot shows the Azure portal interface with the search bar at the top. Below it, a breadcrumb navigation shows 'delta-flyer/staging' and 'Deployment slots'. The main area is titled 'Deployment Slots' with a sub-instruction: 'Deployment slots are live apps with their own hostnames. App content and configurations aren't shared between slots.' A table lists two deployment slots:

NAME	STATUS
delta-flyer-delta-flyer	Production
delta-flyer-delta-flyer-staging	Running



# Azure Administrator

Azure App Services



## Scaling Azure App Service



Follow Along

Scale rule

Instance: All values

If you select multiple values for a dimension, autoscale will aggregate the metric across the selected values, not evaluate the metric for each values individually.

CpuPercentage (Maximum)

70%

60%

50%

40%

30%

20%

10%

0%

3:12 PM 3:13 PM 3:14 PM 3:15 PM 3:16 PM UTC-04:00

Instead,  Enable metric divide by instance count:

Operator: Greater than  Metric threshold to trigger scale action:  70.0

Duration (in minutes): 5

Time grain (in min): 1 Time grain statistic: Maximum

Action

Operation: Increase count by  Cool down (minutes): 5

Instance count: 1

scale count: 1

(A)

Update Delete



# Azure Administrator

Azure App Services



## Azure App Services CheatSheet



# Azure App Services *CheatSheet*



Azure App Service is an **HTTP-based service** for hosting web applications, REST APIs, and mobile back ends.

- You can choose your **programming language** and either a **Windows** and **Linux** environment
- It is a Platform as Service, so it's the **Heroku or AWS Elastic Beanstalk equivalent for Azure**.

**Azure App Service** makes it easy to implement common

Integrations and features such as:

- Azure DevOps (For deployments)
- Github Integration
- Docker Hub Integration
- Package Management
- Easy to setup staging environments
- Custom Domains
- Attaching TLS/SSL Certificates

You pay based on an Azure App Service Plan:

- **Shared Tier** — Free, Shared (Linux not supported)
- **Dedicated Tier** — Basic, Standard, Premium, PremiumV2, PremiumV3
- **Isolated Tier**

Azure App Services you supports the following **runtimes**: .NET, .NET Core, Java, Ruby, Node.js, PHP, Python

Azure App Services can also run **docker** single or multi-containers

- **Custom Containers** are supported, create docker file, upload to Azure Container Registry and deploy

**Deployments Slots** allow you to create **different environments** of your web-application

- You can also **Swap environments** This could be how you perform a Blue/Green deploy.



# Azure App Services *CheatSheet*



**App Service Environment (ASE)** is an Azure App Service feature that provides a **fully isolated and dedicated environment** for securely running App Service apps at high scale

- Customers can create multiple ASEs:
  - within a single Azure region
  - across multiple Azure regions making ASEs
- ideal for **horizontally scaling stateless application tiers** in support of **high requests per second (RPS) workloads**.
- ASE comes with its own pricing tier (Isolated Tier)
- ASEs can be used to configure security architecture
- Apps running on ASEs can have their access gated by upstream devices, such as web application firewalls (WAFs)
- App Service Environments can be deployed into Availability Zones (AZ) using zone pinning.
- There are **2 deployment types** for an App Service environment (ASE):
  1. External ASE
  2. ILB ASE

Azure App Services provides many ways to deploy your applications:

**WebJobs** is a feature of Azure App Service that enables you to run a program or script in the same instance as a web app, API app, or mobile app.

- There is **no additional cost** to use WebJobs.





# Azure Administrator

Availability Follow Along

## Azure VM Images



Follow Along

Search resources, services, and documentation

Connect Stop Start Capture Delete Refresh Open in mobile

Resource group (Change) : wolf

Status : Running

Location : Central US (Zone 1)

Subscription (Change) : Azure subscription

Subscription ID : 701932f6-07d4-496e-94cb-61a42139607b

Availability zone : 1

Tags (Change) : Click here to add tags

Properties Monitoring Capabilities (1) Recommendations Tutorials

**Virtual machine**

Computer name	wolf
Operating system	Ubuntu 16.04
Publisher	Canonical
Offer	UbuntuServer
Plan	16.04-Standard
VM generation	V2
Agent status	Ready
Agent version	2.234.1
Host group	None
Host	-
Resilient placement group	-
Eviction status	N/A

**Availability - scaling**

Availability zone	Zone 1A
-------------------	---------

(A) SUBSCRIBE



# Azure Administrator

Availability Follow Along

## Review Availability Sets



**Follow Along**

[View article](#)

Fault domains define the group of virtual machines that share a common power source and network switch. By default, the virtual machines configured within your availability set are separated across up to three fault domains. While placing your virtual machines across an availability set does not protect your application from operating system or application-specific failures, it does limit the impact of potential physical hardware failures, network outages, or power interruptions.

Fault domain 0	Fault domain 1	Fault domain 2
Update domain 0	•	•
•	•	•
•	•	•
•	•	•
•	•	•
Update domain 5	•	•

VMs are also aligned with disk fault domains. This alignment ensures that all the managed disks attached to a VM are within the same fault domain.

Only VMs with managed disks can be created in a managed availability set. The number of managed disk fault domains varies by region - either two or three managed disk fault domains per region.

Region	Availability Set	(A)
East US	Compute Optimized	

- For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.
- For all Virtual Machines that have two or more instances deployed in the same Availability Set or in the same Dedicated Host Group, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.95% of the time.
- For any Single Instance Virtual Machine using Premium SSD or Ultra Disk for all Operating System Disks and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 99.9%.
- For any Single Instance Virtual Machine using Standard SSD Managed Disks for Operating System Disk and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 99.5%.
- For any Single Instance Virtual Machine using Standard HDD Managed Disks for Operating System Disks and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 95%.



# Azure Administrator

Availability Follow Along

## Create a Scale Sets



Follow Along

Microsoft Azure

Home > Shared image galleries > myGallery > MyDef (myGallery) > G1.1 (myGallery) > Create a virtual machine scale set

Create a virtual machine scale set

Basics Data Networking Scaling Management Health Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more ↗

Disk options

OS disk type \* Premium SSD

Encryption type \* DEFAULT (Encryption at rest with a platform-managed key)

SNAPSHOT Ultra Disk compatibility

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GB)	IOPS	TBWD...	Link type	Host c...
0	Temporary disk	100	100	100	SCSI	Local

CREATE AND ATTACH A NEW DISK

▼ Advanced

(A) SUBSCRIBE



# Azure Administrator

Availability Follow Along

## Create an Application Gateway



Follow Along

The screenshot shows the Microsoft Azure portal interface for creating an Application Gateway. The top navigation bar includes 'Microsoft Azure', 'Search resources', and a user icon. Below it, the breadcrumb navigation shows 'Home > Application gateways > Create application gateway'. The main title is 'Create application gateway'. There are several tabs at the top: 'Basics' (with a checkmark), 'Frontends' (with a checkmark), 'Backends' (with a checkmark), 'Configuration' (which is selected, indicated by a blue border), 'Logs', and 'Metrics'. A note below the tabs says 'Create routing rules that link your frontends and backends. You can also add more backend pools, add a second...'. Under the 'Frontends' section, there is a button '+ Add a frontend IP'. At the bottom right of the screenshot area, there is a small '(A)' icon with a downward arrow and the word 'SUBSCRIBE'.



# Azure Administrator

Azure Monitor



## Introduction to Azure Monitor





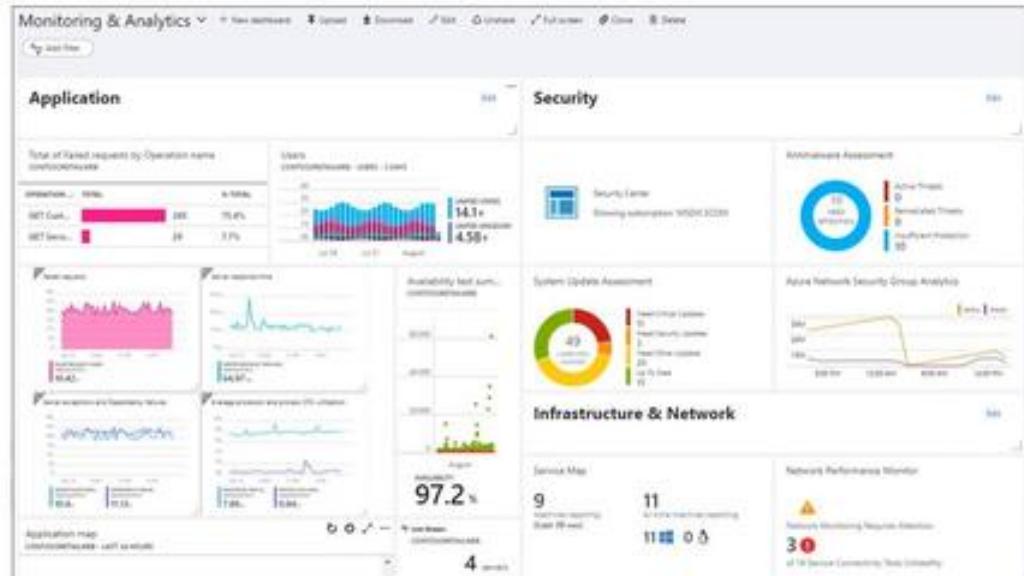
# Introduction to Azure Monitor

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Monitor comprehensive solution **for collecting, analyzing, and acting on telemetry** from your cloud and on-premises environments

- Create Visual Dashboards
- Smart Alerts
- Automated Actions
- Log Monitoring

Many Azure services by default are already sending telemetry data to Azure Monitor





# Azure Administrator

Azure Monitor



## The Pillars of Observability





# The Pillars of Observability

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is Observability?

The ability to measure and understand how internal systems work in order to answer questions regarding performance, tolerance, security and faults with a system / application.

To obtain observability you need to use **Metrics**, **Logs** and **Traces**.

You have to use them together, using them in isolate does not gain you observability

### Metrics

A number that is measured over period of time

eg. If we measured the CPU usage and aggregated it over an a period of time we could have an **Average CPU metric**

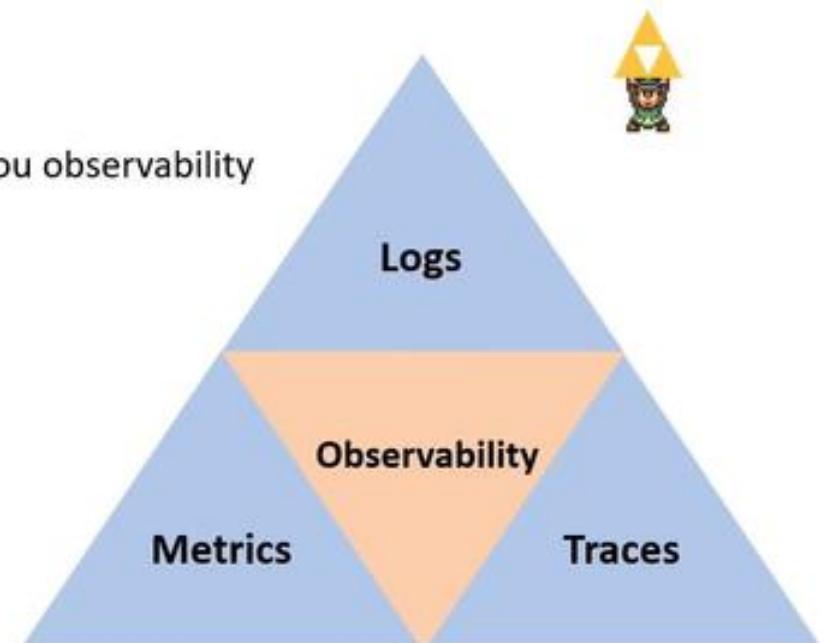
### Logs

A text file where each line contains event data about what happened at a certain time.

### Traces

A history of request that is travels through multiple Apps/services so we can pinpoint performance or failure.

Looks like they should have called it the **Triforce of Observability**





# Azure Administrator

Azure Monitor



## Anatomy of Azure Monitor

(A)  
SUBSCRIBE



# Anatomy of Azure Monitor

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

The **sources of common monitoring data** to populate datastores

Order by (Highest to Lowest)

Application

Operating System

Azure Resources

Azure Subscription

Azure Tenant

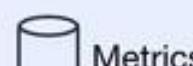
Custom Sources



Azure Monitor



Logs



Metrics

The **functions** that Azure monitor can perform

Insights



Application



Containers



VMs



Monitoring Solutions

Visualize



Dashboards



Views



Power BI



Workbooks

Analyze



Metric Analytics



Log Analytics

Respond



Alerts



Autoscale

Integrate



Logic Apps



Export APIs

The two fundamental data stores are **Metrics** and **Logs**





# Azure Administrator

Azure Monitor



# Sources Application

(A)  
SUBSCRIBE



# Azure Monitor – Sources

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

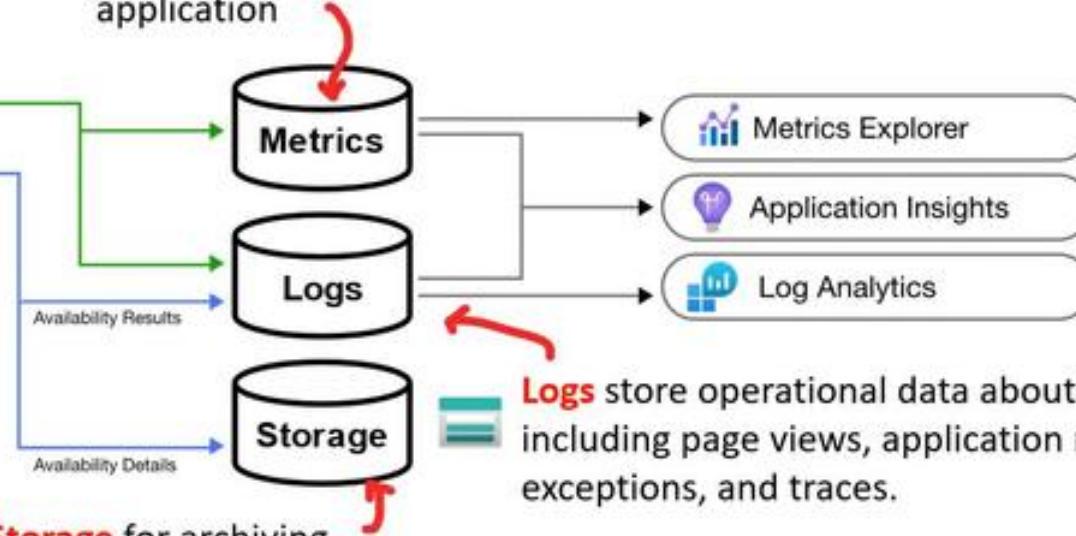
**Application Code:** performance and functionality of application and code.  
Performance traces, application logs, and user telemetry.

You need to install **Instrumentation Package** to collect data for Application Insights



**Availability Tests** responsiveness of your application from different locations on the public Internet

**Metrics** describing the **performance** and **operation** and custom metrics for your application



**Logs** store operational data about your application including page views, application requests, exceptions, and traces.

- Send application data to **Azure Storage** for archiving.
- Details of **availability test** stored
- Debug snapshot data that is captured for a subset of exceptions is stored in Azure Storage.





# Azure Administrator

Azure Monitor



# Sources Operation System

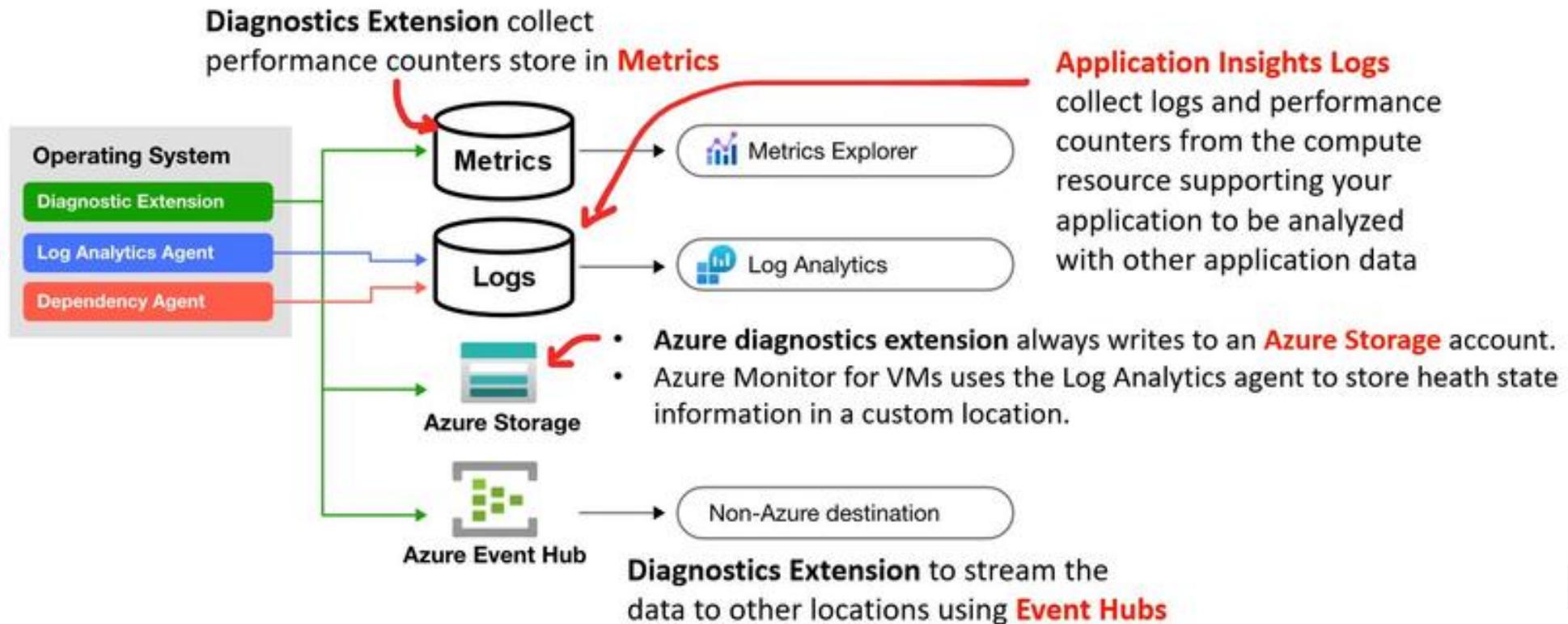
(A)  
SUBSCRIBE



# Azure Monitor – Sources

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

- **Log Analytics Agent** is installed for comprehensive monitoring
- **Dependency Agent** collects discovered data about processes running on the virtual machine and external process dependencies
- Agents can be installed on the OS for VMs running in Azure, On-premise or other cloud provider





# Azure Administrator

Azure Monitor



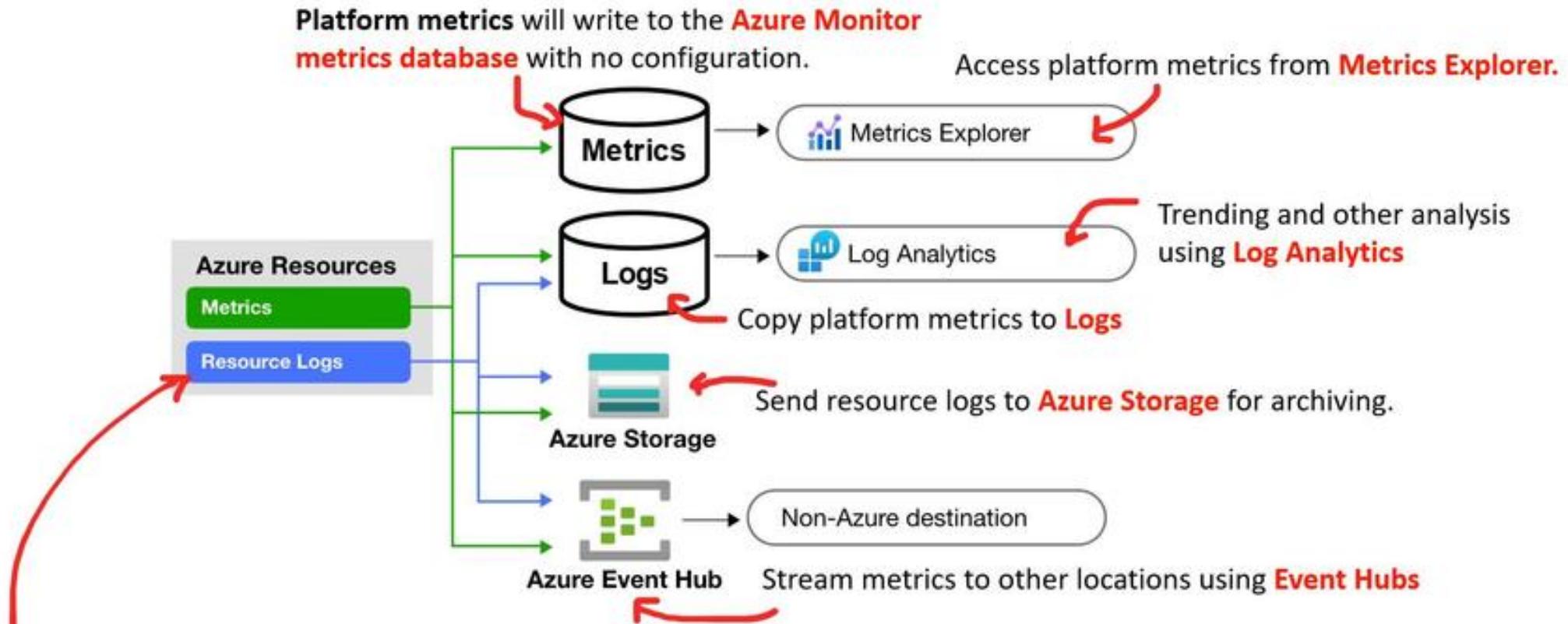
## Sources Azure Resources

(A)  
SUBSCRIBE



# Azure Monitor – Sources

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)



- Resource logs provide insights into the internal operation of an Azure resource.
- Resource logs are created automatically
- you must create a diagnostic setting to specify a destination for them to be collected for each resource





# Azure Administrator

Azure Monitor



# Source Azure Subscription

(A)  
SUBSCRIBE

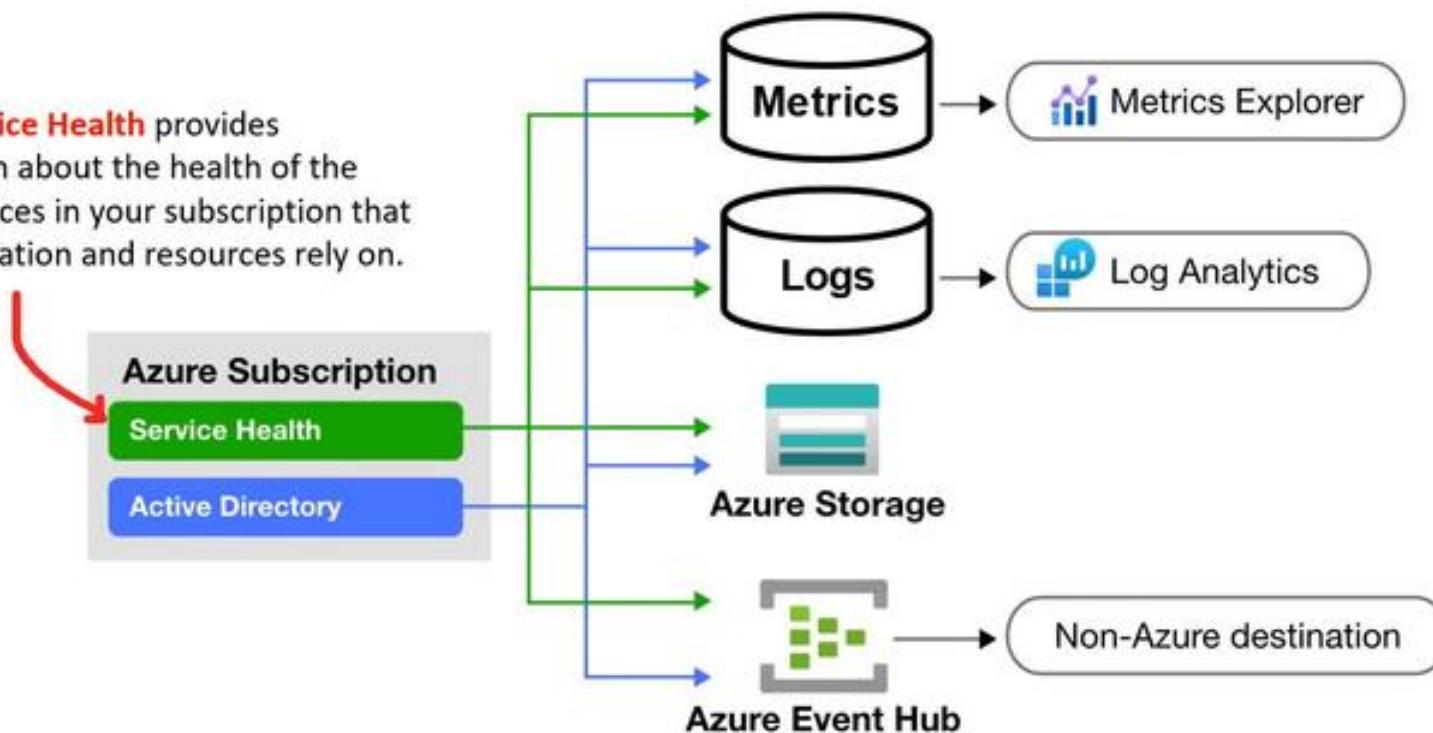


# Azure Monitor – Sources

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

**Azure subscription:** Telemetry related to the health and operation of your Azure subscription

Azure Service Health provides information about the health of the Azure services in your subscription that your application and resources rely on.





# Azure Administrator

Azure Monitor



## Sources Azure Tenant

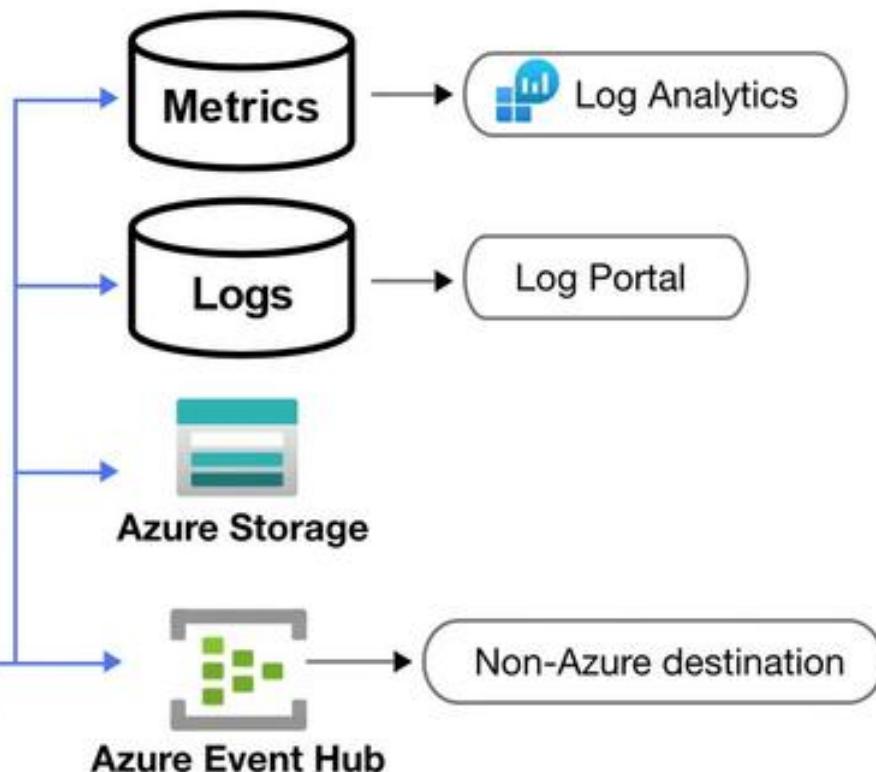
(A)  
SUBSCRIBE



# Azure Monitor – Sources

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

Telemetry related to your Azure tenant is collected from **tenant-wide services** such as **Azure Active Directory**.



**Azure Active Directory** reporting contains the history of sign-in activity and audit trail of changes made within a particular tenant.



# Azure Administrator

Azure Monitor



## Sources Custom Sources

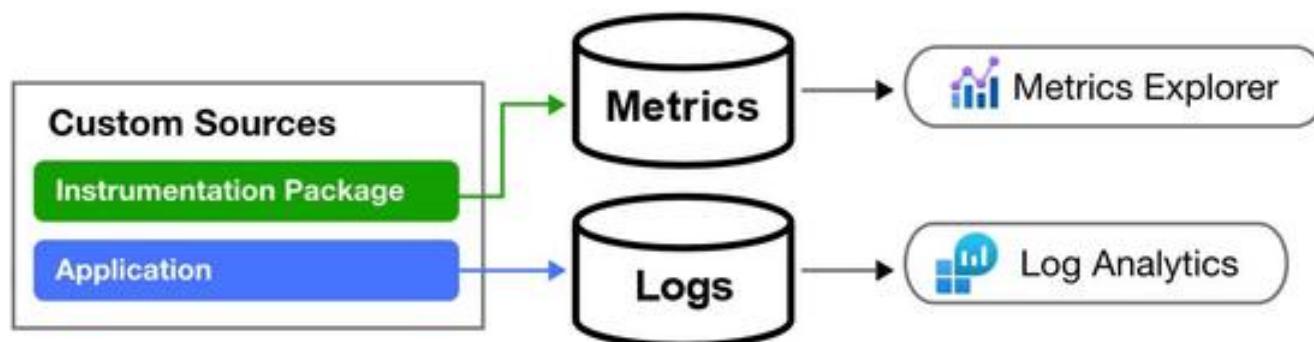
(A)  
SUBSCRIBE



# Azure Monitor – Sources

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

You may need to monitor other resources that have telemetry that can't be collected with the other data sources.  
For these resources, write this data to either Metrics or Logs using an **Azure Monitor API**.



Collect log data from any REST client and store in Log Analytics and Azure Monitor metrics database





# Azure Administrator

Azure Monitor



## Data Stores





# Azure Monitor – Data Stores

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Monitor collects **two fundamental** types of data from sources: **Logs** and **Metrics**

## Azure Monitor Logs

- collects and organizes log and performance data from monitored resources
- data logs are consolidated from different sources into **workspaces**
  - platform logs from Azure services,
  - log and performance data from virtual machines agents,
  - usage and performance data from applications can be consolidated
  - In a workspace so they can be analyzed together using a sophisticated query language capable of analyzing millions of records.
- Work with log queries and their results interactively using **Log Analytics** → 

## Azure Monitor Metrics

- collects numeric data from monitored resources into a **time series database**.
- Metrics are numerical values collected at regular intervals and describe some aspect of a system at a particular time
- lightweight and capable of supporting near real-time scenarios, useful for alerting and fast detection of issues
- You can analyze them interactively with **Metrics Explorer** → 





# Azure Administrator

Azure Monitor



## Log Analytics Workspaces





# Log Analytics Workspaces

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Log Analytics workspace** is a unique environment for Azure Monitor log data  
Each **workspace** has its own data repository and configuration, and data sources and solutions  
are configured to store their data in a particular **workspace**

The screenshot shows the Azure Log Analytics workspace interface for the workspace "examprologanalaytics". The left sidebar contains navigation links for General (Workspace summary, View Designer, Workbooks, Logs, Solutions, Usage and estimated costs, Properties, Service Map), Workspace Data Sources (Virtual machines, Storage accounts logs, System Center, Azure Activity log, Scope Configurations (Preview)), and a search bar. The main area displays a table of virtual machines:

Name	Log Analytics Connection	OS
MyTestVM	Not connected	Lin





# Azure Administrator

Azure Monitor



# Log Analytics

(A)  
ANSWER



# Log Analytics

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

Log Analytics is a tool in the Azure portal used to edit and run log queries with data in Azure Monitor Logs.

The screenshot shows the Azure Log Analytics workspace interface. On the left, there's a sidebar with 'Logs' and 'Demo' sections, and a 'Favorites' section listing various Azure services. The main area has tabs for 'Tables', 'Queries', and 'Filter'. A red arrow points from the text above to the 'Run' button in the top navigation bar. Below the navigation bar is a code editor window containing a KQL query:

```
1 ContainerInventory
2 | where TimeGenerated > ago(24h)
3 | limit 30
```

Below the code editor is a results table titled 'Completed' with columns: TimeGenerated (UTC), Computer, ContainerID, and Name. The table lists 10 records from November 26, 2020, at 1:40:01 PM. The last few rows of the table are:

TimeGenerated (UTC)	Computer	ContainerID	Name
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000	3962607dabc03ce171a799cd05076a0ebd7304bf39526cc82e9...	kbs_c1_purchasing-app-8Mf8c95...
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000		kbs_c2_purchasing-app-8Mf8c95...
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000		kbs_c3_purchasing-app-8Mf8c95...
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000	1efbbab5d1e91613514086093c1883da55e2fb788cefb8d07cd5c...	kbs_coredns_coredns-79766d06...
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000	787ab6945c4c4e9011b37b2237a20af33f304d5ed5841ab403...	kbs_minecraft_minecraft-redmond...
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000	02466930d5683f44145c14645580d12903093218a971ce64591...	kbs_kube-proxy_kube-proxy-zh4...
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000	89c2d3900fa7978ffea2599103578deed8e190088f2e057bd27...	kbs_azure-vm-mgmt-agent_azurin...
11/26/2020, 1:40:01.000 PM	aks-windows-19400979-vmss000000	85f9d9576798f76d88ef784ed9a0987cb1c74718bc50ade5fc...	kbs_azure-cni-networkmonitor_an...

Log Analytics uses a query language called KQL





# Azure Administrator

Azure Monitor



# Kusto

(A)  
SUBSCRIBE

# Kusto and Kusto Query Language (KSL)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Monitor Logs is based on Azure Data Explorer, and log queries are written using the same **Kusto query language (KQL)**

```
StormEvents
| where EventType == 'Flood' and State == 'WASHINGTON'
| sort by DamageProperty desc
| take 5
| project StartTime, EndTime, State, EventType, DamageProperty, EpisodeNarrative
```

KQL can be used in:

- Log Analytics
- Log alert rules
- Workbooks
- Azure Dashboards
- Logic Apps
- PowerShell
- Azure Monitor Logs API

Kusto is based on relational database management systems, and supports entities such as **databases**, **tables**, and **columns**.

Some query operators include

- calculated columns
- searching and filtering on rows
- group by-aggregates
- join functions

Kusto queries execute in the context of some **Kusto database** that is attached to a **Kusto cluster**.





# Azure Administrator

Azure Monitor



## Kusto Entities

(A)  
SUBSCRIBE

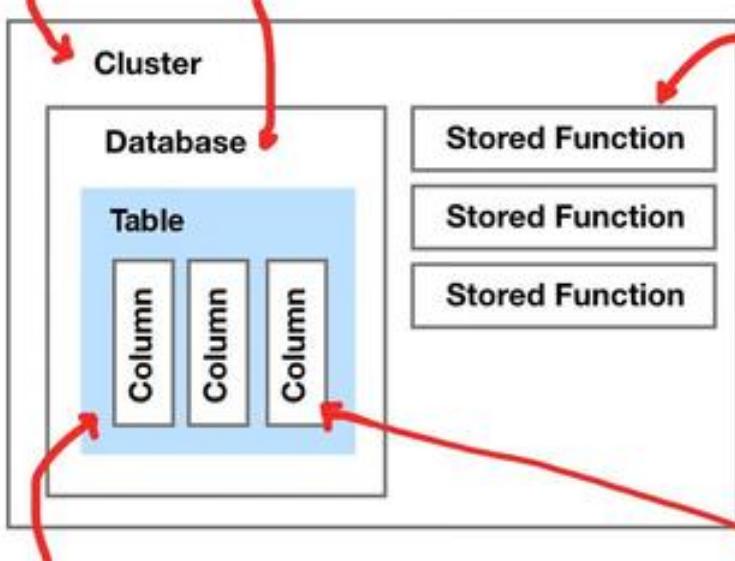
# Kusto Entities

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Kusto is generally composed of the following entities: **Clusters, Databases, Tables, Columns, Functions**

**Clusters** are entities that hold databases

**Databases** are named entities that hold tables and stored functions



**Tables** are named entities that hold data.

A table has an ordered set of columns, and zero or more rows of data, each row holding one data value for each of the columns of the table

**Stored functions** are named entities that allow reuse of Kusto queries or query parts.

External Table

**External tables** are entities that reference data stored outside Kusto database.  
External tables are used for exporting data from Kusto to external storage as well as for querying external data without ingesting it into Kusto.

**Columns** are named entities that have a scalar data type.

Columns are referenced in the query relative to the tabular data stream that is in context of the specific operator referencing them.





# Azure Administrator

Azure Monitor



## Scalar Data Types

(A)  
SUBSCRIBE

# Kusto Scalar Data Types

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What are Scalars?

Scalars are quantities that are fully described by a magnitude (or numerical value) alone

In Kusto, data types are used for various things:

- columns can have defined data type,
- Function parameters expect specific data types and there are

## What are Data Types?

A data type defines how a piece of data is interpreted eg. An Integer number could be a datatype

- **bool**, Boolean represents a **true** or **false** value
- **datetime**, **date** represents a date and/or time eg. **2015-12-31 23:59:59.9** Time is always stored in UTC timezone
- **decimal** represents a 128-bit wide, decimal number eg. **12.88**
- **Int** represents a signed, 32-bit wide, integer eg. **5**
- **long** represents a signed, 64-bit wide, integer
- **guid**, **uuid**, **uniqueid** represents a 128-bit globally-unique value eg. **74be27de-1e4e-49d9-b579-fe0b331d3642**
- **real** represents a 64-bit wide, double-precision, floating-point number
- **string** represents a Unicode string. Kusto strings are encoded in UTF-8 and by default are limited to 1MB eg. **"hello world"**
- **Timespan** represents a time interval eg. **2d = 2 days, 30m = 30 minutes, 1tick = 100 nano seconds**
- **Dynamic** A special datatype that can be:
  - Accept primitive scalar data type eg. **bool, datetime, guid, int, long, real, string, timespan**
  - Be an array of data types eg. **[1,2,3,"hello"]**
  - Be a property bag of data types **{"a":1, "b":{"a":2}}**
- **Null** is special value that represents a missing value. Any Datatype can hold a value of null





# Azure Administrator

Azure Monitor



## Control Commands

(A)  
SUBSCRIBE

# Kusto Control Commands

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

**Control commands** can modify data and metadata and has its own syntax different from KQL

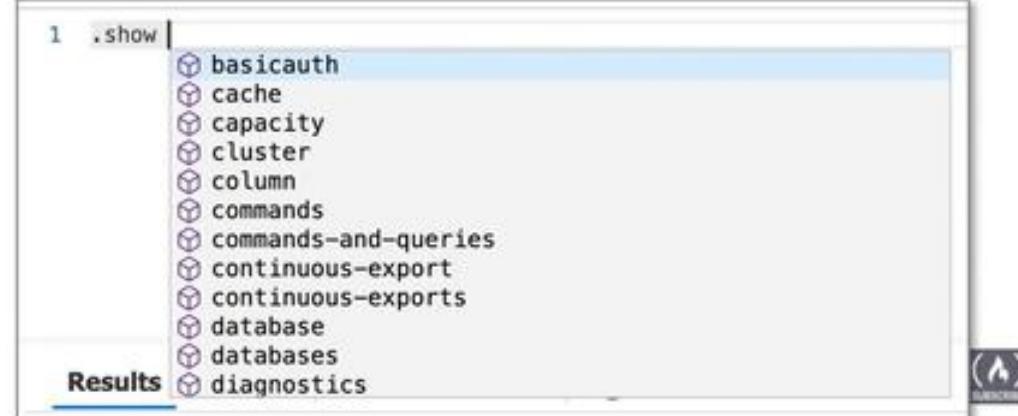
The following control command creates a new Kusto table with two columns

```
.create table Logs (Level:string, Text:string)
```



A very common control command is “.show” for example this will count all tables

```
.show tables  
| count
```





# Azure Administrator

Azure Monitor



# Functions



# Kusto Functions

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Functions** are reusable queries or query parts. Kusto supports several kinds of functions:

**Stored functions**, which are **user-defined functions** that are stored and managed as one kind of a database's schema entities.

User-defined function belongs to one of two categories:

- Scalar functions (input scalar datatypes, and outputs scalar datatypes)
- Tabular functions (in tabular data, and outputs tabular data)

**Query-defined functions**, which are **user-defined functions** that are defined and used **within the scope of a single query**.

**Built-in functions**, which are hard-coded (defined by Kusto and cannot be modified by users)

- **Special functions** selects Kusto entities eg. **cluster()**
- **Aggregation functions** performs a calculation on a set of values, and returns a single value eg. **count()**
- **Windows functions** operate on multiple rows (records) in a row set at a time. eg. **row\_number()**

```
cluster('help').database('Sample').SomeTable
```

```
StormEvents  
| where State startswith "W"  
| summarize Count=count() by State
```

```
range a from 1 to 10 step 1  
| sort by a desc  
| extend rn=row_number()
```





# Azure Administrator

Azure Monitor



## Scalar Operators

(A)  
SUBSCRIBE

# Kusto Scalar Operators

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

These perform comparisons against Scalar Datatypes

## Bitwise (binary) operators

- binary\_and
- binary\_not
- binary\_or
- binary\_shift\_left
- binary\_shift\_right
- binary\_xor

## Logical (binary) operators

- Equality =
- Inequality !=
- Logical and and
- Logical or or

## Datetime /timespan arithmetic

- add or subtract datetime eg. **datetime(1997-06-25) - datetime(1910-06-11)**
- add, subtract, divide or multiple timespan eg. **1d + 2d**

## Numerical operators (works on int, long and real)

- Add +, Subtract -, Multiply \*, Divide /
- Modulo %
- Less <, Greater >, Equal ==, Not Equal !=, Less or Equal <=, Greater or Equal >=
- Equals to one of the elements in
- Not equals to any of the elements !in

## String operators

- == , != , =~ , !~, has, has, hasprefixhasprefix, hassuffix , contains, startswith, endswith, matches, in, has\_any (many more...)

**between operator** Matches the input that is inside the inclusive range.

- Table1 | where Num1 between (1 .. 10)
- Table1 | where Time between (datetime(2017-01-01) .. datetime(2017-01-01))





# Azure Administrator

Azure Monitor



## Tabular Operators

(A)  
SUBSCRIBE

# Kusto Tabular Operators

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

These perform comparisons against a bunch of rows. There are a lot of tabular operators

**count** — Returns the count of rows in the table.

```
StormEvents | count
```

**take** — returns up to the specified number of rows of data

```
StormEvents | take 5
```

**sort** — Sort the rows of the input table into order by one or more columns.

```
StormEvents  
| where EventType == 'Flood'  
| sort by DamageProperty desc  
| take 5  
| project StartTime, EndTime, State, EventType
```

**project** — returns a specific set of columns.

```
StormEvents  
| take 5  
| project StartTime, EndTime, State, EventType
```

**where** — Filters a table to the subset of rows that satisfy a predicate.

```
StormEvents  
| where EventType == 'Flood' and State == 'WASHINGTON'  
| take 5  
| project StartTime, EndTime, State, EventType
```



# Kusto Tabular Operators

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

 **top** — returns the first  $N$  records sorted by the specified columns

```
StormEvents  
| where EventType == 'Flood'  
| top 5 by DamageProperty desc  
| project StartTime, EndTime, State, EventType
```

 **extend** — creates a new column by computing a value

```
StormEvents  
| where EventType == 'Flood'  
| top 5 by DamageProperty desc  
| extend Duration = EndTime - StartTime  
| project StartTime, EndTime, Duration
```

 **summarize** — Aggregates groups of row

```
StormEvents  
| summarize event_count = count() by State
```

 **render** — Renders results as a graphical output

```
StormEvents  
| summarize event_count=count() by bin(StartTime, 1d)  
| render timechart
```





# Azure Administrator

Azure Monitor



## Metrics Explorer

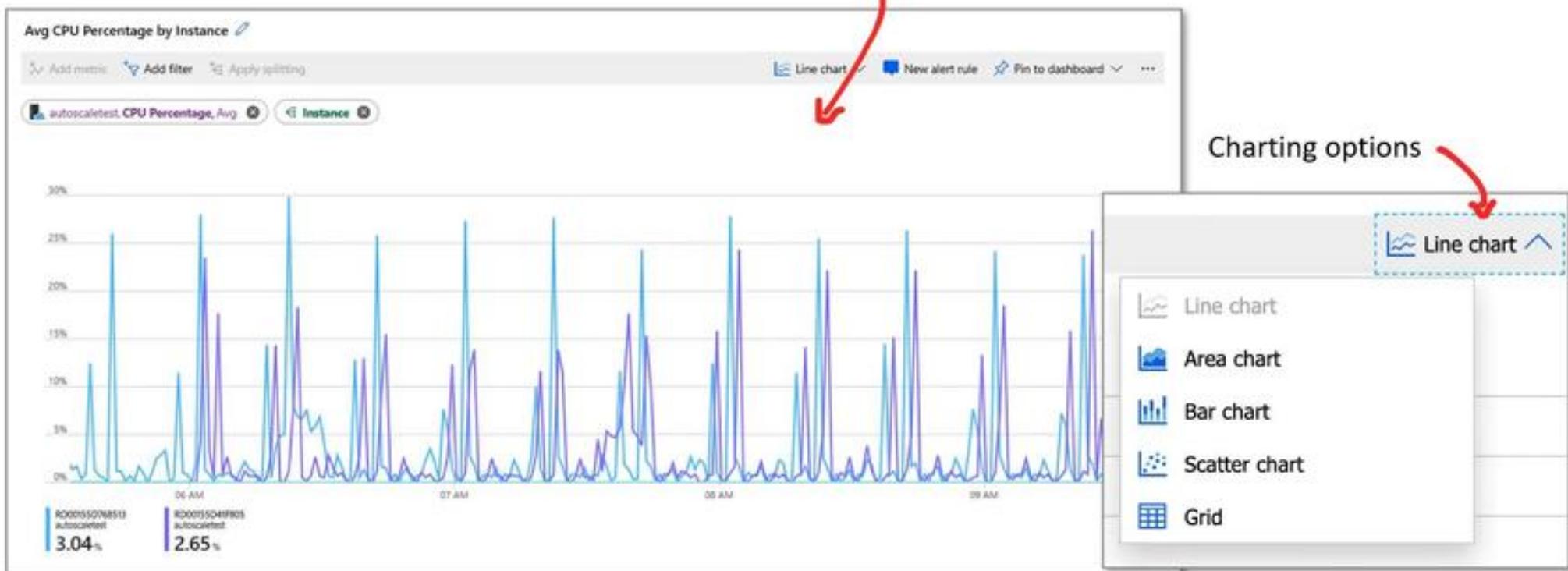
(A)  
SUBSCRIBE



# Metrics Explorer

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

Metrics Explorer is a sub-service of Azure Monitor that allows you to **plot charts**, **visualize correlating trends**, and **investigate spikes and dips** in metrics values.





# Metrics Explorer

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

To visualize a metric you need to *define*:

**Scope:** You can select \*resource(s)  
Eg. VM, StorageAccount

**Metric:** The actual value you  
are interested in visualizing

Metric	Aggregation
Availability	Min
CAPACITY	
Used capacity	
TRANSACTION	
Availability	
Egress	
Ingress	
Success E2E Latency	
Success Server Latency	

The screenshot shows the Metrics Explorer search interface. A red arrow points from the text "Namespace: a specific group of metric data within a resource" to the "Metric Namespace" dropdown, which is set to "Account". Another red arrow points from the text "Aggregation: how you want group the values into the final result" to the "Aggregation" dropdown, which is set to "Min".

**Namespace:** a specific group of metric  
data within a resource

Metric Namespace	Metric
Account	Availability
Blob	
File	
Queue	
Table	

**Aggregation:** how you want group  
the values into the final result

Aggregation
Min
Avg
Max





# Azure Administrator

Azure Monitor



## Azure Alerts





# Azure Alerts

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Alerts** notify you when issues are found with your infrastructure or application  
They allow you to **identify** and **address** issues before the users of your system notice them.

Azure has 3 kinds of Alerts

1. Metric Alerts
2. Log Alerts
3. Activity Log Alerts

When an alert is triggered you can be notified  
and have it take action



# Azure Alerts

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

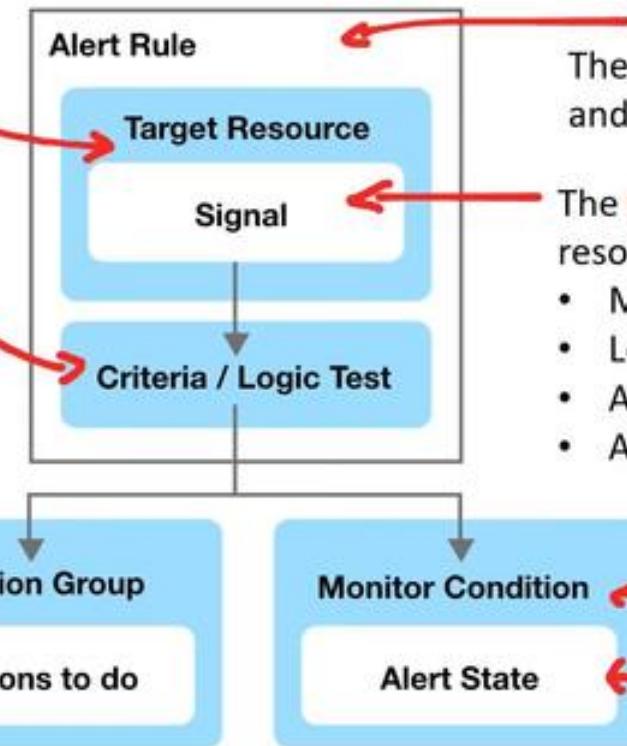
A resource such as an Azure VM is designated as the **Target Resource** and it emits a **signal**

The signal is evaluated against a **criteria or logical test** to determine if the alert has been triggered  
eg. Percentage CPU > 70%

An **action group** contains actions to be taken when alert is triggered

An **action** could be a:

Automation runbook, Azure Function, ITSM, Logic App, Webhooks or Secure Webhooks



The **Alert Rule** defines who should we monitor and when should we react

The **Signal** is a data payload emitted from the resource that could be the following types:

- Metric
- Log
- Activity log
- Application Insights

The current state of your alert  
**Monitor Condition** is set by the system  
**Alert state** is set by the user





# Azure Administrator

Azure Monitor



# Azure Dashboards





# Azure Dashboards

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Dashboards** are a virtual workspaces to **quickly launch tasks for day-to-day operations and monitor resources**  
Build custom dashboards based on projects, tasks, or user roles

The screenshot shows the Azure Dashboard creation interface. On the left, a sidebar titled "Tile Gallery" lists various tile types with "Add" buttons. A red arrow points from this sidebar to the "Metrics chart" tile on the main dashboard. The main dashboard is titled "MyDashboard" and contains several tiles:

- "MyNetworkSecurity..." (Network security group)
- "Top 10 Worst St... STAR TREK DEEP SPACE NINE WORST EPISODES" (Custom content tile with a video thumbnail)
- "Help + support" (User support tile)
- "Eastern Standard Time" (Clock tile showing 2:07 PM, Thursday, November 26, 2020)
- "Metrics chart" (Metrics chart tile showing a line graph from Nov 26 to Nov 27, UTC, with values ranging from 0 to 100. An "Edit in Metrics" button is visible below the graph.)

The "Metrics chart" tile has an "Edit" button above it, which is highlighted with a red arrow. Below the "Edit" button is a preview area showing the current state of the metrics chart.



# Azure Administrator

Azure Monitor



# Azure Workbooks

(A)  
MORE



# Azure Workbooks

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Workbooks** provide a flexible **canvas for data analysis** and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure and combine them into unified interactive experiences.

It tells a **story** about the performance and availability about your applications and services.



Workbooks are temporary workspaces to define a document-like format with visualization intertwined to help investigate and discuss performance.





# Azure Administrator

Azure Monitor



## Application Insights

(A)  
ANSWER



# Application Insights

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Application Insights** is an **Application Performance Management (APM)** service  
It is a sub-service of Azure Monitor.

## What is an APM?

Monitoring and management of **performance and availability** of software apps. APM strives to detect and diagnose complex application performance problems to maintain an expected level of service.

## Why use Application Insights?

- automatically detect performance anomalies
- includes powerful analytics tools to help you diagnose issues and to understand what users do with your app
- designed to help you continuously improve performance and usability
- works for apps on .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud.
- Integrates with your DevOps process
- can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center



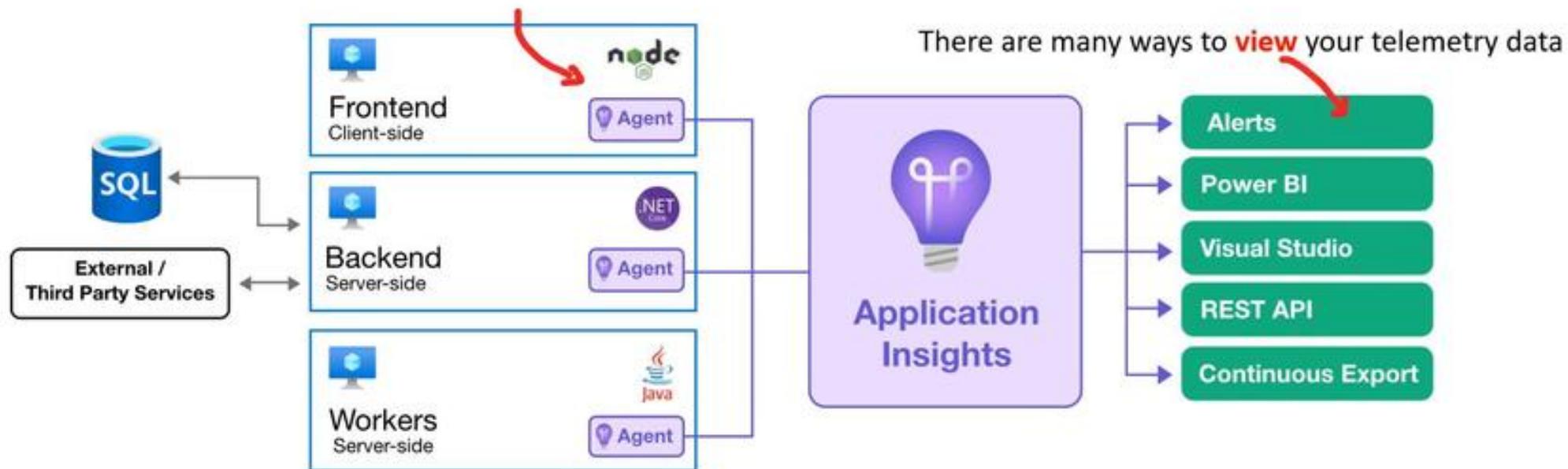


# Application Insights

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

To use Application Insights **you need to instrument your application.**

- To instrument you need to install the instrument package (SDK)
- Or enable Application Insights using the Application Insights Agents when supported



- Apps can be instrumented from anywhere
- When you set up Application Insights monitoring for your web app, you create an Application Insights *resource* in Microsoft Azure.
- You open this resource in the Azure portal in order to see and analyze the telemetry collected from your app.
- The resource is identified by an instrumentation key (ikey)





# Application Insights

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What does Application Insights Monitor?

- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates
- Exceptions
- Page views and load performance
- AJAX calls
- User and session counts
- Performance counters
- Host diagnostics
- Diagnostic trace logs
- Custom events and metrics

## Where do I see my telemetry?

- Smart detection and manual alerts
- Application map
- Profiler
- Usage Analysis
- Diagnostic search for instance data
- Metrics Explorer for aggregated data
- Dashboards
- Live Metrics Stream
- Analytics
- Visual Studio
- Snapshot debugger
- Power BI
- REST API
- Continuous Export





# Azure Administrator

Azure Monitor



## Azure Monitor CheatSheet



# Azure Monitor *CheatSheet*



Azure Monitor comprehensive solution **for collecting, analyzing, and acting on telemetry** from your cloud and on-premises environments

- Create Visual Dashboards
- Smart Alerts
- Automated Actions
- Log Monitoring

To obtain ~~observability~~ you need to use **Metrics, Logs and Traces**.

- You have to use them together, using them in isolate does not gain you observability
  - **Metrics:** A number that is measured over period of time
  - **Logs:** A text file where each line contains event data about what happened at a certain time.
  - **Traces:** A history of request that is travels through multiple Apps/services so we can pinpoint performance or failure.

Azure Monitor collects **two fundamental** types of data from sources: **Logs and Metrics**

**Azure Monitor Logs:** collects and organizes log and performance data from monitored resources

- data logs are consolidated from different sources into **workspaces**
  - platform logs from Azure services,
  - log and performance data from virtual machines agents,
  - usage and performance data from applications can be consolidated
  - In a workspace so they can be analyzed together using a sophisticated query language capable of analyzing millions of records.
- Work with log queries and their results interactively using **Log Analytics**

**Azure Monitor Metrics** collects numeric data from monitored resources into a **time series database**.

- Metrics are numerical values collected at regular intervals and describe some aspect of a system at a particular time
- lightweight and capable of supporting near real-time scenarios, useful for alerting and fast detection of issues
- You can analyze them interactively with **Metrics Explorer**



# Azure Monitor *CheatSheet*

Exam Pro

**Log Analytics** is a tool in the Azure portal used **to edit and run log queries** with data in **Azure Monitor Logs**.

- Log Analytics uses a query language called **KQL**

**Log Analytics workspace** is a unique environment for Azure Monitor log data

- Each **workspace** has its own data repository and configuration, data sources and solutions are configured to store their data in a **workspace**

**Azure Monitor Logs** is based on Azure Data Explorer, and log queries are written using the same **Kusto query language (KQL)**

- KQL can be used in: Log Analytics, Log alert rules, Workbooks, Azure Dashboards, Logic Apps, PowerShell, Azure Monitor Logs API
- Kusto is based on relational database management systems, and supports entities such as **databases**, **tables**, and **columns**.

- Some query operators include
  - calculated columns, searching and filtering on rows, group by-aggregates, join functions
  - Kusto queries execute in the context of some **Kusto database** that is attached to a **Kusto cluster**.
  - Kusto is generally composed of the following entities: **Clusters**, **Databases**, **Tables**, **Columns**, **Functions**
    - **Clusters** are entities that hold databases
    - **Databases** are named entities that hold tables and stored functions
    - **Stored functions** are named entities that allow reuse of Kusto queries or query parts.
    - **Tables** are named entities that hold data.
    - **Columns** are named entities that have a scalar data type.
    - **External tables** are entities that reference data stored outside Kusto database.

- **Metrics Explorer** is a sub-service of Azure Monitor that allows you to **plot charts**, **visualize correlating trends**, and **investigate spikes and dips** in **metrics values**. To visualize a metric you need to *define*:

- **Scope**: You can select \*resource(s)
- **Namespace**: a specific group of metric data within a resource
- **Metric**: The actual value you are interested in visualizing
- **Aggregation**: how you want group the values into the final result



# Azure Monitor *CheatSheet*



Alerts notify you when issues are found with your infrastructure or application

- They allow you to **identify** and **address** issues before the users of your system notice them.
- Azure has 3 kinds of Alerts
  1. Metric Alerts
  2. Log Alerts
  3. Activity Log Alerts

Azure Dashboards are a virtual workspaces to **quickly launch tasks for day-to-day operations and monitor resources**

Azure Workbooks provide a flexible **canvas for data analysis** and the creation of rich visual reports within the Azure portal.

- It tells a **story** about the performance and availability about your applications and services.

Application Insights is an **Application Performance Management (APM)** service It is a sub-service of Azure Monitor.

- automatically detect performance anomalies
- includes powerful analytics tools to help you diagnose issues and to understand what users do with your app
- designed to help you continuously improve performance and usability
- works for apps on a for .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud.
- Integrates with your DevOps process
- can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center

To use Application Insights **you need to instrument your application**.

- To instrument you need to install the instrument package (SDK)
- Or enable Application Insights using the Application Insights Agents when supported
- Apps can be instrumented from anywhere
- When you set up Application Insights monitoring for your web app, you create an Application Insights *resource* in Microsoft Azure.
- You open this resource in the Azure portal in order to see and analyze the telemetry collected from your app.
- The resource is identified by an instrumentation key (ikey)





# Azure Administrator

Azure Backup

## Azure Backup Service





# Azure Backup Service

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Backup Service is a backup layer that spans many Azure services.

You **won't find it** by searching based on the service name

Azure Backup is **directly integrated** with Azure Services

## What can I backup?

- On-Premise
- Azure VMs
- Azure Files
- SQL Server (within Azure VM)
- SAP HANNA databases (within Azure VM)
- Azure Database for PostgreSQL server

## Why use Azure Backup?

- Offload on-premises backups
- Backup your VMs
- Scales Easily
- Get unlimited data transfer (no limit and no charge)
- Keep data secure (built-in security at-rest and in-transit)
- Centralized monitoring and management
- App Consistent Backups (restore apps back to an exact state)
- Automatic Storage Management
- Multiple Storage Options





# Azure Administrator

Azure Backup

## MARS Vaults





# Azure Recovery Service Vault

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Azure Recovery Services (ARS) vault** is a **storage entity** in Azure that **houses data** and **recovery points** created over time.

The data is copies of data, or configuration information for VMs, workloads, servers, or workstations.

Backup data for various Azure services: eg.

- IaaS VMs (Linux or Windows)
- Azure SQL databases.

Recovery Services vaults **supports**:

- **System Center (Data Protection Manager) DPM**
- **Windows Server**
- **Azure Backup Server**
- and more.

Recovery Services vaults has the following **features**:

- Enhanced capabilities to help secure backup data
- Central monitoring for your hybrid IT environment
- Azure role-based access control (Azure RBAC)
- Soft Delete
- Cross Region Restore





# Azure Administrator

Azure Backup

## Mars Agent





# MARS agent

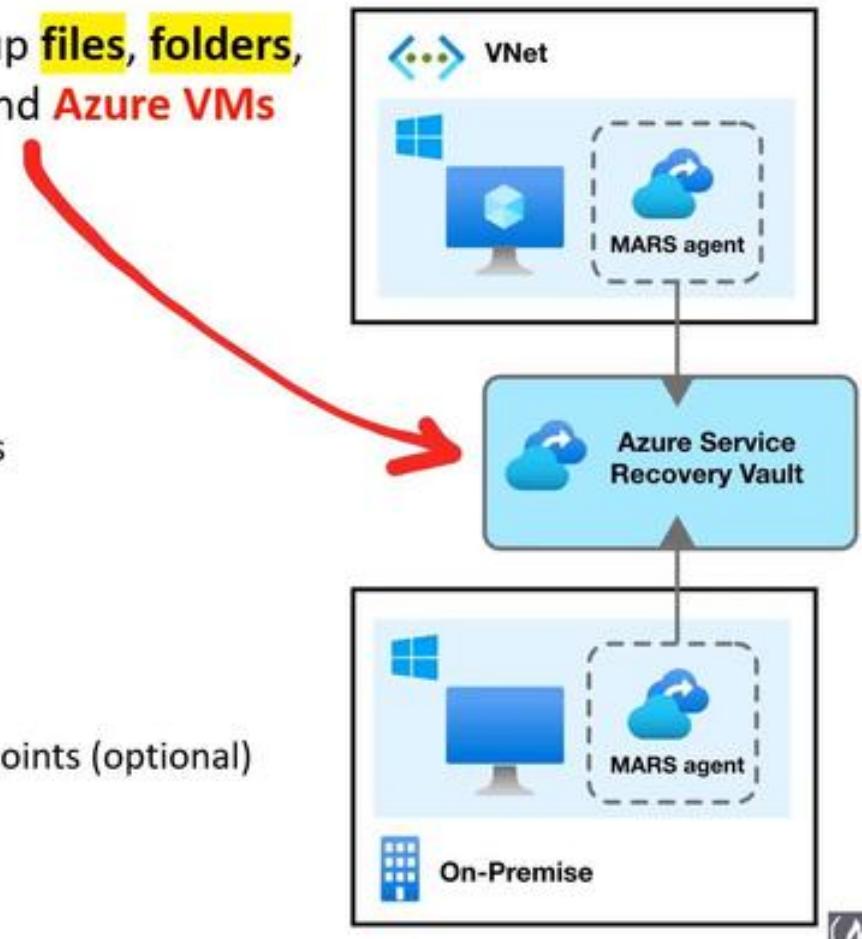
Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Microsoft Azure Recovery Services (MARS) agent can back up **files, folders, and system state** from Windows **on-premises machines** and **Azure VMs**

Backups are stored in a Recovery Services vault in Azure

MARS agent is *also known as* the Azure Backup agent

The MARS agent does not support Linux operating systems



To install the agent and perform backups you'll need to:

- create an Azure Recovery Services vault
- Create a backup policy within the vault
- Configure secure route for back eg. ExpressRoutes or Private Endpoints (optional)
- Download the MARS agent
- Install and register the Agent to your Windows machine.



# Azure Administrator

Azure Backup

## Backup Policy





# Azure Backup Policy

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

To create a backup policy you choose a **datasource** type:

- Azure VMs or PSQL database

Datasource type  Azure Virtual machines

Azure Virtual machines  
Azure Database for PostgreSQL servers

Choose the **frequency**

**How many** snapshots you want to retain

Choose the **time range** for your retention

## Backup policy

Policy name \*  MyBackupPolicy

### Backup schedule

Frequency \*  Daily

Time \*  3:00 AM

Timezone \*

(UTC) Coordinated Universal Time

### Instant Restore

Retain instant recovery snapshot(s) for

2 Day(s)

### Retention range

Retention of daily backup point.

At

3:00 AM

For

180 Day(s)

Retention of weekly backup point.

On \*

Sunday

At

3:00 AM

For

12 Week(s)

Retention of monthly backup point.

Week Based  Day Based

On \*

Day \*

At

3:00 AM

For

60 Month(s)

Retention of yearly backup point.

Week Based  Day Based

In \*

On \*

At

3:00 AM

For

10 Year(s)





# Azure Administrator

Azure Backup

## Azure Site Recovery



# Azure Site Recovery

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Site Recovery (ASR) is a **hybrid** (on-premise to cloud) backup solution for **site-to-site recovery**.

ASR is one of the tools useful for your **business continuity and disaster recovery (BCDR) strategy**

Site Recovery *replicates* workloads from a primary site to a secondary site.

In case primary site suffers a failure, Site Recovery will **fail-over** to the secondary site to ensure continuity of services

Site Recover can replicate:

- Azure VMs between regions (cross region replication)
- Windows, Any OS and Linux
- On-premise to Azure
- Between other Cloud Service Providers eg AWS to Azure
- VMWare, Hyper-V or Physical Machines

- **Recovery Point Objectives (RTO)** how quickly you can recover a backup after experiencing a disaster
- **Recovery Time Objectives (RPO)** how often you backup (how much data lost can you tolerate?)





# Azure Administrator

Azure Backup

## Create a Recovery Services Vault



Follow Along

The screenshot shows the 'Create Recovery Services vault' wizard in the Microsoft Azure portal. The title bar indicates 'Microsoft Azure' and the path 'Home > Backup center > Start Create Vault'. The main section is titled 'Create Recovery Services vault' with a 'Preview' link. Below it, there are tabs for 'Basics', 'Tags', 'Review + create', and 'Create'. The 'Basics' tab is selected. Under 'Project Details', it says 'Select the subscription and the resource group in which you want to create the vault.' A dropdown menu for 'Subscription' shows 'Azure subscription 1' and 'picard' with a 'Create new' option. Under 'Instance Details', there are fields for 'Vault name' (with placeholder 'Enter the name for your vault.') and 'Region' (set to 'Central US'). At the bottom right of the screenshot, there is a small '(A)' icon with the word 'SUBSCRIBE' below it.



# Azure Administrator

Azure Backup



## Backup CheatSheet

# Azure Backup *CheatSheet*

Exam Pro

Azure Backup Service is a backup layer that spans many Azure services.

- On-Premise, Azure VMs , Azure Files, SQL Server (via Azure VM), SAP HANNA databases (via Azure VM), Azure Database for PostgreSQL
- Azure Backup is **directly integrated** with Azure Services (You **won't find it** by searching based on the service name)
- Offload on-premises backups
- Backup your VMs
- Scales Easily
- Get unlimited data transfer (no limit and no charge)
- Keep data secure (built-in security at-rest and in-transit)
- Centralized monitoring and management
- App Consistent Backups (restore apps back to an exact state)
- Automatic Storage Management
- Multiple Storage Options

Azure Recovery Services (ARS) vault is a **storage entity** in Azure that **houses data** and **recovery points** created over time.

- Enhanced capabilities to help secure backup data
- Central monitoring for your hybrid IT environment
- Azure role-based access control (Azure RBAC)
- Soft Delete
- Cross Region Restore

Microsoft Azure Recovery Services (MARS) agent backups **files**, **folders**, and **system state** from Windows **on-premises machines** and **Azure VMs**

- Backups are stored in a Recovery Services vault in Azure
- MARS agent is *also known as* the Azure Backup agent
- The MARS agent does not support Linux operating systems
- **Azure Site Recovery (ASR)** is a **hybrid** (on-premise to cloud) backup solution for **site-to-site recovery**.





# Azure Administrator

Azure Container Instances



## Introduction to Azure Container Instances



Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure Container Instances (ACI)



**package, deploy, and manage** cloud applications using **containers**  
Fully Managed Docker as a Service



# Introduction to ACI

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Container Instances (ACIs) allow you to **launch containers** without the need to worry about configuring or managing the underlying virtual machine

Azure Container Instances is designed for isolate containers:

- simple applications
- task automation
- build jobs

- Containers can be provisioned **within seconds** where VMs can take several minutes
- Containers are **billed per second** where VMs are billed per hour (greater savings)
- Containers have **granular and custom sizing of vCPUs, Memory and GPUs** where VMs sizes are predetermined
- ACI can deploy both **Windows** and **Linux** containers
- You can **persist storage with Azure Files** for your ACI containers
- ACIs are accessed via a fully qualified domain name (FQDN) eg *customlabel.azureregion.azurecontainer.io*.

Azure provides Quickstart images to start launching example applications but you can also **source** containers from:

- Azure Container Registry
- Docker Hub
- Privately Hosted Container Registry

Image source \*

Quickstart images  
 Azure Container Registry  
 Docker Hub or other registry





# Introduction to ACI

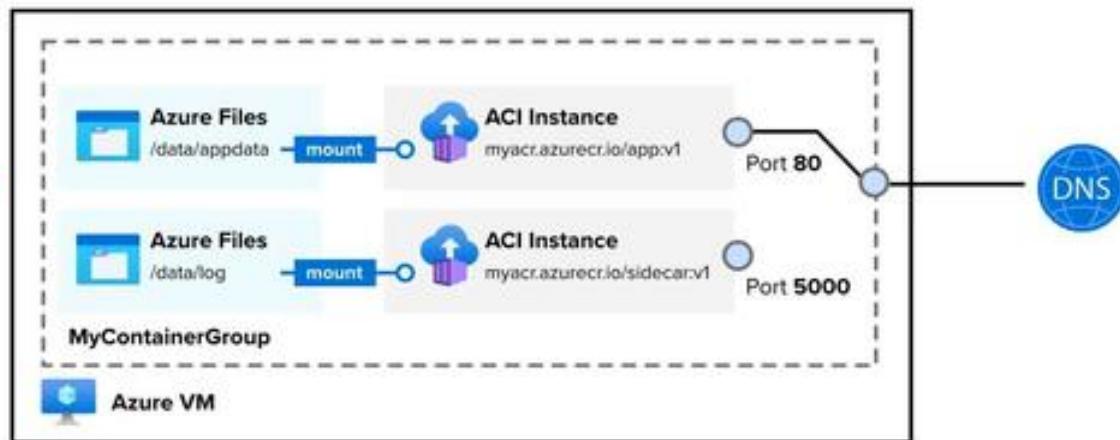
Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

**Container Groups** are collection of containers that get scheduled on the same host machine.

The containers in a container group share:

- lifecycle
- Resources
- local network
- storage volumes

*Container Groups are similar to a Kubernetes pod*



*Multi-container groups **currently support only Linux** containers.*

There are two ways to deploy a multi-container group:

- **Resource Manager Template (ARM template)** — when you need to deploy additional Azure service resources
- **YAML File** — when your deployment includes only container instances.





# Azure Administrator

Azure Container Instances



## Container Restart Policies





# Container Restart Policies

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

A container restart policy specifies what a container should do when their process has completed. Azure Container Instances has 3 restart-policy options:

- **Always** (default) Containers are **always restarted**. Suited for long running tasks eg. **web-servers**
- **Never** Containers **run one time only**. Suited for one off tasks. eg. **background jobs**
- **OnFailure** Containers that encounter an error

The screenshot shows the 'Advanced' tab of a container configuration page. The 'Restart policy' dropdown is open, showing four options: 'On failure' (selected), 'On failure', 'Always', and 'Never'. The 'On failure' option is highlighted with a blue border.

Restart policy
On failure
On failure
Always
Never



# Azure Administrator

Azure Container Instances



## Container Environment Variables





# Container Environment Variables

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Environment variables (Env Vars) allow you to pass configuration details to your containers.

Environment variables can be set via the **Azure Portal**, CLI or PowerShell

Environment variables	
Key	Value
STRIPE_SECRET_KEY	pk_test_Y3n003t2BIP0HD6JHN87L1eE
ENV	production
fruit	banana

## Secured Environment Variables

By default Environment Variables are stored in plaintext.  
If you need to secure your environment variables you  
can use the **--secure-environment-variables** flag

```
az container create \
--resource-group aci-resource-group \
--name aci-demo-secure \
--image exampro/rails:backend \
--ip-address Public \
--location eastus \
--secure-environment-variables \
STRIPE_SECRET_KEY=$STRIPE_SECRET_KEY
```





# Azure Administrator

Azure Container Instances



## Container Persistent Storage





# Container Persistent Storage

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Containers are **stateless** by default.

When a container crashes or stops all state is loss.

To persist state you need to **mount** an external volume

You can mount **the following external volumes:**

- Azure Files (file share)
- Secret volume
- Empty Directory
- Cloud git repo

To mount a file volume you need do this via PowerShell or CLI and specify the **details** to mount the drive

```
az container create \
--resource-group exampro-resource-group \
--name my-app \
--image exampro/web-app \
--location eastus \
--ports 80 \
--ip-address Public \
--azure-file-volume-account-name $STORAGE_ACCOUNT_NAME \
--azure-file-volume-account-key $STORAGE_KEY \
--azure-file-volume-share-name my-fileshare \
--azure-file-volume-mount-path /aci/logs/
```





# Azure Administrator

Azure Container Instances



## Container Troubleshooting





# Container Troubleshooting

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

To troubleshoot a container you can pull logs with **az container logs**

```
az container logs \  
  --resource-group exampro \  
  --name prod-web-app
```

To get diagnostic information during container startup use the **az container attach**

```
az container attach \  
  --resource-group exampro \  
  --name prod-web-app
```

To start an interactive container run **az container exec**

```
az container exec \  
  --resource-group exampro \  
  --name my-web-app \  
  --exec-command /bin/sh
```

To get metrics such as CPU usage **az monitor metrics list**

```
az monitor metrics list \  
  --resource $CONTAINER_ID \  
  --metric CPUUsage \  
  --output table
```





# Azure Administrator

Azure Container Instances



## Create an Azure Container Instances



Follow Along

Search resources, services, and docs (0+)

### Create container instance

Basics Networking Advanced Tags Review + create

Choose between three networking options for your container instance:

- **Public**: will create a public IP address for your container instance.
- **Private**: will allow you to choose a new or existing virtual network for your container for Windows containers.
- **None**: will not create either a public IP or virtual network. You will still be able to access via command line.

Networking type

Public  Private  None

DNS name label

Ports

Ports protocol

80

TCP





# Azure Administrator

Azure Container Instances



## ACI CheatSheet



# Azure Container Images *CheatSheet*

Exam Pro

Azure Container Instances (ACIs) allow you to **launch containers** without the need to worry about configuring or managing the underlying virtual machine

Azure Container Instances is designed for isolate containers:

- simple applications
- task automation
- build jobs

Containers can be provisioned **within seconds** where VMs can take several minutes

Containers are **billed per second** where VMs are billed per hour (greater savings)

Containers have **granular and custom sizing of vCPUs, Memory and GPUs** where VMs sizes are predetermined

ACI can deploy both **Windows** and **Linux** containers

You can **persist storage with Azure Files** for your ACI containers

ACIs are accessed via a fully qualified domain name (FQDN) eg *customlabel.azureregion.azurecontainer.io*.

**Container Groups** are collection of containers that get scheduled on the same host machine.

- The containers in a container group share: Lifecycle, Resources, local network, storage volumes
- Container Groups are similar to a Kubernetes pod
- Multi-container groups currently support only Linux containers.

There are two ways to deploy a multi-container group:

- **Resource Manager Template (ARM template)** — when you need to deploy additional Azure service resources
- **YAML File** — when your deployment includes only container instances.

A **container restart policy** specifies what a container should do when their process has completed. ACI has has 3 restart-policy options

- **Always** (default) Containers are **always restarted**. Suited for long running tasks eg. **web-servers**
- **Never** Containers **run one time only**. Suited for one off tasks. eg. **background jobs**
- **OnFailure** Containers that encounter an error



# Azure Container Images *CheatSheet*



Azure Containers are **stateless** by default.

When a container crashes or stops all state is loss.

To persist state you need to **mount** an external volume

- You can mount the following external volumes:
  - Azure Files (file share), Secret volume, Empty Directory, Cloud git repo

Container troubleshooting (azure CLI commands you show know):

- **az container logs** – pull logs
- **az container attach** - diagnostic information during container startup
- **az container exec** - interactive container run
- **az monitor metrics list** - get metrics such as CPU usage



# Azure Administrator

Azure Container Registry



## Introduction to Azure Container Registry



# Azure Container Registry (ACR)



**Create and maintain Azure container registries** to store and manage your private Docker container images and related artifacts.



# Azure Container Registry

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Container Registry is a managed, private **Docker registry service** based on the **open-source Docker Registry 2.0**

Use **Azure Container Registries** with your existing container development and deployment pipelines, use **Azure Container Registry Tasks** to build container images in Azure.

Pull images from an Azure container registry to various **deployment targets**:

- Kubernetes
- DC/OS
- Docker Swarm

Many **Azure services have direct support** to use ACR:

- Azure Kubernetes Service (AKS)
- Azure App Service
- Azure Batch
- Azure Service Fabric
- and more!

Developers can also **push to a container registry** as part of a container development workflow with delivery tools such as:

- Azure Pipelines
- Jenkins

- Many ways to work with ACR via:  
Azure CLI
- Azure PowerShell
- Azure Portal
- Azure SDK
- **Docker Extension for Visual Studio Code**





# Azure Administrator

Azure Container Registry



## Registry Tasks



# Azure Container Registry Tasks

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

ACR Tasks allow you to **automate OS and framework patching** for your Docker containers.

For **Quick tasks** you can push a single container image to a container registry on-demand, in Azure, without needing a local Docker Engine installation

You can **trigger automated** builds by:

You can create **multi-step** tasks

- source code updates
- updates to a container's base image
- Timers on a schedule

Each ACR Task has an associated **source code context**

- the location of a set of source files used to build a container image or other artifact

Tasks can take advantage of **run variables**

- reuse task definitions and standardize tags for images and artifact





# Azure Administrator

Azure Container Registry



## ACR CheatSheet



# Azure Container Registry *CheatSheet*



Azure Container Registry is a managed, private Docker registry service based on the open-source Docker Registry 2.0

Use Azure Container Registries with your existing container development and deployment pipelines, use Azure Container Registry Tasks to build container images in Azure.

Pull images from an Azure container registry to various deployment targets:

- Kubernetes
- DC/OS
- Docker Swarm

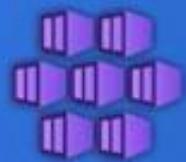
Azure Container Registry (ACR) Tasks allow you to automate OS and framework patching for your Docker containers.

- You can trigger automated builds by:
  - source code updates
  - updates to a container's base image
  - Timers on a schedule
- You can create multi-step tasks
- Each ACR Task has an associated source code context
- Tasks can take advantage of run variables



# Azure Administrator

Azure Kubernetes Service



## Introduction to Azure Kubernetes Service



Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

# Azure Kubernetes Service (AKS)



Fully Managed Kubernetes as a Service





# Introduction to AKS

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Kubernetes Service (AKS) makes it simple to **deploy a managed Kubernetes cluster** in Azure

Azure will manage for you the:

- Kubernetes masters
- health monitoring
- maintenance

You only have to maintain the:

- agent nodes

AKS service is free

You only pay for the agent nodes within the cluster not the masters

When you deploy an AKS cluster, the Kubernetes master and all nodes are deployed and configured for you

Additional features can also be configured during the deployment process such as:

- Advanced networking
- Azure Active Directory integration to use Kubernetes role-based access control (Kubernetes RBAC)
- Monitoring
- Windows Server containers are supported in AKS

You should use AKS for scenarios where you need **full container orchestration**:

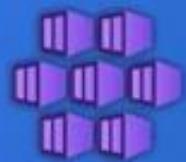
- service discovery across multiple containers
- automatic scaling
- coordinated application upgrades





# Azure Administrator

Azure Kubernetes Service



## Bridge to Kubernetes





# Bridge to Kubernetes

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

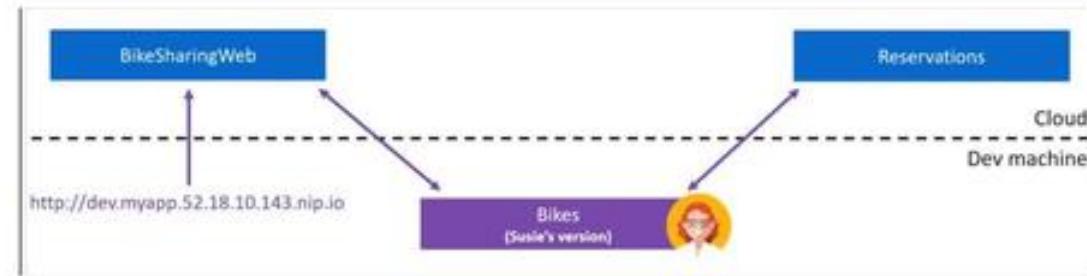


Bridge to Kubernetes is a **extension** in **Visual Studio** and **Visual Studio Code** that allows developers to write, test and debug microservice code on their development workstations



Bridge to Kubernetes allows you **include a locally running service** to your AKS cluster.  
Side-stepping to create Docker, Kubernetes configuration

For the lifetime of this connection, a proxy is added to your cluster in place of your Kubernetes deployment that redirects requests to the service to your development computer. When you disconnect, the application deployment will revert to using the original version of the deployment running on the cluster.





# Azure Administrator

Azure Kubernetes Service



## Create a Kubernetes Cluster



### Follow Along

Microsoft Azure

Home > Subscriptions > Azure subscription 1

Subscriptions

Example Training Inc

+ Add

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here.

Showing subscriptions in Example Training Inc directory. Don't see a subscription? Search directories.

My role:  Selected  All  Global Status:  Enabled  Disabled  All  Global

Apply

Showing 1 of 1 subscriptions  Global Show only subscriptions selected in the dropdown

PowerShell  ?

```
ProviderNamespace : Microsoft.Kubernetes
RegistrationState : Registering
ResourceTypes   : {connectedClusters, locations, locations/operations}
Locations       : {West Europe, East US, West Central US, South Central US}
```

PS /home/andrew> Register-AzResourceProvider -ProviderNamespace Microsoft.Kubernetes

```
ProviderNamespace : Microsoft.KubernetesConfiguration
RegistrationState : Registering
ResourceTypes   : {sourceControlConfigurations, extensionManifests}
Locations       : {East US, West Europe, West Central US, West US}
```



# Azure Administrator

Azure Kubernetes Service



## AKS CheatSheet



# Azure Kubernetes Service *CheatSheet*



Azure Kubernetes Service (AKS) makes it simple to **deploy a managed Kubernetes cluster** in Azure

Azure will manage for you the:

- Kubernetes masters
- health monitoring
- maintenance

You only have to maintain the: agent nodes

AKS service is free, You only pay for the agent nodes within the cluster not the masters

You should use AKS for scenarios where you need **full container orchestration**:

- service discovery across multiple containers
- automatic scaling
- coordinated application upgrades

**Bridge to Kubernetes** is a **extension** in **Visual Studio** and **Visual Studio Code** that allows developers to write, test and debug microservice code on their development workstations



# Azure Administrator

Azure DNS



## Introduction to Azure DNS



# Azure DNS

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a Domain Name System (DNS)?

It is a service that is responsible for **translating (or resolving) a service name** to its IP address.

Azure DNS is a **hosting service** for **DNS domains** that provides name resolution by using Microsoft Azure infrastructure



### Public DNS Internet-facing

- Allows you to manage domains for internet accessible domains
  - Pointing your domain to your website
  - Setting records to prove you own the domain
  - Records to connect your domain to your email server

### Private DNS Internal-facing

- Allow you to use your own custom domains instead of the Azure provided domains
  - Many Azure Services use fully qualified domain name (FQDN) to identify services on the network.
    - eg. Azure Storage Accounts FQDN: <http://storageaccount.file.core.windows.net/>

You **can't use** Azure DNS **to buy a domain name**.

*You can purchase a domain in App Services or a third-party provider and have Azure DNS manage*





# Azure Administrator

Azure DNS



## Zones Records Record Sets





# Azure DNS – Zones, Records and Record Sets

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a DNS zone?

A DNS zone is a container for all your DNS records for a specific domain name

## What is a record?

A DNS record is a rule that says where to send your domain name

A record is composed of **name**, **type** and **value**:

- The **name** tells the record how to listen eg. www
- The **type** tells how to handle the record eg A go to the IP address
- The **value** inform us what we should eg. IP address value 104.194.51.120

## What is a record set?

Sometimes you need to group a bunch of records together, this is what is called a record set.

In Azure DNS you always create record sets, even if they only contain a single record.

Name	Type	TTL	Value
@	NS	172800	ns1-06.azure-dns.com. ns2-06.azure-dns.net. ns3-06.azure-dns.org. ns4-06.azure-dns.info.

This **record set** has multiple records for Name Servers (NS), so if your primary DNS server becomes available it will know to you the second, third or fourth DNS server as a backup server.





# Azure Administrator

Azure DNS



## Record Sets





# Azure DNS – Records Sets

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

In Azure you always create Record Sets even when you just want a single record.

## Naming your Record

**Name** A record that has a name is considered a Fully qualified domain (FQDN) →

or you can think of it as a **subdomain** eg. <https://www.exampro.co>

Name	<input type="text" value="www"/> ✓
	.exampro.co

**No Name** A record that is left empty is considered an apex or **naked domain** →

eg. <https://exampro.co>

Name	<input type="text"/> ✓
	.exampro.co

**Wildcard** You can set wildcards which act as catch-all. Eg \* or \*.trek →

Name	<input type="text"/> ✓
	.exampro.co

**@** You can use an at-sign (@) as your name. This is shorthand for

saying ORIGIN. So this means you're pointing to the naked domain. →

Name	<input type="text"/> ✓
	.exampro.co

## What is a Time to Live (TTL)?

TTL tells other servers requesting your domain how long it should cache this record so it doesn't need to frequently ask you what to do. →

TTL *	<input type="text" value="1"/> Hours
TTL unit	Hours
	Seconds
	Minutes
	Hours
	Days
	Weeks

A **long** TTL can reduce costs because servers check less frequently

A **short** TTL can have failover happen faster, since you have to wait for the cache to expiry for a server to see that you've changed a record to point to your backup server.





# Azure DNS – Records Sets

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## Record Type

Azure Supports the following types of records

**A Address** lets you point your domain to an IPv4 address

**AAAA** lets you point your domain to an IPv6 address

**CAA Certificate Authorities (CAs)** records authorized who can issue certificates for their domain

**CNAME Canonical Name record** creates an alias from one domain to another so you set the record value to a domain

**MX Mail Exchange** records point to mail servers that handle emails

**NS Name Server** records identify multiple DNS servers for the domain and there are multiple in case the primary DNS server fails

**PTR Pointer** record points to a domain or host name but is used for reverse DNS lookup

**SRV Service** record is used to identify computers that host specific services, like locating Domain Controllers for Active Directory

**TXT Text** records is just text, and can serve multiple purposes, such as documentation or as a means of verification

**SOA Start of Authority** record contains administrative details about a domain

Type
A
A
AAAA
CAA
CNAME
MX
NS
SRV
TXT
PTR





# Azure DNS – Records Sets

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure has its own **special record type** called an **Alias** that work with **A, AAAA** and **CNAME** records

Azure Alias record points directly to an Azure resource instead of to an IP or hostname

Imagine you were pointing to an IP or hostname and you deploy a service which causes the IP to change. You domain would be left **dangling** (pointing to now where) And you would have to manually update the record to the new correct address.

Azure Alias records always point to the right place.

Alias type  
 Azure resource  Zone record set

Choose a subscription \*  
Azure subscription 1

Azure resource \*  
Select an Azure resource

The value must not be empty.

Traffic Manager  
No Traffic Manager resource found

Public IP Address  
No Public IP resource found

Azure CDN  
No Azure CDN Endpoint resource found

Front Door  
No Front door resource found

Search for an Azure resource





# Azure Administrator

Azure DNS



## Create a DNS Zone and Record Set



Follow Along

andrew@exampro.co  
EXAMPRO TRAINING INC. EXAM

Add record set  
.wcrf.com

Name: .wcrf.com

Type: A – Alias record to IPv4 address

A – Alias record to IPv4 address

AAAA – Alias record to IPv6 address

CAA – Certificate Authorities to authorize certificates

CNAME – Link your subdomain to another record

MX – Mail exchange records

NS – Name Server records

SRV – Service records

TXT – Text record type

PTR – Pointer record type

(A)



# Azure Administrator

Azure DNS



## DNS CheatSheet



# Azure DNS *CheatSheet*

Exam

Pro

**Domain Name System (DNS)** It is a service that is responsible for **translating (or resolving) a service name** to its IP address.

Azure DNS is a **hosting service** for **DNS domains** that provides name resolution by using Microsoft Azure infrastructure

- You **can't use Azure DNS to buy a domain** name.

**Public DNS** Internet-facing

- Allows you to manage domains for internet accessible domains
  - Pointing your domain to your website
  - Setting records to prove you own the domain
  - Records to connect your domain to your email server

**Private DNS** Internal-facing

- Allow you to use your own custom domains instead of the Azure provided domains

**DNS zone** is a container for all your DNS records for a specific domain name

**DNS record** is a rule that says where to send your domain name. A record is composed of **name, type and value**:

- A **Address** lets you point your domain to an IPv4 address
- AAAA lets you point your domain to an IPv6 address
- CAA **Certificate Authorities (CAs)** records authorized who can issue certificates for their domain
- CNAME **Canonical Name record** creates an alias from one domain to another so you set the record value to a domain
- MX **Mail Exchange** records point to mail servers that handle emails
- NS **Name Server** records identify multiple DNS servers for the domain and there are multiple in case the primary DNS server fails
- PTR **Pointer** record points to a domain or host name but is used for reverse DNS lookup
- SRV **Service** record is used to identify computers that host specific services, like locating Domain Controllers for Active Directory
- TXT **Text** records is just text, and can serve multiple purposes, such as documentation or as a means of verification
- SOA **Start of Authority** record contains administrative details about a domain



# Azure DNS *CheatSheet*

Exam

Pro

Azure has its own **special record type** called an **Alias** that work with A, AAAA and CNAME records

- Azure Alias record points directly to an Azure resource instead of to an IP or hostname (**helps avoid dangling domains**)

**Record Set** A group of records. Azure always creates a record set, even with a single record

**Time to Live (TTL)** says how long a value should be cached



# Azure Administrator

Azure Networking



## Introduction to Virtual Networks

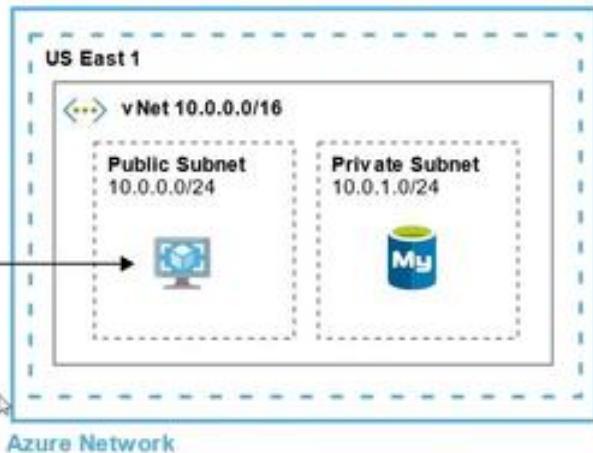




# Azure Virtual Network (VNet)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Virtual Network (vNet)** is a logically isolated section of the Azure Network where you launch your Azure resources.



**Azure DNS** — manage your own DNS domain



**Virtual Network (vNET)** — logically isolated section of Azure network

- Address spaces
- Route Tables
- Subnets



**Network Security Groups** A virtual firewall at the subnet or NIC level



**ExpressRoute** A 50 Mbps-10 Gbps connection between on-premise to VNET



**Virtual WAN** a centralized network to route different network connections



**Virtual Network Gateway** - A site-to-site VPN connection between an VNet and local networks



**Network Interfaces** virtual network device to allow your VMs to communicate using IP protocols





# Azure Administrator

Azure Networking

## VNet Peering

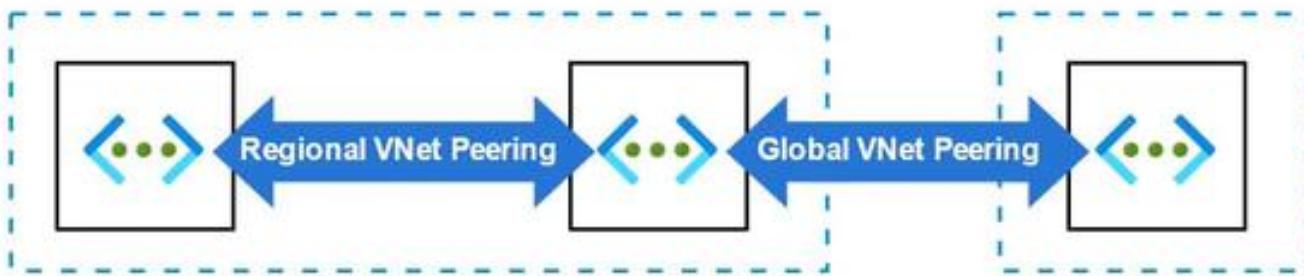




# VNet Peering

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

VNET peering is when you connect multiple VNet so they act as one network.



**There are 2 types of VNet Peering:**

- 1. Regional VNet Peering** When you peer two VNets from the same region
- 2. Global VNet peering** When you peer two VNets from two different regions



# Azure Administrator

Azure Networking



## Network Interfaces





# Network Interfaces

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a Network Interface?

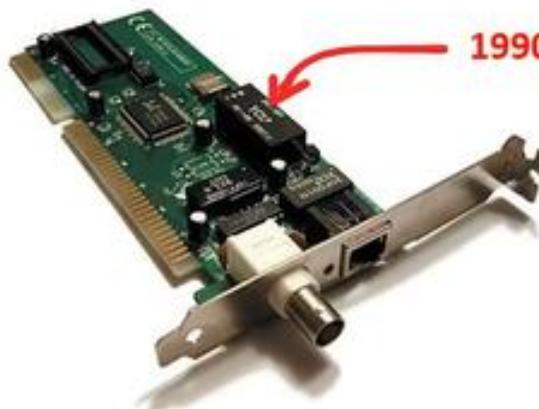
**Software or hardware interface** between two pieces of equipment or protocol layers in a computer network.

## A Network Interface Controller (NIC)

A **computer hardware component** that connects a computer to a computer network.

Also known as:

- network interface card
- network adapter
- LAN adapter
- physical network interface



1990s Ethernet Interface Controller card

NICs communicate using **Internet Protocol (IP)**

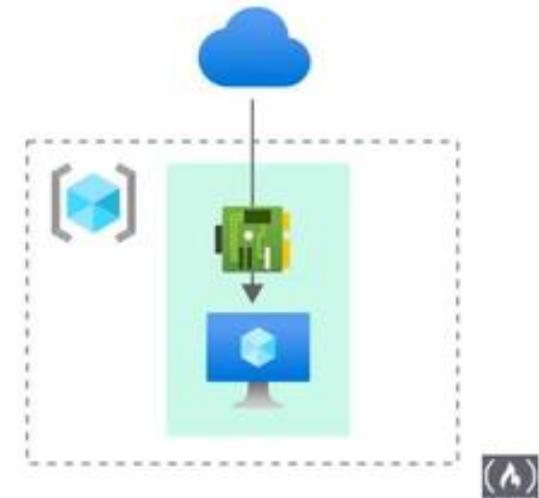


## Azure Network Interfaces (NICs)

Azure Network Interfaces are attached to Azure VM instance.

Without an NIC, An Azure VM instance would have no way to communicate.

An Azure VM instance has to have an NIC and can have multiple NICs.





# Azure Administrator

Azure Networking



## Network Routes and Route Tables





# Network Routes and Routes Tables

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a Route Table?

A Route Table is table of data stored in router or network host that list routes to next destinations.

**Routes are the roads to your virtual network.** Without them data would not know where to go.

## Default System Routes

By default Azure creates a route table with defaults routes and associates them to your subnets so you don't have to do anything to get routing.

If you were to check the **Azure Route Table** service you won't see these default route tables since it hidden and managed by Azure for you. Azure sets the following **default routes**:

Source	Address prefixes	Net hop type	
Default	Unique to VNet	Virtual Network	← <b>A route to your VNet</b>
Default	0.0.0.0/0	Internet	← <b>A route to the Internet</b>
Default	10.0.0.0/8	None	← <b>Reserved for private use in RFC 1918 so don't go anywhere</b>
Default	192.168.0.0/16	None	← <b>Reserved in RFC 6598</b>
Default	100.64.0.0/10	None	← <b>Reserved in RFC 6598</b>

*Azure may assign additional default routes based if you have other capabilities enabled*





# Network Routes and Routes Tables

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

## User Defined Routes

You can override the system routes assigned to your subnets by creating a new route table and associating it with a subnet

A User defined Route table can be assigned to multiple subnets, but a Subnet can only have one user defined route table

When you create your user defined route table, all the default system routes remain unless you override them within your route table

If you wanted to have a private subnet (a subnet that cannot reach the internet)

You would just create a new route for 0.0.0.0/0 that hops to None



Next hop type ⓘ

None

Virtual network gateway

Virtual network

Internet

Virtual appliance

None

The Next Hop is where to send the route:

Route name \*  
NoInternet

Address prefix \* ⓘ  
0.0.0.0/0

Next hop type ⓘ  
None

The virtual appliance is a VM that runs a network application eg. Firewall  
In this hop type you also have to provide the Private IP address to the VM





# Azure Administrator

Azure Networking

## Address Spaces





# VNet – Address Spaces

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is an Address Space?

It is a **range of available IP addresses** that you are **allocating** for you use within your Virtual Network (VNeT)  
The amount of IP addresses available is determined based on the CIDR range notation eg. 10.0.0.0/24

A CIDR Block of /24 will allocate 256 possible addresses

A CIDR Block of /27 will allocate 32 possible addresses

Azure Virtual Network (VNeT) allows you defined a multiple address spaces

Address space	Address range	Address count	
10.0.0.0/24	10.0.0.0 - 10.0.0.255	256	
192.168.0.0/24	192.168.0.0 - 192.168.0.255	256	
<input type="button" value="Add additional address range"/>			

Address ranges cannot overlap **within the same VNet**

The address count **is not** the actual available IP addresses as Azure will reserve 5 of the IP addresses:

- x.x.x.0: Network address
- x.x.x.1: Reserved by Azure for the default gateway
- x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
- x.x.x.255: Network broadcast address (the last IP in the range, its not always 255)





# Azure Administrator

Azure Networking

## Subnets



# VNeT – Subnets

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a Subnet?

A subnet is **a logical division of an address space**. Subnets help you **define different kinds of workloads** and allows you to apply virtual isolation within your network. When you launch an Azure resource you choose the subnet you want to launch within and an IP from that subnet is assigned to your resource

## Associating a Route Table

A subnet needs a Route Table so it can access

## Public vs Private Subnet

Public and Private subnet describes whether a subnet is reachable from the internet or not.

Azure **has no concept of private and public subnets** and its up to you to configure our subnets to have ensure they do no reach the internet by ensuring they have no route via the their route table to the Internet Gateway

## Associating Network Security Gateways (NSG)

You can associate an NSG to protect traffic entering and leaving your subnet by applying security rules that can Allow or deny access based on IP address, port and protocol.

## Gateway Subnet

Azure has a special type of Gateway Subnet that is used by **Azure Virtual Network Gateway** and that service Launches specialized VMs into that subnet.





# Azure Administrator

Azure Networking



## Private Links





# Private Links

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

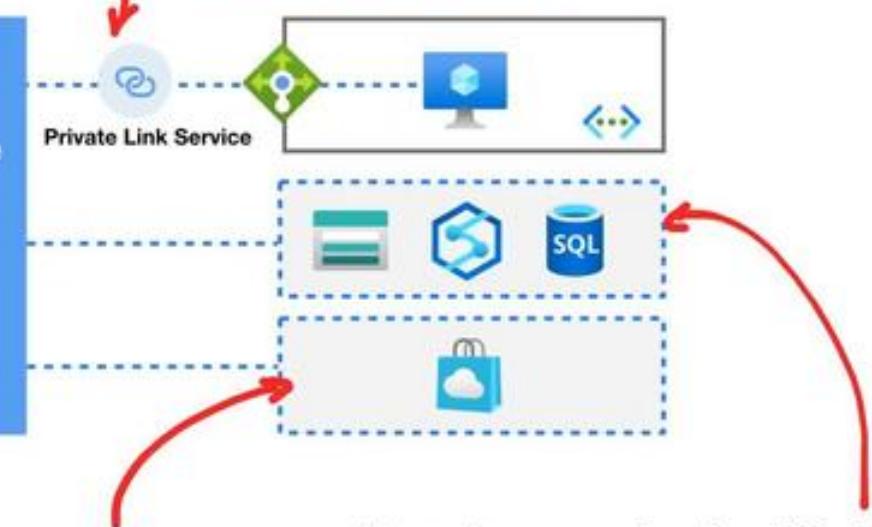
Azure Private Links allows you to **establish secure connections** between Azure resources so traffic **remains within the Azure Network**

**Private Link Endpoint** is an **Network Interface** that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your VNet



Third-Party providers can be powered by Private Link

**Private Link Service** allows you to connect your own workload to Private Link. You need an **Azure Standard Internal Load Balancer** and associate it with the Link Service



Many Azure services by default work with Private Link eg. Azure Storage, CosmosDB, SQL





# Azure Administrator

Azure Networking



## Azure Express Routes





# Azure ExpressRoute

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

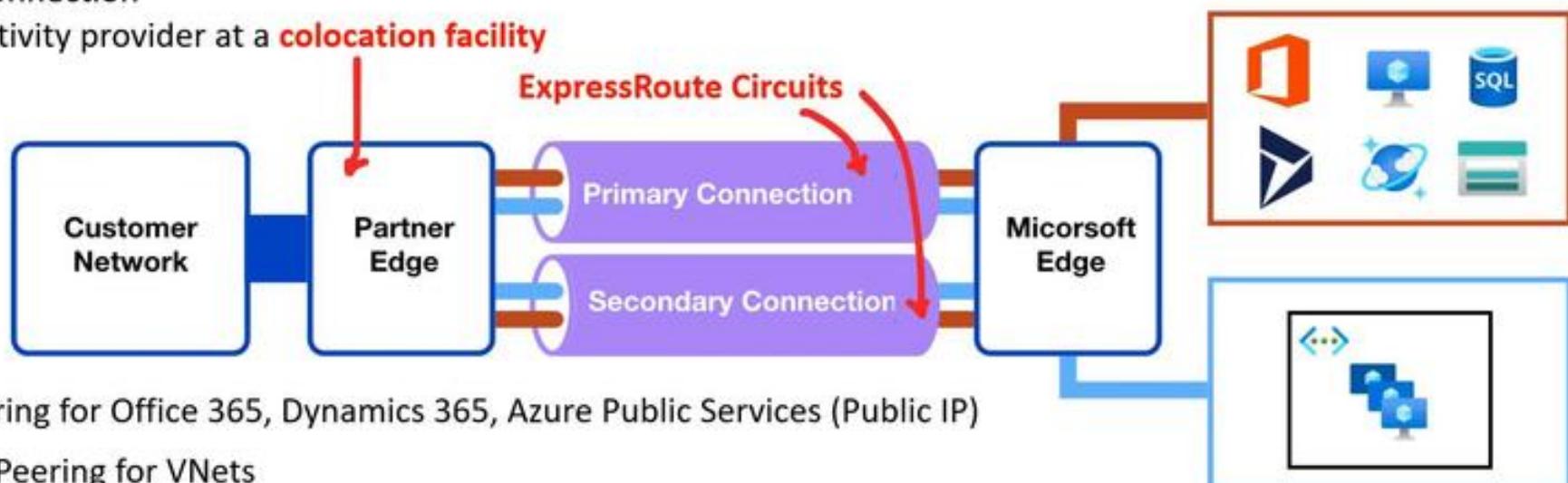
Azure ExpressRoutes creates **private connections** between Azure datacenters and infrastructure on your premises or in a colocation environment

Connectivity can be from an:

- any-to-any (IP VPN) network
- a point-to-point Ethernet network
- virtual cross-connection

through a connectivity provider at a **colocation facility**

ExpressRoute connections don't go over the public Internet and as a result can offer: **more reliability, faster speeds, consistent latencies, higher security**



ExpressRoute Direct allows for **greater bandwidth connections** from 50 Mbps to 10Gbps. Ideal where for hybrid solutions with massive amounts of data or where latency matters.



# Azure Administrator

Azure Networking



## Azure Firewall





# Azure Firewall

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

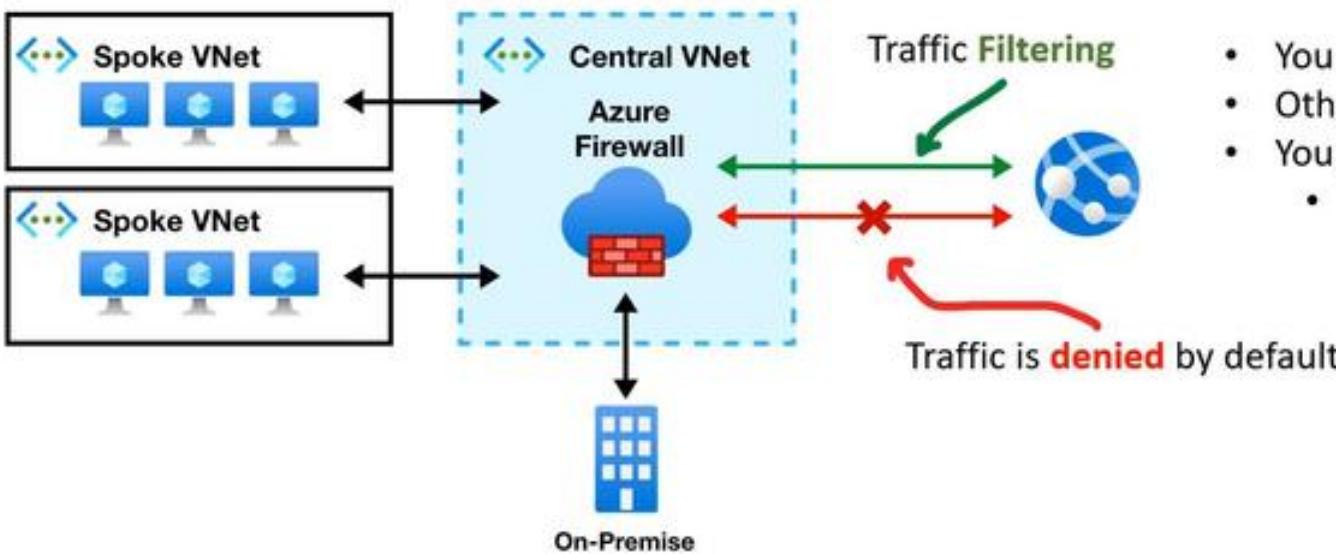
Azure Firewall is a managed, **cloud-based network security service** that protects your **Azure VNets** resources

It is a **fully stateful** Firewall as a Service (FWaaS) with:

- built-in high availability
- unrestricted cloud scalability

You can centrally **create, enforce, and log** application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall uses a **static public IP address** for your VNet resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with **Azure Monitor** for logging and analytics.



- You launch an Azure Firewall in its own VNet
- Other VNets pass through this Central VNet
- You get **Microsoft Threat Intelligence**
  - Blocks known malicious IPs and FQDNs





# Azure Administrator

Azure Networking



## Azure Network Watcher





# Azure Network Watcher

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Network Watcher provides tools to **monitor, diagnose, view network metrics**, and enable or disable logs for resources in an Azure virtual network.

From Network Watcher you can access:

- IP flow verify checks
- Packet Capture
- Troubleshoot VPNs, NSGs
- NSG Flowlogs
- Diagnostic Logs
- Traffic Analytics
- Network Performance Monitor
- And more...!

Network Watcher **can** monitor and repair

Azure resources you provision eg:

- Virtual Machines
- Virtual Networks
- Application Gateways
- Load balancer

Network Watcher **cannot** be used to monitor PaaS (fully managed services) monitoring or Web Analytics

Network Watcher is **disabled by default** in most regions so you need to enable it at per region basis



WEST INDIA	Disabled
Canada Central	Disabled
Canada East	Disabled
West Central US	Disabled

Enable network watcher





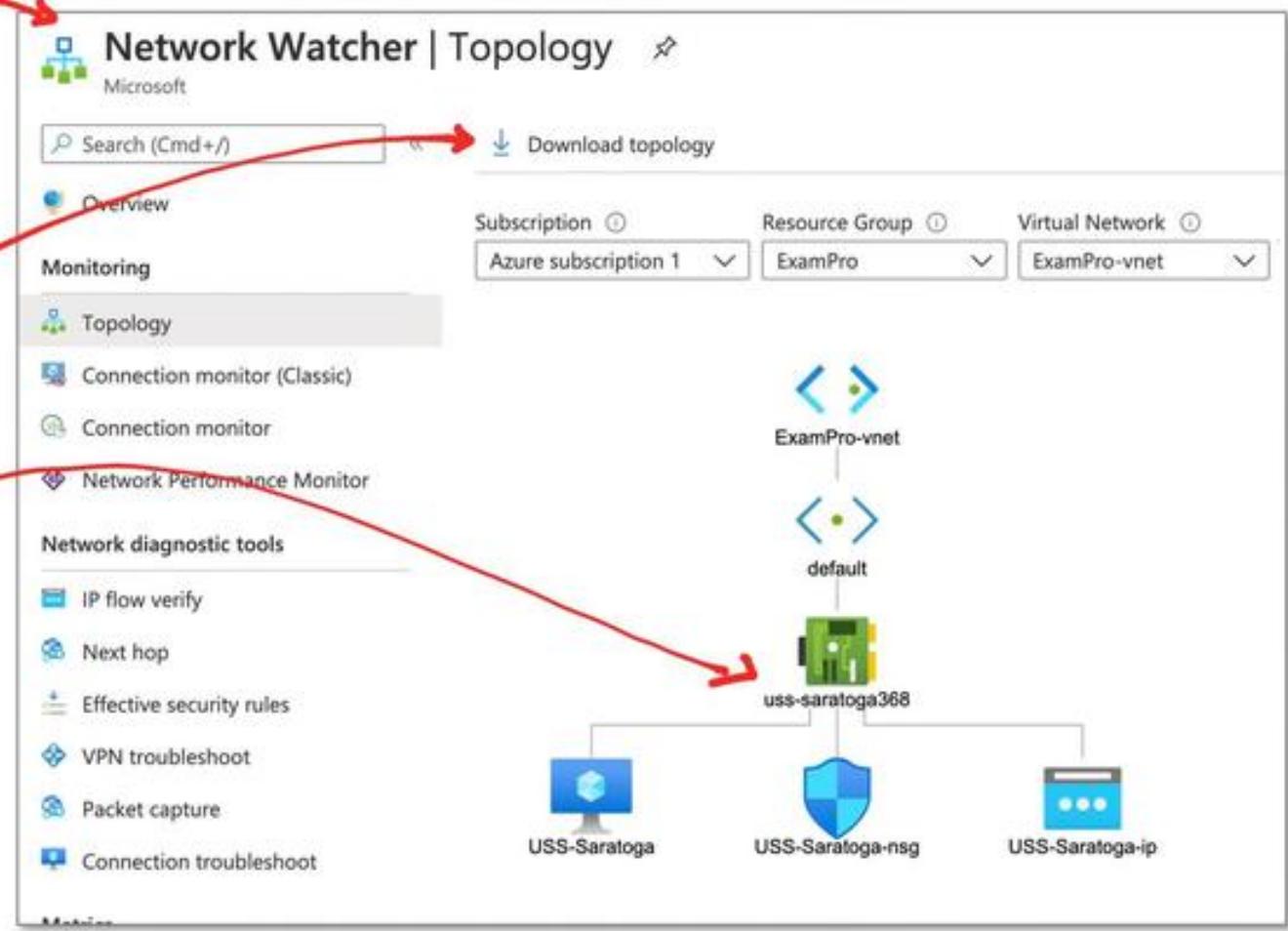
# Azure Network Watcher

Cheat sheets, Practice Exams and Flash cards ↗ [www.exampro.co/az-104](http://www.exampro.co/az-104)

Network Watcher can **visualize** the topology of your VNets

You can download the topology as an SVG you to use in presentations and documentation

You can quickly discover and browse your networking components to quickly monitor and repair your virtual network





# Azure Administrator

Azure Networking



## Network Performance Monitor





# Network Performance Monitor

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Network Performance Monitor (NPM)** is a **cloud-based hybrid network monitoring solution** that helps you **monitor network performance between various points** in your network infrastructure.



It also helps you monitor network connectivity to service and application endpoints and monitor the performance of **Azure ExpressRoute**.

To use NPM you need to create an NPM resource

- In order to create an NPM resource you need to create a **Log Analytics Workspace**

The solution generates alerts and notifies you when a threshold is breached for a network link. It also ensures timely detection of network performance issues and localizes the source of the problem to a particular network segment or device.

Network Performance Monitor detects network issues like:

- traffic blackholing
- routing errors
- unconventional network issues





# Azure Administrator

Azure Networking

## Setup an Azure Firewall



Follow Along

Microsoft Azure (Search resources, services, and documentation)

Home > Virtual networks > Cardassia-vnet > Create a firewall

Create a firewall

Region: Canada East

Availability zone: None

Premium firewalls support additional capabilities such as SSL termination and IPsec. Additional costs may apply. Standard firewall to Premium will require some downtime. Learn more.

Firewall tier:  Standard  Premium (preview)

Firewall management:  Use a Firewall Policy to manage this firewall  Use Firewall rules (classic) to manage this firewall

Choose a virtual network:  Create new  Use existing

Virtual network: Cardassia-vnet (Cardassia) This virtual network must have a subnet named Azurefirewall.

Public IP address: cardassia-prime-ip (52.235.32.117) The IP address 'cardassia-prime-ip (52.235.32.117)' is already in use by the network interface 'cardassia-prime247'.

Force tunneling:  Disabled

Add new

Review + create Preview Next: Tags Download a template for this machine



# Azure Administrator

Azure Networking

## Setup a peering VPC



Follow Along

Search resources, services, and docs (Ctrl+F)

east-a-vnet | Peerings

Virtual network

Add Refresh

east-a-vnet

east-a-vn-1

Connected

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peering

Service endpoints

Private endpoints

Properties

Locks

(A) SUBSCRIBE



# Azure Administrator

Azure Networking

## Setup Test Server for Network Watcher



Follow Along

Microsoft Azure

Home > Network Watcher

### Network Watcher | IP flow verify

denied the packet is returned.  
Learn more.

Specify a target virtual machine with associated network interface and outbound packet to see if access is allowed or denied.

Subscription \*  Azure subscription 1

Resource group \*  Rasa

Virtual machine \*  Rasa

Network interface \*  rasa636

Packet details

Protocol  TCP  UDP

Direction  Inbound  Outbound

Local IP address \*  10.0.0.4

Remote IP address \*

Local port   Remote port

Check (A) RESEND

Monitoring

- Topology
- Connection monitor (classic)
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP Flow verify
- NDS diagnostic
- Net hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Logs

- IP Flow logs
- Diagnostic logs



# Azure Administrator

Azure Networking

## IP Flow Verify via Network Watcher



Follow Along

Microsoft Azure (3) Search resources, services and documentation

Home > Network Watcher

### Network Watcher | IP flow verify

Microsoft

Search (Ctrl + F)

denied the packet is returned.  
[Learn more](#)

Monitoring

- Topology
- Connection monitor (classic)
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP Flow verify
- NGS diagnostic
- Net hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshooting

Metrics

- Usage + quotas

Logs

- NGS flow logs
- Diagnostic logs

IP Flow Verify

Specify a target virtual machine with associated network or outbound packet to see if access is allowed or denied.

Subscription \*  Azure subscription 1

Resource group \*  Risa

Virtual machine \*  Risa

Network interface \*  rnat36

Packet details

Protocol  TCP  UDP

Direction  Inbound  Outbound

Local IP Address \*  10.0.0.4

Local port  8080

Remote IP address \*

Remote port  8080

Check (A) RESEND



# Azure Administrator

Azure Networking

## Debug NSG via Diagnostic Tools



Follow Along

Microsoft Azure

Risa-nsg

Network security group

Search (Ctrl+F)

Move Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

Resource group (change)  
Risa

Location  
East US 2

Subscription (change)  
Azure subscription 1

Subscription ID  
7f3352cf-6c7d-456e-8ecb-83ef2128807b

Tags (change)  
Click here to add tags

Filter by name

Port == all Protocol == all Source == all

Priority	Name	Port
300	SSH	22
300	HTTP	80
45000	AllInbound	Any
45001	AllAzureLoadBalancing	Any
45500	DenyAllInbound	

Inbound Security Rules

Outbound Security Rules

(A) **SEARCH**

Detailed description: This screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The main title is 'Risa-nsg' under 'Network security group'. On the left, there's a navigation menu with links like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Below that is a 'Settings' section with Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Alerts, Diagnostic settings, Logs, and NSG flow logs. To the right, the 'Inbound Security Rules' table lists five rules: port 22 for SSH, port 80 for HTTP, port range 45000 for AllInbound, port 45001 for AllAzureLoadBalancing, and port 45500 for DenyAllInbound. There are also sections for 'Outbound Security Rules', 'Tags', and a search bar at the top.



# Azure Administrator

Azure Networking

## Capture Packets



**Follow Along**

Wireshark screenshot showing captured network traffic. The list view displays a series of HTTP/1.1 requests and responses between two hosts. The details view shows the structure of a selected packet, and the bytes view shows the raw binary data.

Selected packet details:

- Frame 21: 26 bytes on wire (198 bits), 26 bytes captured (198 bits)
  - Internet Protocol Version 4 Header: Src Port: 50084, Dst Port: 8007, Seq: 1, Ack: 1, Len: 4
  - Data (4 bytes): 00 00 00 00



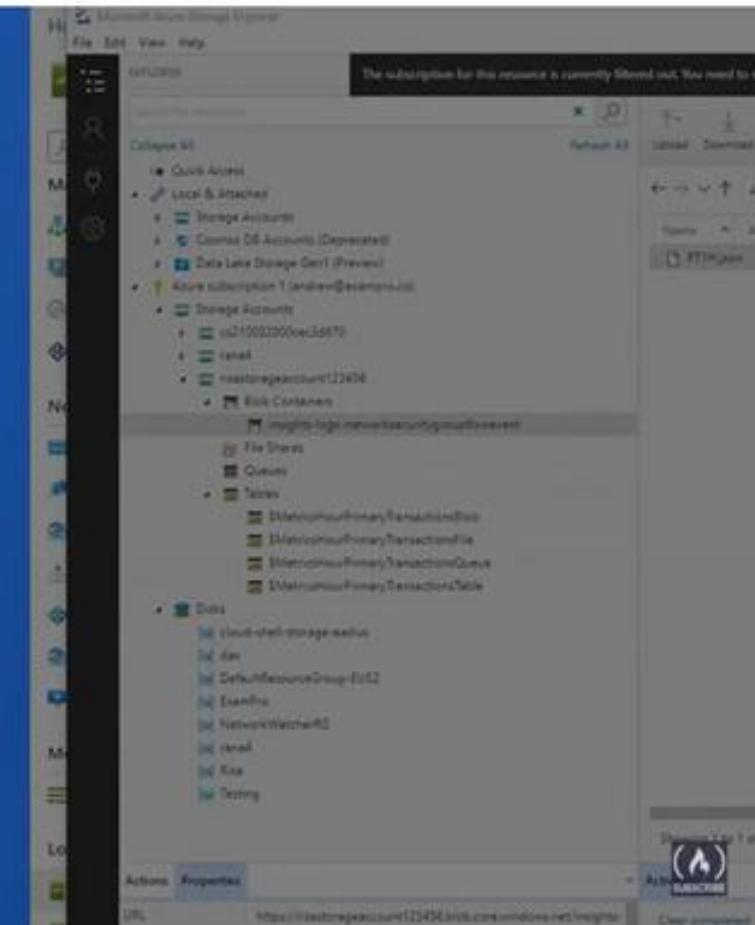
# Azure Administrator

Azure Networking

## Capture NSG Flow Logs



Follow Along





# Azure Administrator

Azure Networking

## Azure Network Watcher Cleanup



Follow Along

Are you sure you want to delete "Risa"?

Warning! Deleting the "Risa" resource group is irreversible. The action you're about to take can't be undone. Going further will delete this resource group and all the resources in it permanently.

Type the resource group name:

Please enter 'yes' to confirm delete.

TYPE THE RESOURCE GROUP NAME

AFFECTED RESOURCES  
There are 29 resources in this resource group that will be deleted.

Name	Type	Location
basicNsgIseines242-nic01	Network security group	East US 2
LoadBalancer0ip	Public IP address	East US 2
NetworkMonitoring(RisaLog-000)	Log Analytics workspace	East US 2
Rana4	Virtual machine	Japan West
Rana4_OsDisk_1_d99bc7bb5...	Disk	Japan West
rana4370	Network interface	Japan West
Rana4-ip	Public IP address	Japan West
Rana4-ing	Network security group	Japan West
Risa	Virtual machine	East US 2
AzureNetworkWatcherExtensi...	Microsoft Compute extension	East US 2
OmsAgentForLinux (Risa/Om...	Microsoft Compute extension	East US 2
Risa_OsDisk_1_37685af84188...	Disk	East US 2
Virtual Machine Scale Set	Virtual machine scale set	East US 2



# Azure Administrator

Azure Networking



## Networking CheatSheet



# Azure Networking *CheatSheet*



**Virtual Network (vNet)** is a logically isolated section of the Azure Network where you launch your Azure resources.

VNET peering is when you connect multiple VNet so they act as one network.

1. **Regional VNet Peering** When you peer two VNets from the same region
2. **Global VNet peering** When you peer two VNets from two different regions

**Network Interface Controller (NIC)** software or hardware interface between two pieces of equipment or protocol layers in a network.

NICs communicate using **Internet Protocol (IP)**

## Azure Network Interfaces (NICs)

- Azure Network Interfaces are attached to Azure VM instance.
- Without an NIC, An Azure VM instance would have no way to communicate.
- An Azure VM instance has to have an NIC and can have multiple NICs.

**Route Table** is table of data stored in router or network host that list routes to next destinations.

- By default Azure creates a route table with defaults routes (system routes) and associate them to your subnets
- You can override the system routes assigned to your subnets by creating a new route table and associating it with a subnet

**Address Space** is a range of available IP addresses that you are **allocating** for you use within your Vnet

- The amount of IP addresses available is determined based on the CIDR range notation

## Subnet is a logical division of an address space

- A subnet needs a Route Table so it can access
- Public and Private subnet describes whether a subnet is reachable from the internet or not.
- Azure **has no concept of private and public subnets** and its up to you to configure our subnets to have ensure they do no reach the internet
- You can associate an NSG to protect traffic entering and leaving your subnet
- Azure has a special type of Gateway Subnet that is used by **Azure Virtual Network Gateway**



# Azure Networking *CheatSheet*

Exam Pro

Azure Private Links allows you to establish secure connections between Azure resources so traffic remains within the Azure Network

- Private Link Endpoint is an Network Interface that connects you privately and securely to a service powered by Azure Private Link.
  - uses a private IP address from your Vnet
- Private Link Service allows you to connect your own workload to Private Link
  - You need an Azure Standard Internal Load Balancer and associate it with the Link Service
- Many Azure services by default work with Private Link eg. Azure Storage, CosmosDB, SQL
- Third-Party provides can be powered by Private Link

Azure Firewall is a managed, cloud-based network security service that protects your Azure VNets resources

- It is a fully stateful Firewall as a Service (FWaaS) with: built-in high availability and unrestricted cloud scalability
- You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.
- uses a static public IP address for your VNet resources allowing outside firewalls to identify traffic originating from your virtual network
- fully integrated with Azure Monitor for logging and analytics.
- You launch an Azure Firewall in its on VNet
- Other VNets pass through this Central Vnet
- You get Microsoft Threat Intelligence
  - Blocks known malicious IPs and FQDNs

Azure ExpressRoutes creates private connections between Azure datacenters and infrastructure on your premises or in a colocation env

- Connectivity can be from an: any-to-any (IP VPN) network, a point-to-point Ethernet network, virtual cross-connection
  - through a connectivity provider at a colocation facility

ExpressRoute Direct allows for greater bandwidth connections from 50 Mbps to 10Gbps.





# Azure Administrator

Azure Networking



## ANW CheatSheet



# Azure Network Watcher *CheatSheet*



Azure Network Watcher provides tools to **monitor, diagnose, view network metrics**, and enable or disable logs for resources in an Azure Vnet

- IP flow verify checks, Packet Capture, Troubleshoot VPNs, NSGs, NSG Flowlogs, Diagnostic Logs, Traffic Analytics, NPM

Watcher **can** monitor and repair Azure resources you provision:

- Virtual Machines, Virtual Networks, Application Gateways, Load balancer

Network Watcher **cannot** be used to monitor PaaS (fully managed services) monitoring or Web Analytics

Network Watcher is **disabled by default** in most regions so you need to enable it at per region basis

Network Watcher can **visualize** the topology of your VNets

**Network Performance Monitor (NPM)** is a **cloud-based hybrid network monitoring solution** that helps you **monitor network performance between various points** in your network infrastructure.

- traffic blackholing
- routing errors
- unconventional network issues
- generates alerts and notifies you when a threshold is breached for a network link



# Azure Administrator



## Network Security Group Rules





# Network Security Groups (NSG)

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

**Network security group (NSG) filter network traffic to and from Azure resources in a VNet**

An NSG is composed of many **Security Rules**

Each Security Rule has the following properties:

**Name** — A unique name within the network security group.

**Source or destination** — An IP Address or CIDR block, Service Tag or

Application Security Group

**Port Range** — Specify a single or range of ports. eg. 80 or 10000-10005

**Protocol** — TCP, UDP, ICMP or ANY

**Action** — All or Deny

**Priority** — A number between 100 and 4096 (lower number higher priority)

- **Inbound Rules** apply to traffic *entering* the NSG
- **Outbound Rules** apply to traffic *leaving* the NSG

Add inbound security rule

MyNSG

Basic

Source \* Any

Source port ranges \* \*

Destination \* Any

Destination port ranges \* 8080

Protocol \* Any TCP UDP ICMP

Action \* Allow Deny

Priority \* 100

Name \* Port\_8080

(A)

This screenshot shows the 'Add inbound security rule' dialog box for a Network Security Group named 'MyNSG'. The 'Basic' tab is selected. The 'Source' field is set to 'Any'. The 'Source port ranges' field contains a single asterisk (\*). The 'Destination' field is set to 'Any'. The 'Destination port ranges' field contains the value '8080'. The 'Protocol' section shows 'Any' selected, with radio buttons for TCP, UDP, and ICMP also available. The 'Action' section shows 'Allow' selected, with a 'Deny' option available. The 'Priority' field is set to '100'. The 'Name' field is populated with 'Port\_8080'. At the bottom right is a blue '(A)' save button.



# Azure Administrator



## Default Security Rules



# NSG – Default Security Rules

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure sets the following **default security rules** when you create an NSG:

## Outbound 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

## Inbound Rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny



# Azure Administrator



## Security Rules Logic



# NSG – Security Rules Logic

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Security Rules has **a lot of logic** to determine how to apply its rules

- You may not create two security rules with the same priority and direction.
- You can have 5000 NSG per subscription, 1000 NSG rules per NSG
- **Priority**
  - Rules are processed in priority order, with lower numbers processed before higher number
  - Network security group security rules are evaluated by priority using the 5-tuple information to allow or deny traffic: 1] source 2] source port 3] Destination 4] destination port 5] protocol
- **Flow Records**
  - The flow record allows a network security group to be stateful.
  - A flow record is created for existing connections
  - Communication is allowed or denied based on the connection state of the flow record.
- **Statefulness**
  - If you specific an outbound security port you don't need to set the inbound port since it will be set for you.
  - You only need to specify an inbound security rule if communication is initiated externally.
  - The opposite is also true. If inbound traffic is allowed over a port, it's not necessary to specify an outbound security rule to respond to traffic over the port.
- **Interruption**
  - Existing connections may not be interrupted when you remove a security rule that enabled the flow.
  - Traffic flows are interrupted when connections are stopped and no traffic is flowing in either direction, for at least a few minutes.





## Azure Administrator

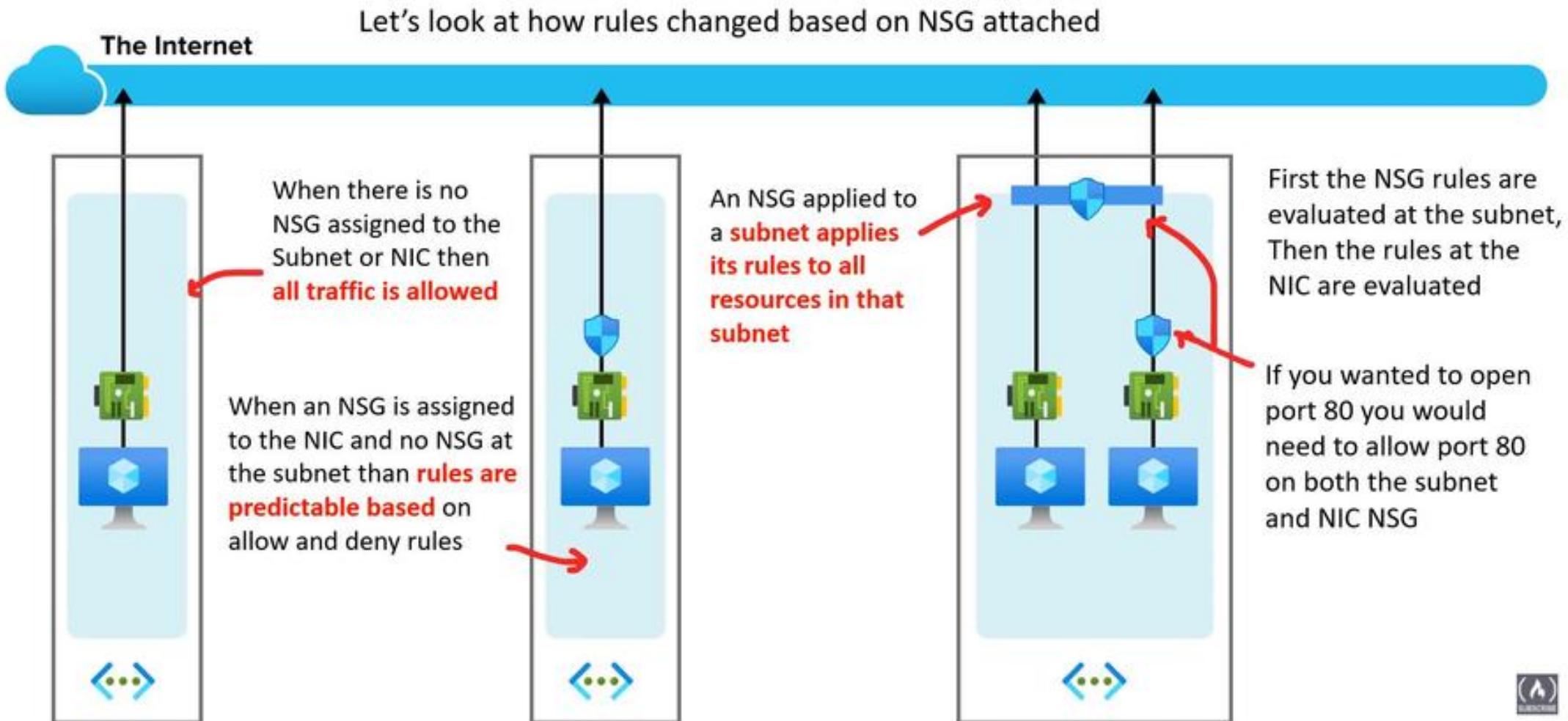


# NSG Combinations



# Network Security Groups (NSG)

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)





# Azure Administrator



## NSG CheatSheet



# Azure Network Security Groups *CheatSheet*

Exam

Pro

Network security group (NSG) **filter network traffic** to and from Azure resources in a Vnet

An NSG is composed of many **Security Rules**

- **Name** — A unique name within the network security group.
- **Source or destination** — An IP Address or CIDR block, Service Tag or Application Security Group
- **Port Range** — Specify a single or range of ports. eg. 80 or 10000-10005
- **Protocol** — TCP, UDP, ICMP or ANY
- **Action** — All or Deny
- **Priority** — A number between 100 and 4096 (lower number higher priority)

**Inbound Rules** apply to traffic *entering* the NSG

**Outbound Rules** apply to traffic *leaving* the NSG

By Default Azure will set a bunch of inbound and outbound rules for you

You may not create two security rules with the same priority and direction.

You can have 5000 NSG per subscription, 1000 NSG rules per NSG

Rules are processed in priority order, with lower numbers processed before higher number

The flow record allows a network security group to be stateful.

If you specific an outbound security port you don't need to set the inbound port since it will be set for you.

The opposite is also true. If inbound traffic is allowed over a port, it's not necessary to specify an outbound security rule to respond to traffic over the port.





# Azure Administrator



## Introduction to Azure Virtual WAN





# Azure Virtual WAN

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

Azure Virtual WAN is a **consolidated networking service** that brings many **networking**, **security**, and **routing** functionalities in a single operational interface.

These functionalities include

- branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE)
- Site-to-site VPN connectivity,
- remote user VPN (Point-to-site)
- connectivity, private (ExpressRoute) connectivity,
- intra-cloud connectivity (transitive connectivity for virtual networks)
- VPN ExpressRoute inter-connectivity,
- routing
- Azure Firewall encryption for private connectivity.

Azure Virtual WAN itself is a **Software Defined WAN (SD-WAN)**

Azure Virtual WAN is a much better way to route to your branches, datacenters, VNet and cloud services.





# Azure Administrator



## Point of Presence

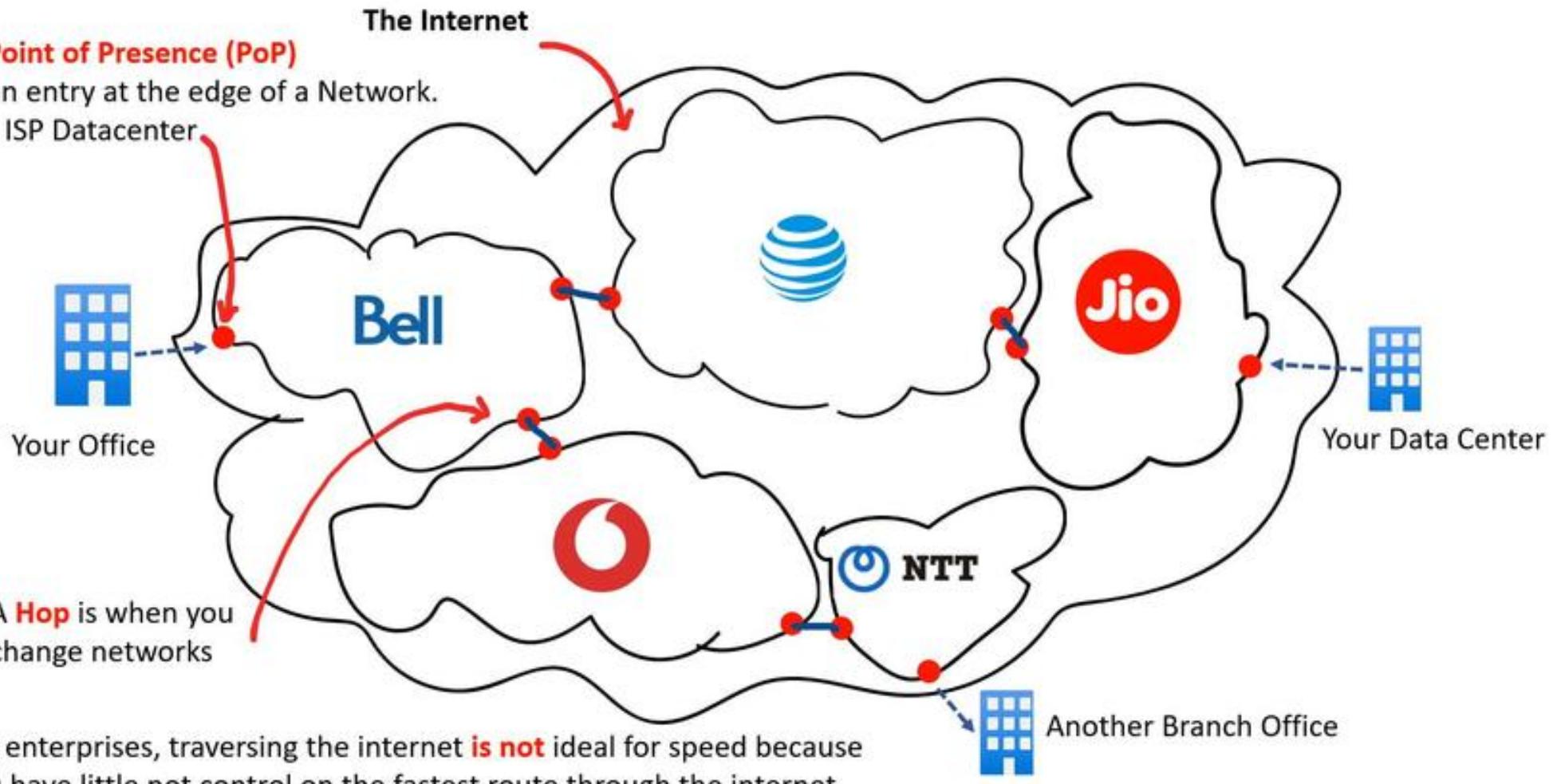


# Azure Virtual WAN – PoPs

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## A Point of Presence (PoP)

Is an entry at the edge of a Network.  
eg. ISP Datacenter





# Azure Administrator



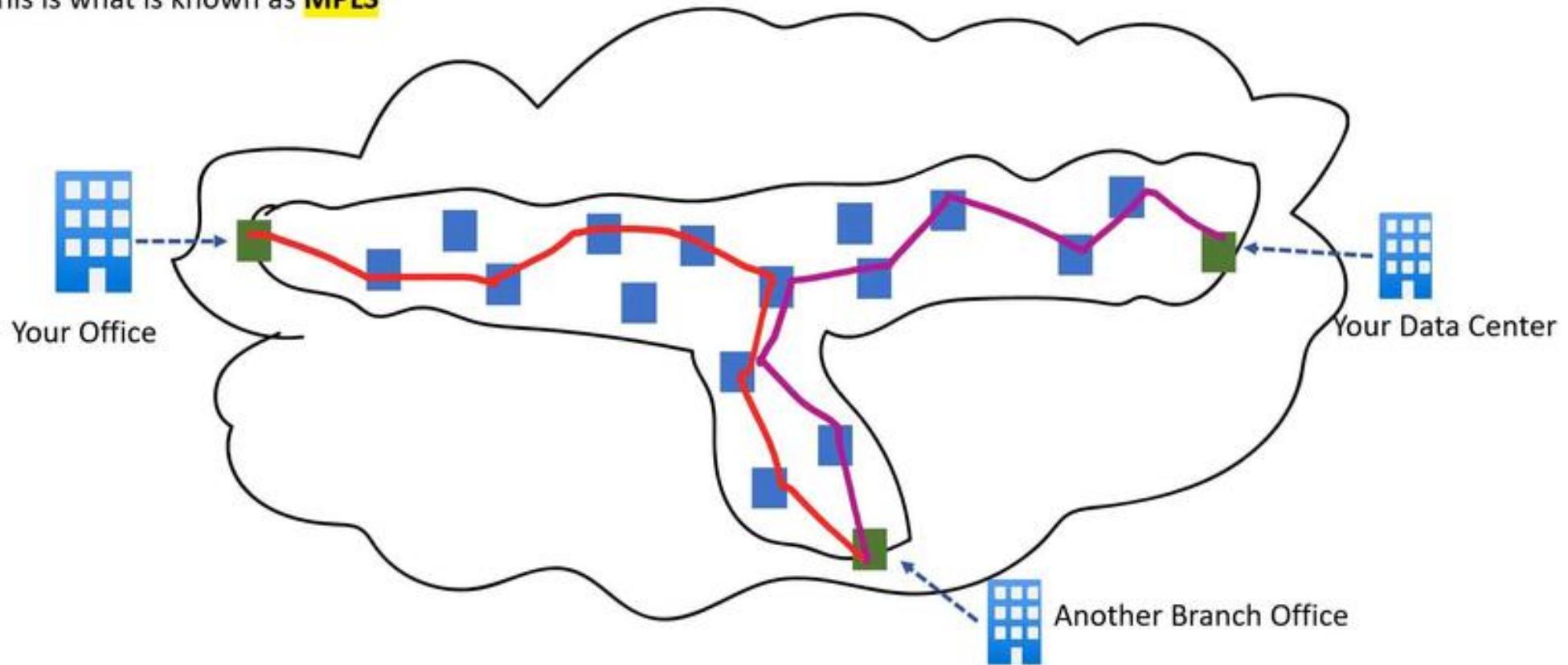
## Multiprotocol Label Switching



# Azure Virtual WAN - MPLS

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

What if instead of using the Internet we **establish a private connection** through trusted partners datacenters  
We apply a **special label** to our packets so **special network devices** can read the label's end destination and forward it  
the packet through the most efficient route through this private network.  
This is what is known as **MPLS**





# Azure Virtual WAN - MPLS

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is Multi-Protocol Label Switching (MPLS)?

It's a method of packet forwarding where instead of using IP Address and Layer 3 information to make forwarding decisions an **MPLS label** is used to determine the shortest route to end destination.

MPLS is a **private connection** linking data centers and branch offices.

MPLS is **outsourced and managed by service providers** who guarantee network performance, quality and availability.

MPLS uses a special network hardware that combines both a router and switch called a **Label Switch Router (LSR)**

MPLS is efficient because the path for a Label across the network will be pre-determined called a Label Switched Path

An MPLS Label is data inserted between Layer 2 and Layer 3 of your IP Packet and this is what they call a **Shim**

## Why use an MPLS?

- Virtual Private Networks (VPNs) — It makes it easy to for us to establish private connections
- Traffic Engineering (TE) — We can control how packets traverse the network
- Quality of Service (QoS) — We can ensure the performance and availability of our packets

## What is the downsides of MPLS?

- They get really **expensive**
- Its **private** and **not secure** (its just a routing mechanism, there is no inherit encryption)
- With the rise of cloud services, you still have to traverse the internet any in many cases





## Azure Administrator



# Software-Defined WAN

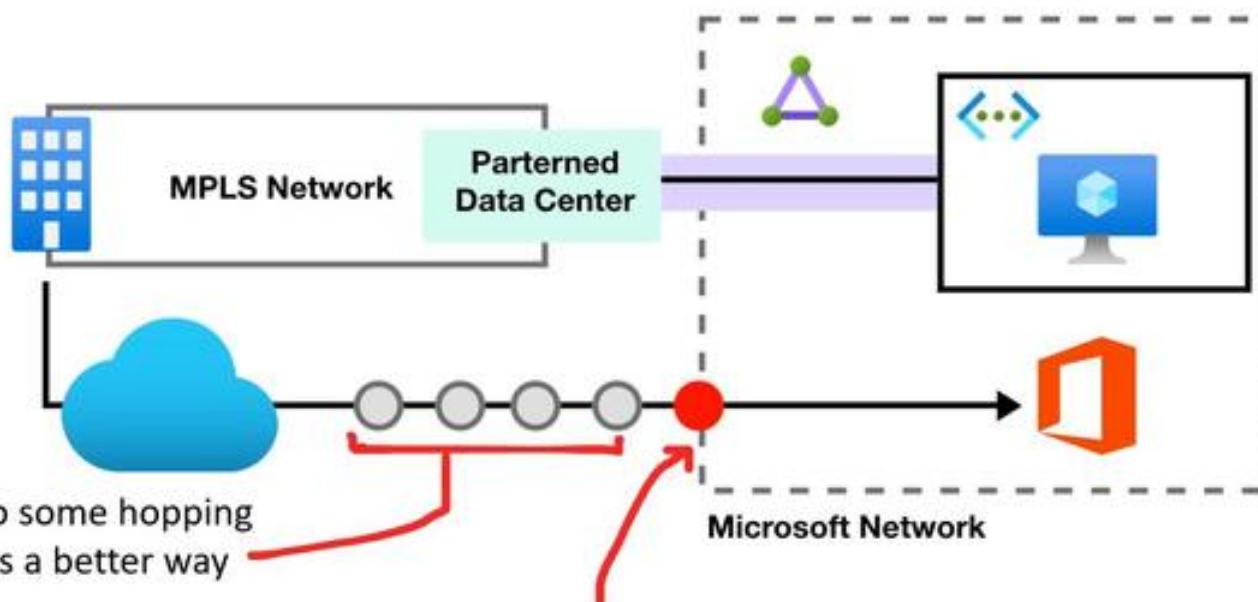


# Azure Virtual WAN – SD WAN

Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

If you want a fast and private connect to Azure you traverse the MPLS to a data center owned by trusted Azure partner and you establish your ExpressRoute to your VPN

If you want to use public facing cloud service like Office 365, traveling through your MPLS over ExpressRoute into the Microsoft Network to Office 365 and back through that route is not always fast



Azure has Point of Presence (PoP) distributed all around the globe that have regional presence and so connecting to Office 365 will be generally faster going through the internet.





# Azure Virtual WAN – SD WAN

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is Software Defined WAN (SD-WAN)?

SD-WAN decouples CPU intensive tasks from routers such as Management, Operations and the Control plane that can now be controlled in a central location remotely and virtually at your headquarters. Since most ISPs support SD-WAN architecture you can directly control the flow of traffic through the internet.

**SD-WAN** can replace MLPS, so you traverse the internet instead of a private network

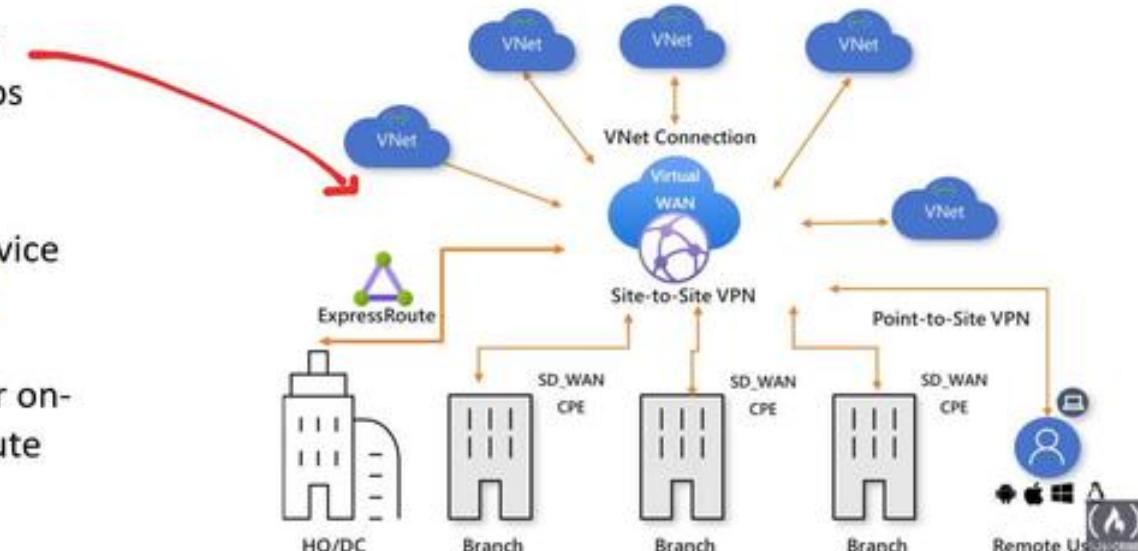
**SD-WAN** is more cost effective and require less configuration than an MLPS initially and at scale

**SD-WAN** is secure because you will use HTTPS which is supported by your ISP

With SD-WAN you are **pre-determining** the path through the Internet. So you can perform the least amount of hops to the closest Azure Point of Presence (PoP)

With Azure VirtualWAN you are deploying VNet with service endpoints on the edge of a region which is called **Hubs**

You are configuring virtual devices in Virtual Wan so your on-premise can connect to your Hub so it has the fastest route to your Azure cloud resources.





# Azure Administrator



## Virtual WAN CheatSheet



# Azure Virtual WAN *CheatSheet*



Azure Virtual WAN is a **consolidated networking service** that brings many **networking**, **security**, and **routing** functionalities in a single operational interface.

These functionalities include

- branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE)
- Site-to-site VPN connectivity,
- remote user VPN (Point-to-site)
- connectivity, private (ExpressRoute) connectivity,
- intra-cloud connectivity (transitive connectivity for virtual networks)
- VPN ExpressRoute inter-connectivity,
- routing
- Azure Firewall encryption for private connectivity.

Azure Virtual WAN itself is a **Software Defined WAN (SD-WAN)**

Azure Virtual WAN is a much better way to route to your branches, datacenters, VNet and cloud services.

**A Point of Presence (PoP)** Is an entry at the edge of a Network. eg. ISP Datacenter

**A Hop** is when you change networks

**Multi-Protocol Label Switching (MPLS)** a method of packet forwarding where instead of using IP Address and Layer 3 information to make forwarding decisions an **MPLS label** is used to determine the shortest route to end destination

**Software Defined WAN (SD-WAN)** decouples CPU intensive tasks from routers such as Management, Operations and the Control plane that can now be controlled in a central location remotely and virtually at your headquarters

- replace MPLS, so you traverse the internet instead of a private network
- more cost effective and require less configuration than an MPLS initially and at scale
- secure because you will use HTTPS which is supported by your ISP





# Azure Administrator



## Introduction to Virtual Network Gateways





# Virtual Network Gateways

Cheat sheets, Practice Exams and Flash cards  [www.exampro.co/az-104](http://www.exampro.co/az-104)

## What is a (Virtual Private Network) VPN?

A VPN **extends a private network across a public network** and enables users **to send and receive data across shared or public networks** as if their computing devices were directly connected to the private network.

## What is a Virtual Network Gateway?

- A **virtual network gateway** is the software **VPN** device for your Azure virtual network.
- When you deploy a virtual network gateway it will deploy two or specialized VMs in specific subnet you need to create called a “gateway subnet”
- These deployed VMs contain routing tables and run specific gateway services.
- You will choose a **Gateway Type** and that will determine if it's a **VPN Gateway** or an **ExpressRoute Gateway**

Gateway type \* 

VPN  ExpressRoute



# Azure Administrator



## VNG Designs



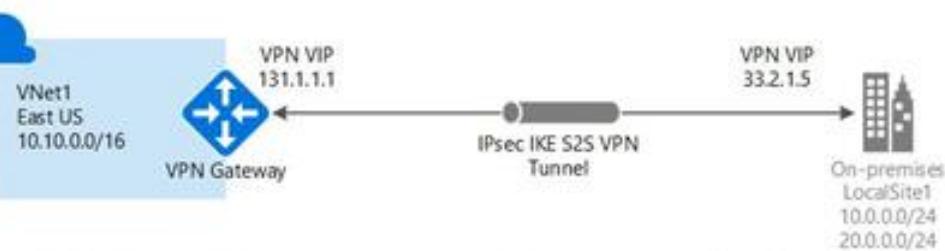
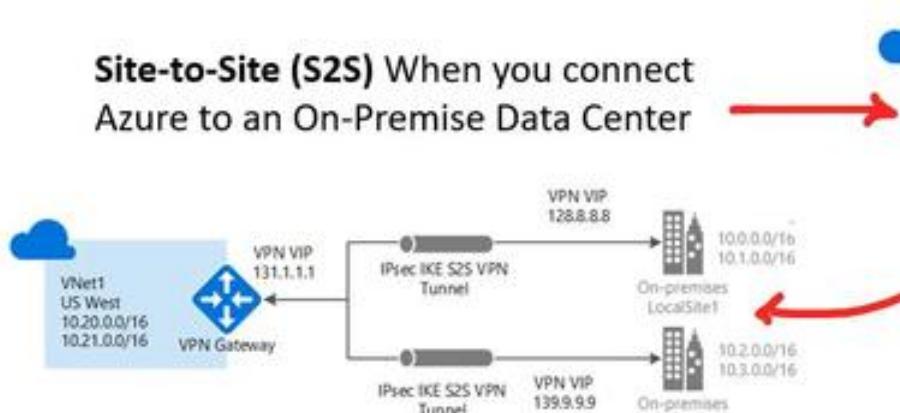


# VPN Gateway Designs

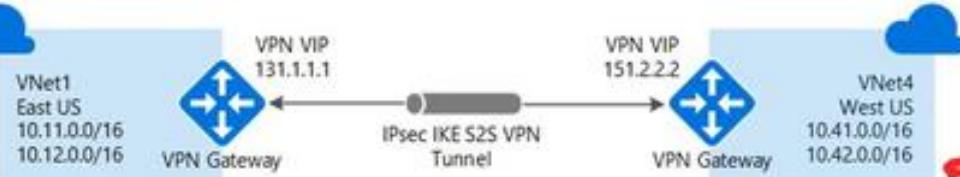
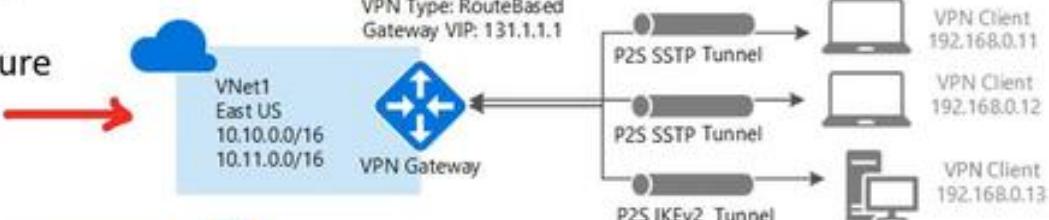
Cheat sheets, Practice Exams and Flash cards [www.exampro.co/az-104](http://www.exampro.co/az-104)

When you create a VPN Gateway you are generally designing for one of the following topologies:

**Site-to-Site (S2S)** When you connect Azure to an On-Premise Data Center



**Point-to-Site (P2S)** When you connect Azure to multiple individual computers



**VNet-to-VNet** When you connect two VNets in different regions, subscriptions or deployment models





# Azure Administrator



## VNG CheatSheet



# Azure Virtual Network Gateways *CheatSheet*



A VPN **extends a private network across a public network** and enables users **to send and receive data across shared or public networks** as if their computing devices were directly connected to the private network.

A **virtual network gateway** is the software VPN device for your Azure virtual network.

- When you deploy a VNG it will deploy two or more specialized VMs in specific subnet you need to create called a “gateway subnet”
- These deployed VMs contain routing tables and run specific gateway services.
- You will choose a **Gateway Type** and that will determine if it’s a **VPN or ExpressRoute**

When you create a VPN Gateway you are generally designing for one of the following topologies:

- **Site-to-Site (S2S)** When you connect Azure to an On-Premise Data Center
- **Multi-Site** When you connect Azure to multiple On-Premise Data Centers
- **Point-to-Site (P2S)** When you connect Azure to multiple individual computers
- **VNet-to-VNet** When you connect two VNets in different regions, subscriptions or deployment models